

# Chapter 1

## Introduction

### 1.1 Purpose and scope of this volume

Issue 2 of the Yellow Book described one proven and effective approach to managing the safety of railway change. Other approaches are being developed in the UK and the rest of Europe, and, although the differences are generally minor, there is increasing potential for confusion. In issue 3 we have tried to distil the fundamentals behind these approaches and then present them in volume 1.

This volume provides guidance on implementing the ESM fundamentals presented in volume 1. None of the content of this volume should be regarded as prescriptive – there are other effective ways of implementing the fundamentals – but the guidance is representative of good practice.

ESM is the process of making sure that the risk associated with *changes* to the railway (such as new trains and signalling) is reduced to an acceptable level. ESM is not just for engineers and can be used for changes that involve more than just engineering. ESM, and this publication, are however scoped to:

- controlling *safety* risk, that is the risk of harming people, rather than the risk of environmental or commercial damage;
- *changes* to the railway rather than day-to-day operational safety; and
- *system* safety rather than occupational health and safety.

The Yellow Book does not provide a complete framework for making decisions about railway changes. It is concerned with safety and does not consider non-safety benefits. Even as regards safety, the Yellow Book does not dictate the values which underlie decisions to accept or reject risk. However, it does provide a rational framework for making sure that such decisions stay within the law and reflect your organisation's values and those of society at large and for demonstrating that they do so.

This guidance has been written with *significant* changes in mind. You may find it useful for smaller changes but you should consider scaling the activities described in order to implement the fundamentals of volume 1 cost-effectively.

### 1.2 How this volume is written

After this introduction, each chapter provides guidance on one or more of the fundamentals from volume 1. The fundamentals are reproduced in a box at the beginning and the summary guidance from volume 1 is reproduced afterwards.

The chapters of volume 2 are in the same order as the fundamentals of volume 1. The fundamentals in volume 1 are arranged under three headings:

- the **organisation**, including the people who work within it, that will carry out the work;

- the proposed **change** to the railway; and
- the **project**, that is the collection of activities which will realise the change.

The chapters of this volume are grouped into three parts corresponding to these headings.

The chapters refer to each other and these cross-references are summarised in 'Related Guidance' sections at the end of each chapter.

Supporting material is supplied in appendices which provide:

- a glossary of terms,
- document outlines,
- checklists,
- examples,
- brief descriptions of relevant specialist techniques, and
- a list of referenced documents.

Specialist terms are printed in bold when introduced (but note that bold text is also used to highlight key words in lists). The most specialist terms, such as 'Safety Case' are written with initial capitals. All of these are defined in appendix A, the glossary.

There is a list of referenced documents in appendix F and references are indicated in the text in the form '[F.1]'.

### 1.3 ESM overview

This volume takes the view that:

- any change to the railway can be regarded as introducing a new system or changing an existing one; and
- any change to the railway should be managed as a project.

Figure 1-1 presents a simplified view of a possible sequence of ESM activities that may be carried out during a project and the interactions between the parties involved. The figure is not a full definition of the process, but an illustration of its main features. It is simplified in that iteration, change, multiple safety assessment and rework are natural ways of working on projects but none of these are shown. Nonetheless it provides an overview of the main activities and their relationship.

Refer to section 1.4 below for a description of the notation. The diagram describes the following sequence of activities.

The Safety Lifecycle begins with the production of **Preliminary Safety Plan** by the project. The Preliminary Safety Plan is typically submitted to the **Safety Authority**, the person or organisation ultimately responsible for approving the change, for endorsement.

The project then establishes a **Hazard Log**. The Hazard Log is used for recording details of accidents and hazards, and details of safety documentation, and is used to provide evidence of the management of safety by the project.

The Hazard Log is at the centre of effective ESM and it should be established early, even though there may be little information to put in it at first.

**Hazard Identification and Analysis** and **Risk Assessment** are then carried out.

On the basis of the Risk Assessment, **Safety Requirements** are prepared. These requirements are typically endorsed by the Safety Authority.

Once the Safety Requirements have been determined, a **Safety Plan** is prepared and submitted to the Safety Authority for endorsement. Safety activities defined by the Safety Plan are then carried out.

At various times, Independent Safety Audits and Assessments may be commissioned. Typically, these will be commissioned in the early stages of a project to ensure an appropriate approach is being taken, and at the later stages of a project to provide evidence for use in the Safety Case. (Note that Figure 1-1, for illustrative purposes, shows only one assessment.)

