

Chapter 10

Safety Evidence and Authorising Change

Your organisation must convince itself that risk associated with a change has been reduced to an acceptable level. It must support its arguments with objective evidence, including evidence that it has met all safety requirements.

No change can be authorised until all necessary safety approvals have been given.

10.1 Guidance from volume 1

10.1.1 Evidence of safety

You should normally put these arguments together in a safety case to show that:

- you have adequately assessed the risk;
- you have set adequate safety requirements and met them;
- you have carried out the safety plan; and
- all safety-related work has been done by people with the proper skills and experience.

If other people must take action before a change is safe, the safety case should describe these actions and show that the other people have accepted responsibility for carrying out these actions.

You may include relevant in-service experience and safety approvals as supporting evidence.

If you are working on signalling systems or equipment, CENELEC standard ENV 50129:1998, '*Railway Applications – Safety Related Electronic Systems for Signalling*' [F.13] is relevant. It places requirements on safety cases.

10.1.2 Safety approval

You must get safety approval from the necessary safety authorities. You will usually need approval from both the railway authority (such as Railtrack and London Underground Limited) and the regulatory authority (HMRI in the UK). Safety approval will normally be based on accepting the safety case.

The approving authority will normally produce a certificate, setting out any restrictions on how the work is used.

The approving authority will usually give safety approval at the end of a project, when the change is about to go into service. Some projects make staged changes to the railway in which case each stage will need safety approval. Large or complicated projects may need additional approval before they change the railway, for example for a safety plan or for safety requirements.

10.2 Background

The Safety Case is a document that provides an argument for the safety of a change to the railway. It provides assurance that risk has been reduced to an acceptable level to the project itself and to the Safety Authorities who will approve the change to the railway.

The main sources of evidence called up by the Safety Case are the records that have been kept and the checks that have been made by independent engineers.

The Safety Case can also be presented as an incremental document which will include ESM data as it becomes available.

The Safety Case required by ESM is an *engineering* Safety Case and should not be confused with the railway safety case which the '*Railways (Safety Case) Regulations 1994*' require all train and station operators to produce. The two are linked however: an operator's railway safety case may rely in part on the engineering safety cases for the operator's major systems.

The Safety Case provides much of the evidence for safety that the Safety Authority requires in order to grant safety approval for the change to proceed.

Note that the phrase 'safety approval' is used by some people to describe a process during which the safety authority accepts liability for the railway change. The phrase 'safety acceptance' is used to describe an endorsement without acceptance of liability. In this volume 'safety approval' is used to describe any process by which a Safety Authority grants its approval for a proposed change to the railway to proceed, regardless of the implications for legal liability.

This chapter is written for:

- anyone preparing a Safety Case, and
- anyone reviewing a Safety Case.

10.3 Application

The size of the Safety Case will depend on the risks and complexity of the project. For example, the Safety Case for a simple and low-risk project should be a concise document with brief arguments justifying that the risk is acceptable. A Safety Case for a high-risk or complex project will require a comprehensive Safety Case with comprehensive safety arguments.

10.4 Responsibilities

The Project Manager is responsible for ensuring that a Safety Case is prepared, maintained, and submitted to the Safety Authorities. He may delegate the preparation to a Project Safety Manager but should retain overall responsibility.

The relevant Safety Authorities are responsible for endorsing the Safety Case.

10.5 Submission

The Safety Case should be submitted to the relevant Safety Authorities for endorsement.

In the UK, the Safety Case may need to be submitted to HMRI as part of type approval as required by the '*Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations 1994*'.

Interim versions of the Safety Case may be submitted as the project proceeds. For instance, for the introduction of rolling stock onto the Railtrack railway network it is usual to make safety submissions after design, before track test, before interim operations and before full fleet operation.

The points at which versions of the Safety Case will be submitted should be agreed with the Safety Authorities and documented in the Safety Plan.

A complete version of the Safety Case should be submitted and endorsed before any change is introduced to the railway. If the project is making staged changes then several versions may need to be submitted and endorsed, each covering one or more stages.

The Safety Case should be modified during operation if the system is changed or if further safety-related information is obtained.

Note: The Safety Case forms part of the evidence of safety, submitted to the Safety Authority. It will typically be accompanied by other documents, including an Independent Safety Assessor's report. Also, other ESM documents such as the Safety Plan and Safety Requirements Specification may have been submitted for endorsement beforehand. The Safety Authority's review of these documents can constitute a Safety Review in the terminology used by prEN 50126 [F.8].

10.6 General guidance

The Safety Case should demonstrate that the system complies with its Safety Requirements and that risk has been reduced to an acceptable level.

