

# 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:

<b>Concept and Feasibility</b>	All activities that precede the construction of a requirements specification for the system or equipment.
<b>Requirements Definition</b>	The construction of a requirements specification
<b>Design</b>	All activities that result in a design baseline for the system and equipment.
<b>Implementation</b>	All activities that are involved in realising the design before introducing any changes to the railway.
<b>Installation and Handover</b>	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.
<b>Operations and Maintenance</b>	All activities involved with the normal operation of the system or equipment.
<b>Decommissioning and Disposal</b>	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

**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.

<b>Generic lifecycle phase</b>	<b>Principal ESM Activities</b>	<b>See Chapter</b>
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