When the development is complete (that is when the ESM activities have finished) a **Safety Case** is prepared. Endorsement of the Safety Case is required before **Safety Approval** can be given

After the safety approval, safety responsibility for the system may be transferred to a user, for example an infrastructure manager. There is an ongoing responsibility to manage safety during operation, through to, and including, decommissioning or disposal, but this is outside the scope of this book.

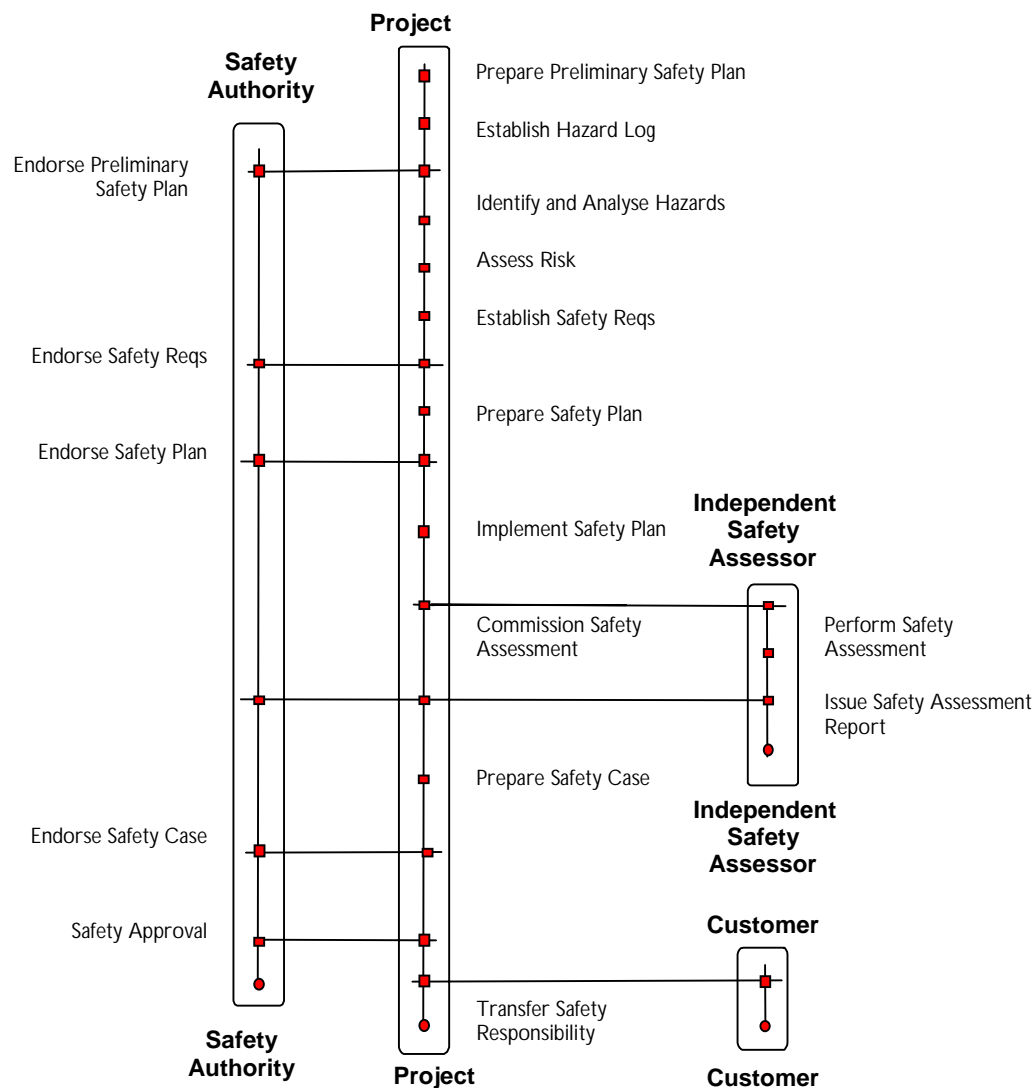


Figure 1-1 – Illustrative interactions between roles (Concept to Implementation Projects)

The ESM process described results in certain key safety deliverables which are listed below.

The **Preliminary Safety Plan** summarises the ESM activities to be carried out to derive and then meet the Safety Requirements. It evolves into a more detailed **Safety Plan**, which describes all the ESM activities that will be carried out to ensure risk is controlled, and justifies the approach taken.

The **Hazard Log** records details of all hazards and potential accidents identified during safety analyses of the project and logs all safety documentation produced by the project.

The **Risk Assessment Report** records the hazards identified and assesses the risks presented by the hazards.