The Safety Case should identify and justify any unresolved hazards and any non-conformances with the Safety Requirements Specification and Safety Plan.

The Safety Case should consider safety relating to the entire system as it consists of a combination of hardware, software, procedures and people interacting to achieve the defined objective.

The Safety Case should present information at a high-level and reference detail in other project documentation, such as the Hazard Log. Any referenced documentation should be uniquely identified and traceable. References should be accurate and comprehensive.

The Safety Case should present or reference evidence to support its reasoning. Evidence may come from many sources, although the Safety Case is likely to depend heavily on entries in the Hazard Log and the results of Safety Assessments and Safety Audits.

The Safety Case should accurately reflect information obtained from other project documentation.

Although the Safety Case is primarily used to satisfy the project and Safety Authorities of the safety of the system or equipment, the Safety Case may have a wider readership, including Safety Auditors and Assessors, and this should be taken into account when preparing the Safety Case.

10.7 CENELEC standard ENV 50129:1998

This pre-standard defines the conditions which should be met to accept a safety-related electronic railway signalling system.

The principal normative contents of the standard are:

- requirements on Safety Case structure and content (clauses 5.1 through 5.4 and appendix B);
- requirements on safety acceptance and approval (including types of safety cases) (clause 5.5);
- requirements on the establishment of Safety Integrity Levels (appendix A); and
- requirements on the identification of hardware component failure modes (appendix C).

Note though that this standard is not intended to provide comprehensive guidance on writing a Safety Case. It provides a structured framework for demonstrating safety but requires interpretation to deliver a convincing demonstration of safety for a railway change.

Volume 2 of the Yellow Book in general, and this chapter in particular, have been written to allow the reader to comply with ENV 50129:1998 [F.13] while following the guidance provided, and to help with interpreting this standard effectively.

10.8 Types of Safety Case

Three different types of Safety Case can be considered, see ENV 50129:1998 [F.13]

- A *generic product Safety Case* provides evidence that a generic product is safe in a variety of applications.
- A *generic application Safety Case* provides evidence that a generic product is safe in a specific class of applications.
- A *specific application Safety Case* is relevant to one specific application.

These may be used to allow efficient re-use of safety evidence. For instance a specific application Safety Case for a resignalling scheme may refer to a generic application Safety Case for the use of a points machine in a particular type of junction which may in turn refer to a generic product Safety Case for that points machine.

NB ENV 50129:1998 [F.13] requires that a specific application Safety Case be split into two Safety Cases: *application design* and *physical implementation*. This publication however does not recommend splitting the Safety Case in that way for all applications.

10.9 Content of the Safety Case

The structure described in Figure 10-1, which is consistent with ENV 50129:1998 [F.13], is recommended for a Safety Case.

Alternative structures may be appropriate in some cases but they should cover the same topics as this structure.

Note though that above all, a Safety Case should deliver a convincing and comprehensive argument for safety. This cannot be provided just by complying with any given structure but should arise from an effective programme of ESM activities.

1. **Executive Summary**
2. **Introduction**
3. **Definition of System**
4. **Quality Management Report**
5. **Safety Management Report**
 - Introduction
 - Roles and responsibilities
 - Safety lifecycle
 - Safety analysis
 - Safety requirements
 - Safety standards
 - Safety audit and assessment
 - Supplier management
 - Safety controls
 - Configuration management
 - Project safety training
6. **Technical Safety Report**
 - Introduction
 - Assurance of correct functional operation
 - Effects of faults
 - Operation with external influences
 - Safety-related application conditions
 - Safety qualification tests
 - Other outstanding safety issues
7. **Related Safety Cases**
8. **Conclusion**

Figure 10-1 – Recommended Safety Case Structure

While this section provides a framework for *structuring* the Safety Case, the ESM activities should drive the *content* – any activity which was necessary to achieve acceptable risk should contribute some content to the Safety Case.

10.10 Safety Case: Executive summary

The executive summary should summarise the key information contained in the Safety Case. It should contain the following:

- a brief description of the change, its purpose, functionality and location;
- a summary of the safety design and development process undertaken;
- a summary of the assessment and audit processes undertaken;
- a summary of the test and operational experience; and
- a summary of the current safety status in terms of evidence obtained and unresolved hazards.

10.11 Safety Case: Introduction

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

10.12 Safety Case: Definition of system

This section should provide an overview of the change in order to provide an understanding of the safety issues raised. It should cover, or reference, documentation dealing with the purpose, functionality, architecture, design, operation and support of items under review.

It should include:

- a description of the system including its physical location;
- definition of system boundaries and interfaces, including assumptions about other systems, services and facilities; and
- identification of constituent sub-systems, and if appropriate, a reference to sub-systems' Safety Cases.

