

Part 4

Project Fundamentals

Chapter 11

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.

11.1 Guidance from volume 1

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.

11.2 Background

It is always more effective to build safety in than to try to retrofit it later. Decisions on the form and structure of systems start to be taken at the beginning of projects and safety analysis should therefore start at the beginning so that safety considerations can influence the earliest decisions.

At the beginning of a project there is insufficient information to perform a detailed hazard analysis or risk assessment and the analysis is usually limited to a preliminary identification of hazards. This is sufficient to support early discussions on the approach to controlling each hazard, to ensure that each hazard is taken into account.

As decisions on the scope, functionality and design of the system are taken it is possible to improve the identification of hazards, to analyse their causes and consequences and, eventually, to assess the risks. In each phase of the project, the analysis should be taken as far as the available information permits, in order to provide the best support for decisions taken during that phase.

An iterative approach to analysis should therefore be taken, and the analysis will be improved and extended in step with the specification and design, with constant interaction between the two.

Other ESM activities also need to be performed during these phases. This chapter provides guidance on what should be done when. This chapter is written for:

- anyone involved in starting up a project and planning the later stages.

See also chapter 12 which provides guidance on safety planning.

11.3 Project lifecycle

To schedule ESM activities, it is necessary to know the lifecycle of your project (that is, the sequence of phases into which it is divided).

Different lifecycles are appropriate for different sorts of project. You should adopt a lifecycle that has been proven for the sort of work that is being undertaken.

To use the guidance in the following section, you will need to relate the lifecycle to the following generic lifecycle:

Concept and Feasibility	All activities that precede the construction of a requirements specification for the system or equipment.
Requirements Definition	The construction of a requirements specification
Design	All activities that result in a design baseline for the system and equipment.
Implementation	All activities that are involved in realising the design before introducing any changes to the railway.
Installation and Handover	All activities of introducing the change to the railway continuing up until normal operations start. For instance construction of civil works, installation and commissioning of signalling equipment and track testing of rolling stock.
Operations and Maintenance	All activities involved with the normal operation of the system or equipment.
Decommissioning and Disposal	All activities involved in removing the system or equipment from the railway. For instance demolition of civil works and removing or making safe trackside cabling.

Table 11-1 shows, as an example, a relationship between the generic lifecycle and the lifecycle presented in CENELEC standard prEN 50126 [F.8]:

50126 phase	Generic lifecycle phase
Concept	Concept and Feasibility
System Definition and Application Conditions	Requirements Definition
Risk Analysis	
System Requirements	
Apportionment of System Requirements	Design
Design and Implementation	Implementation
Manufacture	
Installation	Installation and Handover
System Validation	
System Acceptance	
Operations and Maintenance	Operations and Maintenance
Modification and Retrofit	
Performance Monitoring	
Decommissioning and Disposal	
Decommissioning and Disposal	Decommissioning and Disposal

Table 11-1 - The relationship between the generic lifecycle and the lifecycle presented in CENELEC standard prEN 50126

The relationship may be more complex. For instance:

- There may be submissions of interim, incomplete Safety Cases.
- With the staged introduction of a signalling scheme, there may be multiple Installation and Handover phases with Implementation activities in between.
- There may be a period when the new system is running in parallel with the old one.

11.4 Activities by phase

Having established a project lifecycle and related it to the generic lifecycle, then you can use Table 11-2 for guidance on the minimum ESM activities that are appropriate to each phase. Note that it is necessary to keep all documents, such as the Hazard Log up-to-date throughout the lifecycle but the necessary updates are not shown. Note also that the guidance on Independent Professional Review in chapter 14 may suggest more Safety Audits and Assessments than are shown in the table and that it may be necessary to make more than one Safety Case submission.

