

Appendix B

Document Outlines

This appendix provides suggested document outlines for the following ESM documents:

- 1 Safety Plan (see chapter 12)
- 2 Hazard Log (see chapter 13)
- 3 Safety Assessment and Audit Remits (see chapter 14)
- 4 Safety Assessment and Audit Reports (see chapter 14)

The outlines do not show administrative document sections such as change history, terminology and referenced documents sections which should be added according to your own document standards.

B.1 Outline Safety Plan

The scope and coverage of this outline is designed to be consistent with the CENELEC standard prEN 50126 [F.8]. This is one of a group of European standards for safety within the rail industry. prEN 50126 defines a process for the management of Reliability, Availability, Maintainability, and Safety (RAMS). The letters in square brackets refer to the CENELEC requirement detailed in clause 6.2.3.4 of prEN 50126.

The recommended structure for the Safety Plan is as follows:

Introduction	Aims and objectives
	(describe the aims and objectives of this Safety Plan for readers unfamiliar with ESM or this project)
	Scope [b]
	(include the lifecycle phases this Safety Plan addresses)
	Structure
	(describe the structure of the plan)
	Background and requirements
	Summary of system [c, m]
	(include, or refer to, a description of the system, including interfaces to other related programmes)
	Outline of project [a]
(a brief description of the conduct of the project, to include a statement of compliance with the organisation's safety policy, or a justification of an alternative approach)	
Safety requirements [f]	
(a summary of the safety requirements or a reference to them and a description of the process by which the safety requirements were established and maintained; where none are available the Safety Plan should indicate how and when the Safety Requirements are to be determined)	
Risk assessment criteria [f]	
(a brief description of the criteria used to derive risk tolerability targets for the system)	
Assumptions and constraints [n]	
(list any assumptions or constraints on the system or the project)	

(cont.)

Safety management activities**Safety roles and responsibilities [d, f]**

(indicate and justify competence and independence of appointments)

- Project Manager;
- Project Safety Manager;
- Safety Assessor;
- Safety Auditor;
- Safety Authorities.

Safety lifecycle [e]

(describe and relate the project and safety lifecycles)

Safety analysis [f]

(describe and justify the approach, see chapter 8)

Safety deliverables [g]

(justify exclusion of key deliverables)

Safety standards

(justify use of Safety Standards on project)

Safety assessments [f, p]

(justify frequency of assessments)

Safety audits [f, p]

(justify frequency of audits)

Safety case and certification [h, i]

(describe certification requirements additional to those of ESM)

Contractor management [o]

(refer to contractor-produced plans and other documentation where appropriate)

Configuration management

(refer to technical and quality planning documentation where appropriate)

Safety training

(including contractors where appropriate)

System operation, modification and maintenance [j, k]

(briefly describe, or refer to, process and approval mechanisms for analysing operation, system modification, and performing system maintenance)

(cont.)

Safety controls [p]	(define controls, for instance formal review, approvers and standards for safety deliverables, including: <ul style="list-style-type: none">• Hazard Log• Hazard Analysis• Risk Assessment• Safety Req Spec• Safety Case
Safety docn. [f, l]	(describe production, approval and maintenance of each document; justify any not produced) <ul style="list-style-type: none">• Preliminary Hazard Analysis• Risk assessment report• Hazard Log• Safety Requirements Specification• Safety Audit and Safety Assessment Reports• Safety Case• Design and Test Specifications• Review reports• Testing and Acceptance records• Training records
Safety engineering [f]	(indicate activities to meet and validate Safety Requirements for each phase of the lifecycle)
Validation and verification of external items [f]	(justify a decision to not validate and verify any external items)

B.2 Outline Hazard Log

The scope and coverage of this outline is designed to be consistent with the CENELEC standard prEN 50126 [F.8]. The Hazard Log contains the following sections:

The recommended structure for the Hazard Log is as follows:

Introduction This section will describe the purpose of the Hazard Log and indicate the environment and safety requirements to which the system safety characteristics relate.