The configuration of the system to which the Safety Case applies should be explicitly identified. This section should demonstrate that the system is subject to effective configuration management and change control, referring to any standards called up in the Safety Plan.

10.13 Safety Case: Quality management report

A pre-requisite for an effective Safety Case is that the quality of the work is and has been, controlled by an effective quality management system (QMS). This section should summarise the QMS activities and justify their appropriateness to the project. Large volumes of detailed evidence and supporting documentation need not be included provided precise references are given to a description of the relevant QMS.

10.14 Safety Case: Safety management report

10.14.1 Introduction

This section should describe and discuss how ESM aspects of the project were carried out. It should summarise and refer to the activities described in the Safety Plan and provide or refer to evidence to show that the activities were carried out as planned and justify that these activities proved to be appropriate and adequate.

The Hazard Log will be the primary source of evidence that hazards have been controlled.

The following ESM issues should be addressed:

- Roles and responsibilities;
- Safety lifecycle;
- Safety analysis
- Safety requirements;
- Safety standards;
- Safety audit and assessment;
- Supplier management;
- Safety controls;
- Configuration management; and
- Project safety training.

Each issue is treated in a separate section, below.

10.14.2 Roles and responsibilities

This section should provide evidence to show that the key safety personnel on the project carried out the roles defined in the Safety Plan.

It should justify the appointment of the key safety personnel by referring to competence and experience.

10.14.3 Safety lifecycle

This section should justify the project and safety lifecycles followed during the project, particularly if they differed significantly from those defined in the Safety Plan.

10.14.4 Safety analysis

This section should present a detailed discussion of the safety analysis process used on project. It should provide assurance that all foreseeable hazards have been identified, that intolerable risks have been eliminated and that other risks have been reduced ALARP.

This section should show that the safety analyses have taken into account the scope of the system and its normal and abnormal operation. System and component failure and malfunction, procedural failures, human error and environmental conditions should be considered.

The following should be provided:

- A list of the analysis methods used and their application on the project.
- Identification of the design documents referenced during the analysis work, clearly indicating the configuration and status of the design for each analysis.
- Evidence that the safety analysis process is capable of addressing the safety of future system changes.

This section should review all the incidents that have occurred. It should state the cause, potential and actual effects, and the actions required to prevent the re-occurrence of all incidents that have occurred during operational experience which could have compromised safety during operation in-service. The review should refer to the Hazard Log.

This section should also present a review of reliability data based on data obtained from operating experience, including the Hazard Log. The data should be used to quantify and justify the safety analysis evidence.

This section should discuss the approach used to demonstrate that risk has been reduced ALARP and demonstrate that the approach follows good practice.

This section should record any elements of the safety policy set by the railway authority which are relevant to the analysis. These may include safety targets set by the railway authority and latitude allowed to their contractors and suppliers to change aspects of the railway environment in which the system or equipment will run.

10.14.5 Safety requirements

This section may either restate the safety requirements for the system or equipment or summarise them and refer to the Safety Requirements Specification.

A discussion of the safety implications of the requirements, indicating how each requirement affected the project, should be included.

Any assumptions made should be stated and justified.

Evidence for compliance with the Safety Requirements is addressed in section 10.15.3 below.

10.14.6 Safety standards

This section should provide evidence that the procedures and standards called up by the Safety Plan were followed, and justify any non-conformances.

10.14.7 Safety audits and safety assessments

Evidence for the implementation of the Safety Audit and Assessment programme is a key element of the Safety Case. The findings of these audits and assessments are normally presented in separate documents. This section should present the following:

- a description and justification of timing of the audits and assessments should be described;
- a justification that the auditors and assessors had sufficient competence and independence;
- a justification of any decision not to take action in response to a finding or recommendation.

10.14.8 Supplier management

This section should show that the work of contractors and suppliers has been carried out to the safety standards expected for the SIL applicable, and as specified in the supplier's Safety Plan.

10.14.9 Safety controls

This section should provide evidence that the safety controls identified in the Safety Plan have been applied.

10.14.10 Configuration management

This section should justify the configuration management system employed and show that it has been implemented correctly.

Evidence that all safety-related project items are under configuration management should be provided.

10.14.11 Project safety training

This section should show that the personnel carrying out the safety-related activities were adequately trained by providing evidence for the implementation of defined training plans.

10.15 Safety Case: Technical safety report

The Technical Safety Report should explain the technical principles which assure the safety of the design including (or giving references to) all supporting evidence (for example, design principles and calculations, test specifications and results, and safety analyses). Large volumes of detailed evidence and supporting documentation need not be included, provided precise references are given to such documents. The following gives a guideline for the structure of the Technical Safety Report,

- 1 Introduction;
- 2 Assurance of correct functional operation;
- 3 Effects of faults;
- 4 Operation with external influences;
- 5 Safety-related application conditions;
- 6 Safety qualification tests;
- 7 Other outstanding safety issues.