Generic lifecycle phase	Principal ESM Activities	See Chapter
Concept and Feasibility	Preliminary Hazard Identification	8, Assessing and Reducing Risk
	Establish Hazard Log	13, Config. Management, Documentation and Records
	Preliminary Safety Plan	12, Safety Planning and Good Practice
Requirements Definition	Hazard Analysis (and revisiting Hazard Identification)	8, Assessing and Reducing Risk
	Risk Assessment	8, Assessing and Reducing Risk
	Establish Safety Requirements	9, Safety Requirements
	Full Safety Plan	12, Safety Planning and Good Practice
Design	Risk Assessment	8, Assessing and Reducing Risk
	Safety Audit	14, Independent Professional Review
Implementation	Risk Assessment	8, Assessing and Reducing Risk
	Safety Case	10, Safety Evidence and Authorising Changes
Installation and Handover	Safety Assessment	14, Independent Professional Review
	Safety Endorsement	10, Safety Evidence and Authorising Changes
	Transfer Safety Responsibilities	2, Safety Responsibilities
Operations and Maintenance	Update Hazard Log and Safety Case	13, Config. Management, Documentation and Records
Decommissioning and Disposal	Update Hazard Log and Safety Case	13, Config. Management, Documentation and Records

Table 11-2: Minimum ESM activities for each phase in the generic lifecycle

11.5 Reacting to modifications and new information

Your configuration management arrangements (see chapter 13) should establish baselines and then provide a procedure for assessing, authorising and tracking changes to these baselines. This procedure should assess the affect on safety of any proposed change and should ensure that, when a change is authorised, any necessary changes to ESM documents, including the Hazard Log, are made.

Your configuration management arrangements should provide a procedure for assessing faults discovered in baselines, defining any corrective action and then following this through. This procedure should include assessing whether any faults show the need to amend any ESM documents, including the Hazard Log, and if so ensure that the amendments are made. These procedures should make use of a Data Recording And Corrective Action System (see appendix E).

When the system or equipment is introduced to the railway, your management of the Hazard Log (see chapter 13) should include a procedure for logging any incidents that occur, assessing them and defining any corrective action that is necessary to prevent them from recurring. This procedure should also assess the need to change any ESM documents.

11.6 Related guidance

Guidance on writing a Safety Plan is provided in chapter 12.

Guidance on maintaining a Hazard Log provided in chapter 13.

Guidance on establishing a Data Recording And Corrective Action System is provided in appendix E.

This page left intentionally blank

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.

Chapter 13

Configuration Management, Documentation and Records

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

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

13.1 Guidance from volume 1

13.1.1 Configuration management

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.

13.1.2 Documentation and records

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.

13.2 Background

A convincing demonstration of safety rests on good housekeeping.

Certain items within a system need to be accurately identified and changes to them need to be assessed for any safety implications and then monitored and tracked. This provides information on the different versions that may exist for that item, its relationship with other items, and the history of how it has developed and changed.

This chapter describes how to identify items whose configuration should be recorded and kept under control. It explains why configuration management should be applied to safety-related system items and documents and how it may be monitored.

There are three main reasons for keeping records of safety-related activities:

- 1 to show others that you have reduced risk to an acceptable level;
- 2 to explain to people making future changes why decisions were taken, so that they do not undo the work that you have done; and
- 3 to support the hand-over of safety responsibilities to other people.

Project managers are responsible for keeping adequate records of ESM activity (safety records), to provide evidence that these activities have been carried out and to record the results of these activities.

A log of all safety records and documentation and all identified hazards and potential accidents should be maintained; this log is termed the **Hazard Log**.

This chapter describes the Hazard Log and other safety records that should be produced and kept. It also describes how they may be managed and controlled so that the most up-to-date versions are available.

This chapter is written for:

- Project Managers who are responsible for controlling the configuration of safety-related projects,
- engineering staff who make changes to any safety-related item, and
- managers and engineers who are responsible for preparing or updating safety records.

13.3 Roles and responsibilities

The Project Manager is responsible for the configuration management of all items relating to the project. The Project Manager should write a configuration management plan detailing how this will be achieved, and should ensure that it is followed. These responsibilities may be delegated but the Project Manager normally retains overall accountability.

The Project Manager will normally be responsible for setting configuration management policy and defining processes for configuration control.

The Project Manager is responsible for the creation and maintenance of the Hazard Log and other safety records until the transfer of overall safety responsibility to another party.

The Project Manager may delegate this role to a Project Safety Manager but should retain overall responsibility. Guidance on transferring safety responsibility is provided in chapter 2.