The **Safety Requirements Specification** identifies the requirements to be met to ensure the system or equipment is safe.

The Independent Safety Auditor and Assessor produce **Safety Audit Reports** and **Safety Assessment Reports**, respectively, on completion of their work.

The **Safety Case** provides the evidence for the safety of the system or equipment developed by the project and draws on the safety records kept throughout the project.

**Safety Approval** is granted by the Safety Authority on the basis of endorsement of the Safety Case and other safety deliverables. A Safety Certificate may be issued to record the Safety Authority's approval of the system or equipment subject to the conditions on the certificate.

Table 1-1 provides a cross-reference into the rest of this volume which identifies where further guidance can be found on each of the activities and deliverables described above.

Activity	Deliverable	Chapters	Appendices
Establishment and maintenance of Hazard Log	Hazard Log	13	B, C
Preparation of Preliminary Safety Plan	Preliminary Safety Plan	11, 12	
Hazard Identification and Analysis	Risk Assessment Report	7, 8	B, C, E
Risk Assessment	Risk Assessment Report	7, 8	B, C, D, E
Establishment of Safety Requirements	Safety Requirements Specification	9	
Safety Planning	Safety Plan	11, 12	B, C, E
Independent Safety Audits and Assessments	Independent Safety Audit or Assessment Report	14	B, D
Preparation of Safety Case	Safety Case	10	
Safety Approval	Safety Certificate	10	
Transfer of Safety Responsibility	-	2	

**Table 1-1 – Where to find further guidance on activities and deliverables**

Table 1-2 lists the people that each chapter has been principally written for.

No	Chapter title	Intended readers
1	Introduction	All readers
2	Safety responsibilities	Managers Anyone assessing competence
3	Safety culture	Directors Managers
4	Competence and training	Managers Anyone assessing competence
5	Discharging responsibilities through suppliers	Managers Project Managers
6	Communicating and co-ordinating	Managers Project Managers Engineers
7	Defining changes	Project Managers Anyone performing or reviewing risk assessments
8	Identifying hazards and assessing and reducing risk	Anyone performing or reviewing risk assessments
9	Safety requirements	Anyone writing or reviewing Safety Requirements
10	Safety evidence and authorising change	Anyone writing or reviewing a Safety Case
11	ESM from start to finish	Anyone involved in project planning
12	Safety planning and good practice	Anyone writing or reviewing a Safety Plan Safety Auditors and Assessors
13	Configuration management, documentation and records	Project Managers Engineers
14	Independent professional review	Project Managers Safety Auditors and Assessors

**Table 1-2 – Who each chapter is written for**

## 1.4 Role activity diagrams

This section gives a brief introduction to role activity diagrams. The notation is described in full in '*Business Processes, Modelling and Analysis for Re-engineering and Improvement*' [F.1]

A role activity diagram presents a process in terms of *roles* and *activities*. It shows the relationship between roles and activities. For example, it is possible to identify that a role performs a particular activity. It is also possible to show activities that involve more than one role; such activities are called *interactions*. The order in which actions and interactions occur can be depicted.

Figure 1-1 shows a role activity diagram that models the Safety Lifecycle. This role activity diagram shows four roles: Safety Authority, Project, Safety Assessor and customer. The main role is the Project whose sequence of actions and interactions is shown in the middle column. The first action occurs at the top of the page and the last action at the bottom. Actions are shown as single boxes and interactions are shown as boxes connected by horizontal lines. The other three roles are secondary.

Figure 1-2 gives a key to the role activity diagram notation used in this document.

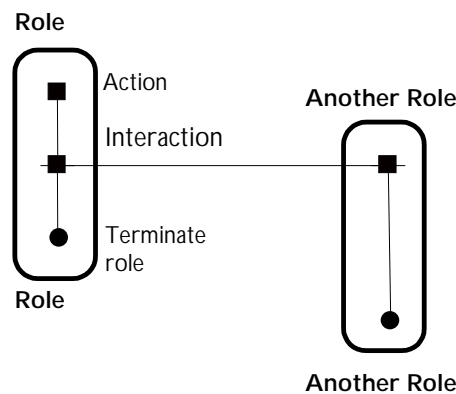


Figure 1-2 - Key to role activity diagram notation

## 1.5 How to use this volume

This volume can be used for reference. You can use the fundamentals of volume 1 or the tables above to find the chapter that you want.

Alternatively, the fundamentals and hence the chapters are laid out in a logical order so you may read a whole part, or even the whole volume in order.

This page left intentionally blank