Items 2 to 7 inclusive are each treated in the sections below.

10.15.1 Assurance of correct functional operation, effects of faults, operation with external influences

These three sections should describe and discuss the activities carried out in each phase of the project in order to satisfy the Safety Requirements. They should summarise and refer to the activities described in the Safety Plan and provide or refer to evidence to show that the activities were carried out and that these activities proved to be appropriate and adequate for the defined SIL.

These activities should be provided under three headings:

- **Assurance of correct functional operation**

Demonstrating that the system will contribute acceptable risk in the absence of faults and external influences. Routine maintenance should be considered as well as normal operation.

- **Effects of faults**

Demonstrating that the system will contribute acceptable risk in the presence of foreseeable internal faults. Relevant safety features, fall-back modes and alternative operating procedures should be described.

- **Operation with external influences**

Demonstrating that the system will contribute acceptable risk in the presence of foreseeable external influences, such as weather, electromagnetic interference and vandalism, Relevant safety features, fall-back modes and alternative operating procedures should be described.

The Hazard Log should be used as the primary source of evidence.

These sections should show that the approach adopted reduced risk ALARP.

These sections should show that the Safety Requirements have been met. They should include the following, where relevant:

- a) Evidence that the Safety Requirements were defined according to good practice (see chapter 12);
- b) Identification and justification of major changes made to the Safety Requirements throughout the project;
- c) A summary and reference to all analyses carried out during requirements definition;
- d) Evidence that high-level allocation of safety requirements to sub-systems has been carried out;
- e) An explanation and justification of all use of sub-systems, pre-fabricated sections, dependencies on other systems and so on, which have been produced outside the direct control of the project;
- f) Safety evidence acquired from verification and validation of the system summarised, including the strategy and method employed and the results and evidence obtained;
- g) Evidence that further work or improvements identified as a result of validation and verification activities have been carried out;
- h) Evidence that the system has been integrated with existing systems and procedures in a safe and controlled manner;
- i) Evidence that commissioning activities have been examined for commissioning-specific hazards;
- j) Evidence that, for systems with extensive or complex hardware, software or human-factors considerations, a formal hazard identification and analysis activity has been carried out;
- k) Practical experience of operating the system, including testing, integration, commissioning and any in-service experience summarised;
- l) Evidence that the hazards associated with system operation will be adequately controlled under both normal and abnormal conditions and for all modes of operation;
- m) Evidence that all aspects effecting safe operation and maintenance, including staffing levels, training requirements, operational management and interfaces to other systems, have been addressed;
- n) Evidence that response time requirements and other analogue issues, such as non-overlapping tolerances have been considered.

10.15.2 Safety-related application conditions

This section should specify (or reference) the rules, conditions and constraints which should be observed in the application of the system. This should include the application conditions contained in the Safety Case of any related sub-system or item of equipment.

10.15.3 Safety qualification tests

This section should provide evidence of test activities which demonstrate that each Safety Requirement has been met.

If this evidence is not available or sufficient, this section should present analytical evidence that each Safety Requirement has been met, or adequately justify any that have not been met. Such a justification should include an assessment of the residual risk presented by the non-compliance.

This section should review the fault history and status of the system or equipment as recorded in the Data Recording And Corrective Action System (DRACAS) and justify the conclusion that risk has been reduced to an acceptable level in the light of this evidence.

10.15.4 Other outstanding safety issues

All outstanding safety issues not covered by documented Safety Requirements should be discussed here, whenever they would have a bearing on operational safety.

10.16 Safety Case: Related safety cases

This section should contain references to any other Safety Cases upon which this Safety Case depends, together with a demonstration that any assumptions, limitations or restrictions in the related Safety Cases are either fulfilled or carried forward into this Safety Case.

10.17 Safety Case: Conclusion

This section should make a statement on the acceptability of the system in terms of the safety requirements. This statement should include:

- a list of assumptions made in the safety case especially those made about the safety requirements;
- a statement of the residual risk presented by the system;
- a statement of system deficiencies;
- identification of all unresolved hazards and other outstanding issues;
- operating restrictions or procedures imposed for safety reasons; and
- recommendations for or identification of further work to be carried out.

The conclusions section should document any caveats on which the conclusion is based including assumptions and limitations and restrictions on use. The Safety Authority may carry these forward as conditions of safety approval.

10.18 Related guidance

Chapter 12 provides guidance on establishing safety requirements.

This page left intentionally blank