13.4 Identification of configuration items

The identification of configuration items should be started during the early stages of project definition. There may be a number of hierarchical levels of items under configuration control, reflecting the system structure (though it may not be necessary to control all system items). The relationship between configuration items should be documented to provide traceability information. For example, there may be composite items consisting of smaller items; items may be derived from other items (such as design items derived from the requirements).

You should place all items which will support the Safety Case under configuration management. You should consider placing the following items under configuration management:

- safety-related items;
- items interfacing to other systems;
- items identified as deliverables;
- documentation of enduring value, such as:
 - specifications,
 - designs,
 - drawings,
 - test specifications,
 - user and maintenance manuals,
 - other technical manuals;
- items particularly susceptible to change (for example, software);
- items supplied by other suppliers.

The following information should be maintained for each item

- unique identifier;
- item name and description;
- version number;
- modification status.

All items placed under configuration management control should be indexed, and the index itself should be placed under configuration management.

Section 13.5.4 details considerations specific to software items.

13.5 Configuration management plan

Configuration management on a project should be planned and documented in a configuration management plan or a configuration management section of the project plan. This plan should define:

- a) a list of the types of configuration items;
- b) responsibilities for configuration management within the project, including the person responsible for approving updates to configuration items;
- c) the baselines that will be produced;

- d) the version control arrangements;
- e) the change control process;
- f) software configuration management arrangements (if required); and
- g) any configuration management tools used.

Items c) to g) inclusive are expanded on below.

13.5.1 Baselines

A baseline is a consistent and complete set of configuration item versions. It should specify:

- an issue of the requirements specification;
- all of the configuration items that are derived from these requirements; and
- all the component items and their versions that the configuration items are built from.

Baselines are established at major points in the system lifecycle as a departure point for the control of future changes.

13.5.2 Version control

Different versions of the same item may be needed as the system develops, to allow for different applications both during the project (such as testing and debugging) and while in operation (such as different processors, or increased functionality).

Versions may be controlled by assigning a unique reference number, a meaningful name and a status to each version, and by monitoring changes to the versions.

Changes made to different versions should be tracked to provide and maintain a change history. In addition, superseded versions of documentation and software should be archived to allow for reference.

It should be possible to readily establish the status of a version, to tell if it has been approved for use or not. Items known to be faulty should be clearly marked as such so that they are not used by mistake.

13.5.3 Change control process

Any changes to a baselined item should be assessed to identify the safety implications of the change (such as the introduction of a new hazard). Changes should be documented and should follow a process for requesting change, assessing the change and the effect that it may have on other configuration items, and reviewing the change.

13.5.4 Software configuration management

All software programs that are deliverable, or affect the delivered product, should be held under change control, including:

- application programs,
- test programs,
- support programs,
- sub-programs used in more than one higher-level program,
- firmware components,
- programs for operation in different models,
- sub-programs from separate sources to be used in one higher-level program.

13.5.5 Configuration management tools

Configuration management requires a means of storing and controlling the configuration items. Some form of electronic database may be the best option and there are many tools available to perform this function. However, it is possible to perform configuration management without using electronic tools.

It is not necessary to contain all items under the same system. In fact it is often more efficient to separate the items into logical groups, such as software items, documentation, physical items, and so on and to choose the best tool for each group.

You should consider whether there is any plausible way in which a configuration management tool could contribute to a system hazard. If there is then you should regard the tool as safety-related and collect evidence of its dependability for inclusion in the Safety Case for the system.

13.6 Safety records

All safety-related projects should produce at least the following safety records:

- Hazard Log,
- Safety Plan,
- Safety Case.

Further records may be required for many projects. The extent of the safety records maintained by a project will depend on the complexity and level of risk presented by the project. Simple and low-risk projects will carry out only a small number of safety-related activities and the records required of these will be small. High-risk and complex projects will produce more safety records.

Safety records are valuable and difficult to replace. Appropriate security and backup safeguards should be employed to ensure their integrity.

The Hazard Log is the key safety record. Its functions include:

- detailing hazards and potential accidents;
- maintaining a list of safety records and a chronological journal of entries;
- providing traceability to all other safety records; and
- collating evidence for the Safety Case.

Figure 13-1 illustrates the relationship between the Hazard Log and other safety records.

