iESM
BROUGHT TO YOU BY ARC

international Engineering Safety Management

GOOD PRACTICE HANDBOOK

VOLUME 2
METHODS, TOOLS AND TECHNIQUES FOR PROJECTS

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.4 May 2022

arc

iESM
VOLUME 2

CONTENTS

Issue 1.4
© Abbott Risk Consulting Ltd. 2022

© Abbott Risk Consulting Ltd. 2022

© Abbott Risk Consulting Ltd. 2022

© Abbott Risk Consulting Ltd. 2022

© Abbott Risk Consulting Ltd. 2022

DISCLAIMER

Abbott Risk Consulting Limited (ARC) and the other organizations and individuals involved in preparing this handbook have taken trouble to make sure that the handbook is accurate and useful, but it is only a guide. We do not give any form of guarantee that following the guidance in this handbook will be enough to ensure safety. We will not be liable to pay compensation to anyone who uses this handbook.

ACKNOWLEDGEMENTS

This handbook and its updates have been written with help from the people listed below:

- D Beacham
- Dr G Bearfield
- S Bickley
- D Bonvoisin
- N Bowley
- M Castles
- P Cheeseman
- Dr K Chan
- J-M Cloarec
- Dr Chen Roger Lei
- Dr R Davis
- Dr B Elliott
- E Fan
- S Hughes
- Dr KM Leung
- C Lowe
- Dr I Lucic
- J McDonald
- G Newman
- Niu Yingming
- Ng Nelson Wai Hung
- G Parris
- M Roome
- A Russo
- J Shaw
- Shi Lisa
- G Topham
- Tse Shirley Lai
- Dr Fei Yan
- Liu Weiqing
- LC Wong
- Dr Zhang Simon

These people worked for the organizations listed below:

- Abbott Risk Consulting
- Arbutus Technical Consulting
- Beijing Metro Construction Corporation
- Beijing National Railway Research and Design Institute of Signal and Communication Co. Ltd.
- Beijing Traffic Control Technology Company
- Bombardier Transportation
- Certifer
- China Academy of Railway Sciences
- Crossrail
- EC Harris (now Arcadis)
- Electrical and Mechanical Services Department, Hong Kong Government
- Jacobs
- Liv Systems
- Lloyd's Register
- London Underground
- MTR Corporation, Hong Kong
- Orient Systems Assurance
- RATP
- Ricardo Rail
- Rio Tinto
- RSSB, UK
- SNC-Lavalin
- Sydney Trains
- Systra
- Technical Programme Delivery Group

This handbook does not necessarily represent the opinion of any of these people or organizations.

© Abbott Risk Consulting Ltd. 2022

Good practice in engineering safety management advances as people build on the work done before by others.

This handbook has drawn on the work carried out by the contributors to the Yellow Book [YB4] and to guidance on European Common Safety Methods [CSM-RA] among others and we acknowledge our debt to them.

© Abbott Risk Consulting Ltd. 2022

Part I: Introductory Material

© Abbott Risk Consulting Ltd. 2022

1 INTRODUCTION

1.1 Purpose and scope of this volume

This handbook (the international Engineering Safety Management Good Practice Handbook, or 'iESM' , for short) describes good practice in railway Engineering Safety Management (ESM) on projects. This volume covers both projects that build new railways and projects that change existing railways.

ESM is the process of making sure that the risk associated with work on the railway is controlled to an acceptable level. ESM is not just for engineers and can be used for work that involves more than just engineering. ESM, and this handbook, are however scoped to controlling safety risk, that is the risk of harming people, rather than the risk of environmental or commercial damage. Some of the techniques described in this handbook may be useful for controlling these other sorts of risk but we only claim that they represent good practice for controlling safety risk.

The techniques are primarily concerned with **railway safety**, that is, making sure that the work you do does not introduce problems onto the railway that later give rise to accidents.