The following should be included:

- The aim, purpose and structure of the Hazard Log in sufficient detail to enable understanding by all project personnel;
- A unique identifier of the system to which the Hazard Log relates and a reference to a description and the scope of the system;
- A reference to the Safety Plan (in early stages of the project this will have to be omitted);
- A reference to the system Safety Requirements Specification or, if this has yet to be written, the safety analysis documentation;
- The process for managing the Hazard Log, such as who may modify it and the approval process for each new entry.

Journal The Journal should describe all amendments to the Hazard Log in order to provide a historical record of its compilation and provide traceability. It should record, for each amendment:

- The date of the amendment (not necessary if a diary format is used);
- A unique entry number;
- The person making the amendment;
- A description of the amendment and the rationale for it; and
- The sections in the Hazard Log that were changed.

If the Hazard Log is stored in a database then it may be possible to use the intrinsic change recording facilities to maintain a Journal semi-automatically.

(cont.)

Directory

The Directory, sometimes known as the Safety Records Log, should give an up-to-date reference to every safety document produced and used by the Project. The documents referred to should include (but not be limited to) the following, where they exist:

- Safety Plan;
- Safety Requirements Specification;
- Safety standards;
- Safety Documents;
- Incident/accident reports;
- Analyses, assessment and audit reports;
- Safety Case;
- Correspondence with the relevant Safety Authorities.

For each document the Directory should include the following:

- A unique reference;
- The document title;
- The current version number and issue date;
- The physical location of the master.

It may be convenient to keep the Directory separate from the rest of the Hazard Log, or event to integrate it with a project document management system.

(cont.)

Hazard data This section should record every identified hazard.

For each hazard, the information listed below should be recorded, as soon as it becomes available. Data collected during Hazard Analysis and Risk Assessment should be transcribed to the Hazard Log when the reports have been endorsed.

- a unique reference;
- a brief description of the hazard which should include the system functions or components affected and their states that represent the hazard;
- the causes identified for the hazard;
- a reference to the full description and analysis of the hazard;
- assumptions on which the analysis is based and limitations of the analysis;
- the severity for the related accident, the likelihood of the hazard occurring and the likelihood of an accident occurring with the hazard as a contributing factor;
- the predicted risk associated with the hazard;
- target likelihood for its occurrence;
- the status of the hazard; Typically one of the following:
 - Open (action to close the hazard has not been agreed);
 - Cancelled (the event has been determined not to be a hazard or to be wholly contained within another hazard);
 - Resolved (action to close the hazard has been agreed but not completed);
 - Closed (action to close the hazard has been completed);
- if the hazard is not closed or cancelled then the name of a person or company who is responsible for progressing it towards closure;
- a description of, or a reference to, the action to be taken to remove the hazard or reduce the risk from the system to an acceptable level; This should include:
 - a statement as to whether the hazard has been avoided or requires further action (with a justification if no further action is to be taken);
 - details of the risk reduction action to be taken;
 - a discussion of the alternative means of risk reduction and justification for actions considered but not taken;
 - a comment on the need for accident sequence re-evaluation following risk reduction actions;
 - a reference to any design documentation that would change as a result of the action;
 - a reference to all Safety Requirements associated with this hazard.

(cont.)

Incident data This section should be used to record all incidents that have occurred during the life of the system or equipment. It should identify the sequence of events linking each accident and the hazards that caused it. For each incident the following should be provided:

- a unique reference;
- a brief description of the incident;
- a reference to a report describing an investigation of the incident;
- a description of any action taken to prevent recurrence or justification of the decision not to take any.

Accident data This section should be used to record every identified possible accident. It should identify possible sequences of events linking identified accident with the hazards that may cause it. For each accident the following should be provided:

- a unique reference;
- a brief description of the potential accident;
- a reference to a report giving a full description and analysis of the accident sequence;
- a categorisation of the accident severity and the highest tolerable probability of the accident (the accident probability target);
- a list of the hazards and associated accident sequences that could cause the accident.