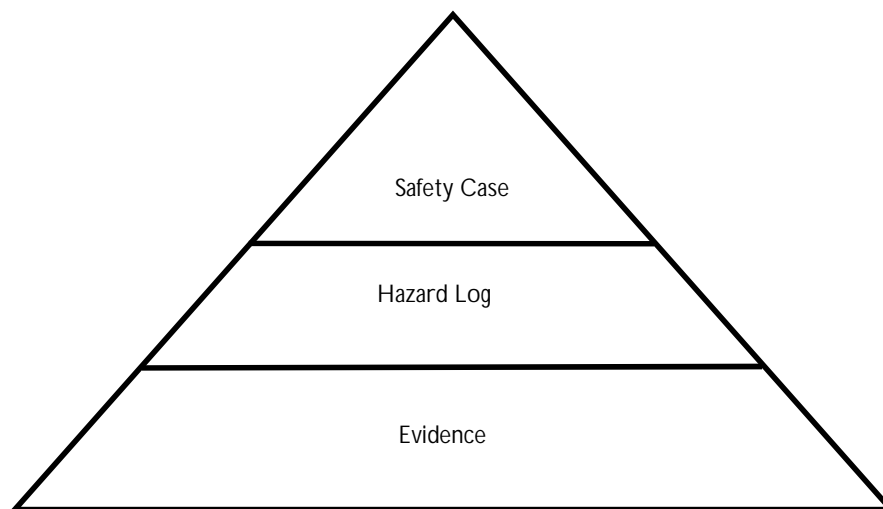


Figure 13-1 - Pyramid of safety management documentation

Note: there is variation in terminology in the industry and the phrases 'Safety Case' and 'Hazard Log' are sometimes used to include the evidence below them in Figure 13-1.

13.7 Management and control of the Hazard Log

The Hazard Log evolves and should be updated whenever:

- a relevant hazard or potential accident is identified;
- a relevant incident occurs;
- further information relating to existing hazards, incidents or accidents comes to attention; or
- safety documentation is created or re-issued.

The Hazard Log should be stored with the project file so that referenced material is easily accessible. Each section of the Hazard Log may be a separate document, as long as the individual documents are stored together.

The Project Manager should identify a process for updating the Hazard Log, to include project staff with authority to make entries. Each entry in the Hazard Log should be approved by the Project Manager, or delegate.

The Hazard Log should be available for inspection by the Safety Auditor, the Safety Assessor and representatives of the relevant Safety Authorities.

The Project Manager should ensure that adequate provision is made for security and backup of the Hazard Log and other safety records.

It is not necessary to repeat information documented elsewhere and so the Hazard Log should make reference to other project safety documentation such as analyses and reports. It is recommended that the Hazard Log be implemented electronically. Special purpose tools are available to enable this, but it is also possible to store the Hazard Log in a database, keeping Hazard Data, Accident Data, Incident Data and the Directory in separate tables. An outline Hazard Log is provided in appendix B.

13.8 Related guidance

Chapter 8 provides guidance on assessing and mitigating any safety implications of changes.

Safety Audits and Assessments of safety documentation are described in chapter 14.

Appendix B provides an outline Hazard Log.

Appendix C provides checklists for updating the Hazard Log.

This page left intentionally blank

Chapter 14

Independent Professional Review

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

14.1 Guidance from volume 1

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.

14.2 Background

Review of safety-related projects by professionals independent of the work is an important contribution to the confidence in the safety of the change being made to the railway.

We divide independent professional review into two activities:

- Safety Audits focus on the ESM processes being used and check that they are adequate and are being followed.
- Safety Assessments focus on the product of the project and check that the risk associated with the system being developed is (or will be) reduced to an adequate level.

In practice there is overlap between the two.

There is variation in terminology and practice in this area. Some practitioners divide the topic of independent professional review up differently and use the phrases 'Safety Audit' and 'Safety Assessment' with different meanings. For example, a distinction is sometimes drawn between technical assessment of engineering design and process assessment of safety management activities. You may need to refer to the guidance under both the audit and assessment headings even if the activity that you are asked to commission or perform is described as one or the other type of review.

This chapter describes these two types of review and the documentation that is required by them. It also discusses how to go about commissioning a review, what the reviews should be checking for, and how the results should be used. Outlines and checklists are provided in appendices B and C, respectively.