You must, of course, also take steps to ensure **occupational health and safety**, that is, the health and safety of the people involved with the work itself. We recommend that you co-ordinate the activities that you carry out to ensure railway safety and occupational health and safety. We only claim that the techniques described in this handbook represent good practice for controlling railway safety risk. If you intend to adapt the iESM guidance to help ensure occupational health and safety then you should make sure that you are familiar with good practice and legislation in that field first.

This handbook does not provide a complete framework for making decisions about railway work. It is concerned with safety and does not consider non-safety benefits. Even as regards safety, this handbook 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 organization's values and those of society at large and for demonstrating that this is the case.

1.2 How the iESM Guidance is written

The iESM Guidance is structured in three layers:

- Layer 1: Principles and process
- Layer 2: Methods, tools and techniques (this volume)
- Layer 3: Specialized guidance

The first layer comprises one volume, Volume 1. Volume 1 describes some of the safety obligations on people involved in changing the railway or developing new railway products. It also describes a generic ESM process designed to help discharge these obligations.

This volume, Volume 2, provides guidance on implementing the generic ESM process presented in Volume 1 on projects. Volume 2 belongs in the second layer. A separate Volume 2 has been written for those maintaining the railway.

The third layer comprises a number of Application Notes providing guidance in specialized areas, guidance specific to geographical regions and case studies illustrating the practical application of the guidance in this handbook.

The structure of the iESM Guidance is illustrated Figure 1-1 below.

© Abbott Risk Consulting Ltd. 2022

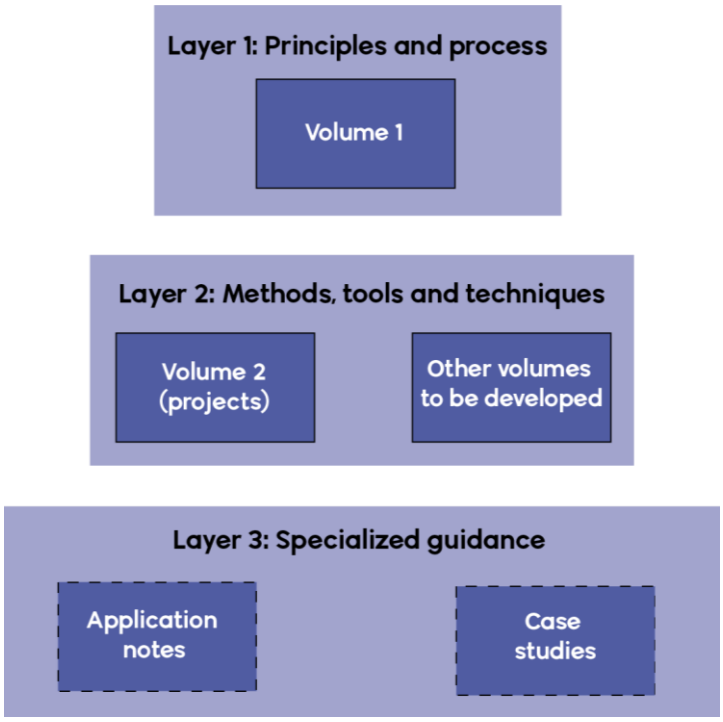


Figure 1-1: The Structure of the iESM Guidance

In this chapter and the following two, we introduce some concepts, we summarize the generic ESM process which was described in volume 1 and then we introduce a System Lifecycle and present high-level guidance on what ESM activities you should carry out in each phase of this lifecycle.

More detailed guidance is then presented in a series of chapters, where each chapter deals with an activity from the generic ESM process. These chapters of volume 2 are in the same order as the corresponding sections of volume 1. The activities in volume 1 are arranged under five headings:

- Definition
- Risk analysis
- Risk control
- Technical support
- Team support

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

The chapters refer to each other and these cross-references are summarized in 'Sources of further guidance' sections at the end of each chapter.

© Abbott Risk Consulting Ltd. 2022

Color coding is provided in these parts in order to assist the reader, as follows:

Principles reproduced from volume 1 are shown in a blue table like this.