B.3 Outline Safety Audit and Assessment remits

The following structure is recommended for either an audit or an assessment remit.

Safety Auditor/Assessor	The name of the auditor/assessor.
Independence	Requirements for auditor/assessor independence.
Qualifications and Experience	Requirements for auditor/assessor qualifications and experience.
Requirements	Requirements for the audit/assessment itself, including <ul style="list-style-type: none">• the scope of the audit/assessment);• the purpose of the audit/assessment);• the documents that the project will be audited against, and the prevailing legal framework for accepting risk;• any previous assessments or audits which should be taken into account.
Other Information	As required.
Report to be issued by	Target date.
Commissioned by:	Name of person commissioning the audit/assessment.

B.4 Outline Safety Audit and Assessment reports

B.4.1 Outline Safety Audit report

The following structure is recommended for an audit report.

Summary	Management summary of rest of document.
Requirements	This section should state the audit requirements and identify any areas where the audit deviated from it.
Audit details	This section should provide details of the conduct of the Safety Audit, such as who was interviewed and what was examined.
Findings	<p>This section should list each finding and should discuss its impact. Evidence to support each finding should be given.</p> <p>Chapter 14 contains a suggested classification for findings.</p>
Conclusions and recommendations	<p>This section should include a judgement on the extent of the Project's compliance with the Safety Plan and a statement about the adequacy of the Safety Requirements. The degree of compliance may be graded as:</p> <ul style="list-style-type: none">• Unqualified compliance with the Safety Plan;• Compliance qualified by the need for implementation of minor recommendations that are based on each non-compliance of minor impact;• Non-compliance requiring implementation of major recommendations that are based on each non-compliance of major impact, followed by a subsequent Safety Audit.

This section may also provide a prioritised list of recommended actions for improvement to be carried out to resolve findings. The recommended actions should state who should do what, and by when. The recommendations may also include general suggestions for improvement beyond that required for compliance.

The completed audit checklist should be included as an appendix to the report.

The audit report should provide evidence to justify the Safety Auditor's findings and conclusions. The report should be dated and signed by the Safety Auditor.

B.4.2 Outline Safety Assessment report

The following structure is recommended for an assessment report.

Summary	Management summary of rest of document.
Requirements	This section should state the assessment requirements and identify any areas where the assessment deviated from it.
Assessment Details	This section should provide details of the conduct of the Safety Assessment, such as who was interviewed and what was examined.
Findings	This section should list each finding and should discuss its impact. Evidence to support each finding should be given. Chapter 14 contains a suggested classification for findings.
Conclusions and recommendations	This section should state the Safety Assessor's opinion as to the degree of compliance of the system or equipment with its Safety Requirements, in one of the following four forms: <ul style="list-style-type: none"> a) The Safety Assessor concludes that the system meets its safety requirements. b) The Safety Assessor concludes that the system will meet its safety requirements provided that specified recommendations are carried out and without a further assessment. c) The Safety Assessor cannot be sure that the system will meet its safety requirements. d) The Safety Assessor concludes that the system does not meet its safety requirements.

The Safety Assessor should state the reasons for the conclusions. The assessor should quantify the discrepancy between the safety requirements and the assurance achieved. A further assessment should be required before safety approval.

This section may also contain a numbered, prioritised list of proposed actions that should be carried out to resolve findings.

The assessment should give a professional judgement on the acceptability of the risk associated with the system or equipment.

The critical and most sensitive arguments of the document should be clearly and concisely highlighted and a professional opinion should be given as to the robustness of the argument. Where the argument is contained in whole or part within other documents or is part of existing custom and practice this should be clearly identified. A professional opinion should also be given, with regard to the railway system as a whole, as to the practicality of any measures used to mitigate against the hazards raised.

The assessment should identify any non-compliances with respect to the relevant standards and legal requirements.

This page left intentionally blank