This chapter is written for Project Managers who will need to commission reviews and interpret the results, and the auditors and assessors who will be performing them.

14.3 Safety Audits and Assessments

14.3.1 Safety Audits

Safety Audits are intended to check that the ESM of a project is adequate and has been carried out in conformance with the Safety Plan. If there is no Safety Plan, one should be written before a Safety Audit is carried out.

The primary output of an audit is a Safety Audit Report. This report should include: a judgement on the extent of the project's compliance with the Safety Plan; a judgement on the adequacy of the Safety Plan; and recommendations for action to comply with the Plan or to improve it.

A Safety Audit should consider:

- work since the previous audit (all work so far if first audit);
- plans for the next stage;
- recommendations of the previous audit.

14.3.2 Safety Assessments

Safety Assessment is the process of forming a judgement as to whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level.

The safety requirements for the system are central to a Safety Assessment. The assessor should review the Safety Requirements Specification to assess whether it is sufficient to control risk and review the system to assess whether or not it meets or will meet the Safety Requirements Specification.

Safety Assessment involves the use of design analysis, auditing techniques and practical assessment by competent and experienced persons.

The assessor should also review the processes and organisation employed on the project. This aspect of the assessment is easier if the results of a recent Safety Audit are available. If a Safety Audit has not been carried out on the project recently enough that its conclusions are still valid, then one should be commissioned before a Safety Assessment, to ensure that the documentation to be assessed has been produced under a correctly applied Safety Plan. If the audit results are unsatisfactory then the assessment may be postponed until corrective action has been taken.

The result of a Safety Assessment is a Safety Assessment Report. This report should include an assessment on whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level and recommendations for corrective action if necessary.

If the risk is not assessed as acceptable then the system may need to be re-assessed after corrective action is taken.

14.4 Commissioning a Safety Audit or Assessment

In general the frequency and depth of each type of review and the level of independence of the reviewer (the Safety Auditor or Safety Assessor) will depend on the complexity and level of risk presented by the project.

Typically, Safety Audits and Assessments of the simplest and lowest risk projects should not take more than about a day of effort from a single auditor or assessor. Safety Audits of the most complex and highest risk projects may involve much more effort from an independent organisation.

Audits and assessments should be commissioned at the points defined in the Safety Plan (see chapter 12). The Project Manager or Safety Authority may commission additional audits or assessments.

Whoever commissions an audit or assessment should write a Safety Audit/Assessment Remit. This should record the requirements of the Audit or Assessment and all the relevant details, including:

- 1 the project title and reference;
- 2 the name of the Safety Auditor/Assessor, their qualifications and experience, and their level of independence;
- 3 references to previous audits and assessments;
- 4 audit or assessment requirements defining:
 - a) the scope of the audit/assessment which may be limited in extent (for instance, to a part of the system) or in time (for instance, to changes since the last release);
 - b) the purpose of the audit/assessment (for instance, to support a submission for safety approval);
 - c) the basis of the audit/assessment. For an audit this will define the documents that the project will be audited against (normally the Safety Plan and the documents that it references). For an assessment this should specify the legal framework (for instance, the ALARP principle in the UK) and the ESM framework (for instance, the Yellow Book) within which the project is being run; and
 - d) any previous assessments or audits whose results may be assumed in the performance of the current audit/assessment.

The remit should be agreed and signed by the Project Manager and the Safety Auditor/Assessor. An outline for a Safety Audit/Assessment remit is provided in appendix B and an example generic Safety Assessment remit is provided in appendix D.

14.4.1 Independence

The Safety Auditor/Assessor should be independent of the project. Whoever commissions an audit or assessment should decide the level of independence. The following paragraphs provide guidance only.

The level of independence should be dependent primarily on the level of risk presented by the project (for electronic systems this is indicated by the Safety Integrity Level (SIL) of the system or equipment being developed. SILs are discussed in chapter 9.)

Table 14-1 provides guidance (derived from IEC 61508 [F.14]) on the level of independence appropriate at each SIL. Note that 'HR' indicates Highly Recommended, 'NR' indicates Not Recommended, and '-' indicates no recommendation for or against; however, a lower level of independence may be chosen by agreement with the Safety Authority. For the highest risk projects the Safety Auditor or Assessor should work for an independent organisation. For the lowest risk projects they may be organisationally close to the project, but should not be working on the project.