High-level guidance from volume 1 on the application of these principles is shown below the principles.

a. Checklist items to consider when implementing the principles are shown in a pink table like this.

Detailed guidance on the application of these checklist items is shown under the items. Many of the checklist items start with a clause of the form, "If you *are doing something"*. You can use this to find the guidance which is relevant to you. If you (or your organization) are not doing what the introductory clause refers to, then the guidance may be inapplicable to you.

A similar layout is used in chapter 3 to organize guidance on the execution of specific ESM activities at different phases of the system lifecycle.

If the version of this handbook that you are reading is printed in black and white, please do not worry – the color coding is provided to make it easier to use this handbook but you do not need to see the colors to use it.

Supporting material is supplied in a final part, including:

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

Specialist terms are printed in bold when introduced (but note that bold text is also used to highlight key words in lists). All of these are defined in a glossary in chapter 24.

There is a list of referenced documents in chapter 25 and references are indicated in the text with annotations of the form '[50126]'.

1.3 How to use this volume

You can use the guidance in this volume directly to guide your work. Alternatively you can use it to help you write, review or improve your organization's procedures for carrying out its work. If you do the latter then you would expect the people doing the work to refer to your organization's procedures in the normal course of business and only refer to this volume if these procedures do not fully cover their situation.

Volume 1 of this handbook contains a generic ESM process and one or more principles for each activity in this process. There is broad consensus that any effective ESM approach will put these principles into practice. If you have not already checked your organization's processes against the principles of volume 1, you will almost certainly find it worthwhile to do that first – it will help you identify the activities where further guidance would be valuable.

© Abbott Risk Consulting Ltd. 2022

None of the content of this volume should be regarded as prescriptive – there are other effective ways of carrying out the activities – but the guidance is representative of good practice.

Before applying the guidance, it will help:

- To be clear which phases of the system lifecycle your organization is working in. Some of the guidance is specific to particular phases and this may help you to identify what is relevant to you. The generic System Lifecycle described in section 3.1 describes the phases that are used in this handbook.
- To have made an initial assessment of the risk, novelty and complexity associated with your work. If you are carrying out low-risk, routine and simple work, you may be able to rely largely on following standards and procedures to control the risk associated with this work. If your work is higher-risk, novel or complex, then you may need to use more elaborate analytical methods to control the risk

The precise program of ESM activities that you carry out will need to be tailored to your specific circumstances. Chapter 3 provides some advice on the ordering and timing of activities which you can use to construct such a program.

Do bear in mind though that there are important aspects of ESM that do not fit easily into such a program. Promoting a good safety culture for example is not something that can be associated with a stage in the System Lifecycle. It cuts across the lifecycle and it is something that requires continuous attention.

1.4 Comments and suggestions

If you have any comments on this handbook or suggestions for improving it, we should be glad to hear from you. You will find our contact details on our web site, www.intesm.org. This web site contains the most up-to-date version of this handbook. We intend to revise the handbook periodically and your comments and suggestions will help us to make the handbook more useful for all readers.

© Abbott Risk Consulting Ltd. 2022

2 CONCEPTS AND TERMINOLOGY

We explain some concepts and terminology that we use throughout this volume.

2.1 Accidents and risk

When working to prevent accidents, it helps to have an understanding of potential **accident sequences**, the progression of events that result in accidents. Figure 2-1 represents an accident sequence.

An **accident** is an unintended event or series of events that results in harm.

A **hazard** is a condition that could lead to an accident. Not all hazards result in accidents because it may be necessary for some other hazard or triggering event occur, or for some 'barrier', that is a mechanism created to protect against hazards, to fail, or both.

We define a **causal factor** to be any condition or event which might contribute to a hazard.

Casual factors can include **failures**, that is, occasions when a system, product or component is unable to fulfill its operational requirements.