MINIMUM LEVEL OF INDEPENDENCE	SAFETY INTEGRITY LEVEL			
	1	2	3	4
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	NR
Independent Organisation	-	-	HR	HR

Table 14-1 - Levels of independence at each SIL

Where the Safety Integrity Level of the system or equipment is not known, for example when Safety Requirements have not yet been set, the level of independence should depend on the likely consequence of an accident caused by the system or equipment. Table 14-2 provides guidance on the level of independence appropriate at each classification of consequence defined in chapter 8. The nomenclature is as for Table 14-1.

MINIMUM LEVEL OF INDEPENDENCE	CONSEQUENCE			
	Negligible	Marginal	Critical	Catastrophic
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	-
Independent Organisation	-	-	HR	HR

Table 14-2 - Levels of independence at each consequence category

Where the tables indicate a choice of independence (for example, Table 14-1 indicates that both Independent Person and Independent Department are Highly Recommended for a SIL 2 system), the following factors should be considered in deciding an appropriate level of independence:

- the degree of previous experience with a similar design;
- the degree of complexity;
- the degree of novelty of the design, or technology; and
- the degree of standardisation of design features.

These factors may also guide the determination of the duration of a particular Safety Audit or Assessment. For example a system development utilising a novel technology is likely to require a more extensive Safety Audit/Assessment than a development using proven technology.

14.4.2 Qualifications

The Safety Auditor should have the following qualifications:

- prior experience as a Safety Auditor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- experience of process assurance (for instance quality or safety audits);
- familiarity with external safety standards and procedures;

- familiarity with the legal and safety regulatory framework within which UK railways operate;
- training in ESM.

The Safety Assessor should have the following qualifications:

- Chartered Engineer status in an engineering or scientific discipline relevant to the system or equipment;
- prior experience as a Safety Assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- demonstrable application domain experience;
- experience of process assurance (for instance quality or safety audits);
- familiarity with external safety standards and procedures;
- familiarity with the legal and safety regulatory framework within which UK railways operate;
- training in ESM.

The following factors should be taken into account in establishing the relevance of experience:

- purpose of the project;
- technology and methods used;
- Safety Integrity Level and accident potential.

Where a Safety Assessment is carried out by a team, the team as a whole should exhibit the necessary domain and process assurance experience and the lead assessor as an individual should possess the other qualifications.

It is a good idea to retain the same Safety Auditor and Assessor throughout the project.

14.4.3 Depth of review

Engineering judgement should be applied to determine the degree to which the guidance above need be applied on a particular project. For the simplest and lowest risk projects, for example:

- The requirements for Safety Auditor or Assessor qualifications may be relaxed.
- Audit or Assessment activities listed in section 14.5 may be limited to interviewing personnel and reviewing documentation.
- The detail of the audit checklist or assessment checklist may be reduced.
- The Safety Audit or Assessment Report described in appendix B should concentrate on the findings and recommendations of the Safety Audit; the requirements and audit details sections should be brief.

The Safety Audit or Assessment Report should record and justify significant changes to the processes defined in section 14.5.

The Safety Assessment Report should concentrate on the findings and recommendations of the Safety Assessment; the requirements and assessment details sections should be brief.

14.4.4 Roles and responsibilities

The Project Manager is responsible for:

- initiating Safety Audits or Assessments when scheduled in the Safety Plan;
- preparing the Safety Audit/Assessment requirements;
- appointing an auditor or assessor acceptable to the Safety Authority;
- ensuring the auditor/assessor has appropriate access to personnel, the Hazard Log and other documents;
- commenting on the Safety Audit or Assessment Report;
- formulating any necessary improvement actions in response to the report's recommendations;
- passing on any parts of the report which materially affect the Safety Assessment process to the Safety Authority; and
- implementing the improvement actions.

The Safety Auditor is responsible for:

- planning the Safety Audit;
- carrying out the Safety Audit; and
- preparing a Safety Audit Report.

The Safety Assessor is responsible for:

- planning the Safety Assessment;
- carrying out the Safety Assessment; and
- preparing a Safety Assessment Report.

14.5 The Safety Audit and Assessment processes

14.5.1 Performing a Safety Audit

The Safety Audit process consists of three activities:

- 1 Planning the Safety Audit and producing an audit schedule;
- 2 Executing the audit schedule;
- 3 Preparing the Safety Audit Report.

The audit schedule should be produced by the Safety Auditor and endorsed by the Project Manager. Planned activities may be modified to reflect any required change of emphasis based on information gathered during the audit, although it is not always necessary for the audit schedule to be re-issued.

The schedule should be brief and should include:

- A statement of the audit requirements, according to the Audit Remit, but taking into account any agreed amendments;
- Identification of audit activities to be undertaken;
- Identification of individuals to be interviewed;
- Identification of documentation to be examined;

- Audit time-scales;
- Safety Audit Report distribution and the expected date of issue.

During audit planning the Safety Auditor should become familiar with:

- The Safety Plan;
- The findings and recommendations of any previous Safety Audits;
- Details of progress since the last Safety Audit (if any);
- Details of the next stage of work;
- Details of project staffing.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The audit activities should include:

- Interviews with project personnel;
- Examination of project documents;
- Observation of normal working practices, project activities and conditions;
- Demonstrations arranged at the auditor's request.

The evidence for compliance or non-compliance with the Safety Plan that arises from these activities should be noted for inclusion in the Safety Audit Report.

14.5.2 What to look for in a Safety Audit

The Safety Audit is a check for adequacy of the Safety Plan and compliance against the Safety Plan. The audit should check therefore, that the planned project activities are being or have been carried out and in the manner and to the standards prescribed in the Safety Plan.

The Safety Auditor should derive an audit checklist for the investigation, to guide the enquiries and to record results and evidence. An outline for the checklist and an example are included in appendix D. The format of the checklist should mirror that of the Safety Plan and associated ESM activities such that each aspect of these is directly addressed by a question in the checklist. It should be in the form of a checklist with questions that may be answered 'Yes' or 'No'.

The checklist should be drawn up to meet the audit requirements, using the documents referenced in the Remit. The auditor should note anything that he or she finds that is objectively wrong, whether or not it relates to a checklist item. Note that the checklist is an aid for the Safety Auditor – it should not be completed by the project personnel.

The audit should check that any standards or procedures called up by the Safety Plan have been correctly applied. It should also check that there is traceability from the Safety Plan to project activities that implement it.

The audit should look for documentary evidence that every safety activity has been carried out. The answer to each question on the audit checklist should be supported by documentary evidence.

All instances where there is no evidence of compliance should be documented in the Safety Audit Report along with a recommendation for remedial action. Each non-compliance should be identified in terms of the specific requirements of the Safety Plan. The auditor should classify each finding. A suggested classification is shown in section 14.6.

Audit findings should be documented on the checklist. Where evidence of compliance is lacking, further in-depth examination should be carried out.

Information gathered through interviews should, where possible, be verified by acquiring the same information from other independent sources.

14.5.3 Performing a Safety Assessment

The Safety Assessor should become familiar with:

- The Hazard Log;
- The Safety Plan;
- The Safety Requirements Specification;
- The findings and recommendations of any previous Safety Assessments or Safety Audits;
- Details of progress since the last Safety Assessment;
- Details of the next stage of work.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The Safety Assessor should prepare an assessment plan. The plan should be brief and should include:

- A statement of the assessment requirements, according to the assessment remit, but taking into account any agreed amendments;
- Identification of any dependencies on the project or others, such as access to project personnel or documents;
- Identification of the assessor or assessment team, including qualifications, experience and level of independence;
- Identification of individuals to be interviewed;
- Management arrangements for reporting findings and reviewing, endorsing and distributing the Safety Assessment Report;
- Assessment time-scales, including the expected date of issue of the Safety Assessment Report.

The assessment activities should include:

- Interviews with project personnel;
- Examination of project documents;
- Observation of normal working practices, project activities and conditions;
- Re-work of parts of the safety analysis work to check accuracy, concentrating on particularly critical areas or where the assessor has reason to suspect a problem;
- Demonstrations arranged at the assessor's request.

14.5.4 What to look for in a Safety Assessment

The primary objective in planning and carrying out a Safety Assessment is to make sure that you collect enough information to support a judgement on the acceptability of the risk. The following guidance may help in planning the assessment but you should also employ your professional judgement and experience to tailor the guidance to the application in hand.

The assessment should examine the development or application process, review the design decisions taken by the project staff which have safety implications and verify that that risk has been reduced As Low As Reasonably Practicable (ALARP) and in accordance with the Safety Requirements.

The Safety Assessor should derive an assessment checklist to guide the enquiries and to record results and evidence. Example checklists are presented in appendix D. The checklist should be drawn up to meet the assessment requirements, using the documents referenced in the remit. The assessor should note anything that he or she finds that is objectively wrong, whether or not it relates to a checklist item. Note that these checklists are an aid for the Safety Assessor – they should not be completed by the project personnel.

The assessment should not just focus on documents but should look at the processes and organisation behind them. The assessor should look for any shortcomings in the approach to safety and make recommendations.

The assessment should pay particular attention to the Hazard Log, which should provide traceability from the Safety Requirements to documentation supporting engineering activities on the project.

The assessment should check that there is documentary evidence for every safety activity carried out. The answer to each question on the assessment checklist should be supported by documentary evidence.

If operational data is available, the assessor should analyse it for evidence of:

- hazards not previously identified;
- risks incorrectly classified;
- Safety Requirements not met;
- changes in the pattern of operational use.

The Safety Assessor may call for the repetition of any formal tests and the Project Manager should arrange for these to be run under the Safety Assessor's supervision.

If a previous assessment has been carried out and has not been invalidated by changes to the design or new knowledge then the assessor need not repeat the analyses carried out there and should concentrate instead on analysing new and changed material.

If the assessment detects a flaw in the ESM programme then the assessor should review the ESM documentation to establish the most likely root cause. The assessor should consider whether this throws doubt on any other aspects of the ESM, and the assessment recommendations should include measures to restore confidence in affected areas as well as addressing the defects detected.

Information gathered through interviews should, where possible, be verified by checking the same information from other independent sources.

14.5.5 Findings

Findings should be communicated to the Project Manager and project team as soon as possible. You should not wait until the Safety Audit/Assessment Report is prepared and distributed.

This may conveniently be done with a simple three-part form:

- Part 1: Finding
- Part 2: Project response
- Part 3: Assessor's/auditor's comments on project response.

14.6 Audit/assessment findings

All auditor's and assessor's findings should be uniquely numbered and classified. The following classification scheme is widely used and is recommended. Categories 1 to 3 should be used when the audit/assessment is supporting a request for safety approval.

Category 1 - Issue is sufficiently important to require (substantial) resolution, prior to recommending that the change may become operational. (Alternatively a specific control measure may be implemented to control the risk in the short term.)

Category 2 - Issue is sufficiently important to require resolution within 3-6 months, but the change may become operational in the interim (possibly with a protective control measure.)

Category 3 - Issue is highlighted for incorporation into the Safety Case at the next periodic review, but no action is required separately.

Where there are a large number of lower category issues, the auditor/assessor should consider whether, in totality, they represent sufficient residual risk that they in effect equate to one or more higher category issues (that is, that they would warrant the imposition of any additional mitigating control measures). In these circumstances, it should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document that has been reviewed.

The Project Manager should review and endorse the Safety Audit/Assessment Report, and formulate improvement actions in response to the Safety Auditor's/Assessor's findings. It may be appropriate to record any faults discovered in the system itself in the Data Recording and Corrective Actions System (see chapter 12). The Project Manager should implement these improvement actions.

The Safety Assessment Report may include recommendations for action by the relevant Safety Authorities, for example reviewing the approval of systems or equipment in service. If the report contains any such recommendations the Project Manager should pass that part of the report to the relevant Safety Authorities, who should then consider any such recommendations and implement promptly any necessary actions.

14.7 Related guidance

Chapter 8 provides guidance on risk assessment

Chapter 9 provides guidance on the safety requirements specification and Safety Integrity Levels.

Chapter 12 provides guidance on safety planning.

Appendix B provides outline audit and assessment remits and reports.

Appendix D provides an example assessment remit and example audit and assessment checklists.

This page left intentionally blank