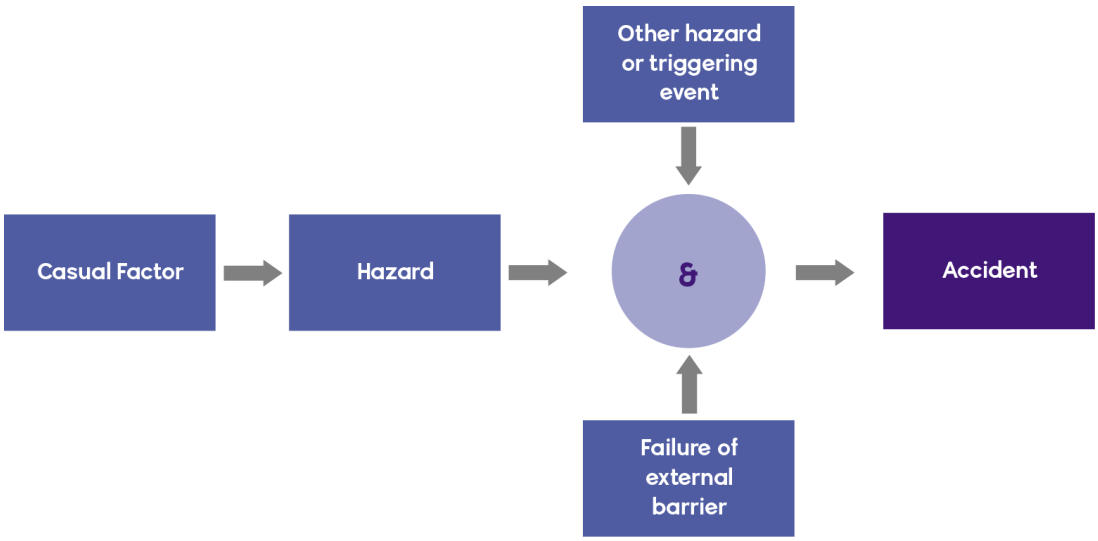


Figure 2-1: An Accident Sequence

Not all hazards give rise to accidents: there may be **barriers** in place which are designed to stop the sequence of events before an accident occurs. But no barriers are perfect and an accident may result despite them.

It may also be necessary for other events to occur before a hazard will give rise to an accident. Some of these events may be hazards of other systems but this does not have to be the case and we use the phrase **triggering event** to describe these in general.

Fault-tolerant mechanisms may mean that more than one failure is required before a hazard occurs. Similarly, hazards may not result in accidents due to the action of mitigating features.

© Abbott Risk Consulting Ltd. 2022

Failures may be classified into two types:

- **Random.** Failures resulting from random causes such as variations in materials, manufacturing processes or environmental stresses. These failures occur at predictable rates, but at unpredictable (that is random) times. The failure of a light bulb is an example of a random failure.
- **Systematic.** Failures resulting from a latent fault which are triggered by a certain combination of circumstances. Systematic failures can only be eliminated by removing the fault. Software bugs are examples of systematic failures.

There are well-established techniques for assessing and controlling the risk arising from random failures. The risk arising from systematic failures is controlled in many engineering activities through rigorous checking. The risk arising from both sorts of failure is also often controlled through the application of mandatory or voluntary standards, codes and accepted good practice.

However as the complexity of designs increases, systematic failures contribute a larger proportion of the risk. For software, all failures are systematic. In software and some other areas where designs may be particularly complex, such as electronic design, current best practice is to make use of **Safety Integrity Levels (SILs)** to control systematic failures. SILs are discussed further in section 9.2.4.

Even in complex systems and products, SILs are not the only means of controlling systematic failures; they may be controlled through architectural design features as well**.**

We will use the word **'risk'** to mean the combination of the likelihood of occurrence of harm and the severity of that harm.

© Abbott Risk Consulting Ltd. 2022

2.2 Systems and products

A railway is a **system**, that is, a collection of equipment, people and procedures which are intended to work together to accomplish some function. There are smaller systems within railways. These include signaling systems, stations, depots and trains. A system does not have to have electricity running through it – the track may be regarded as a system, for example.

The concept of a system provides a very useful focus to safety work and can also support some clearer vocabulary.

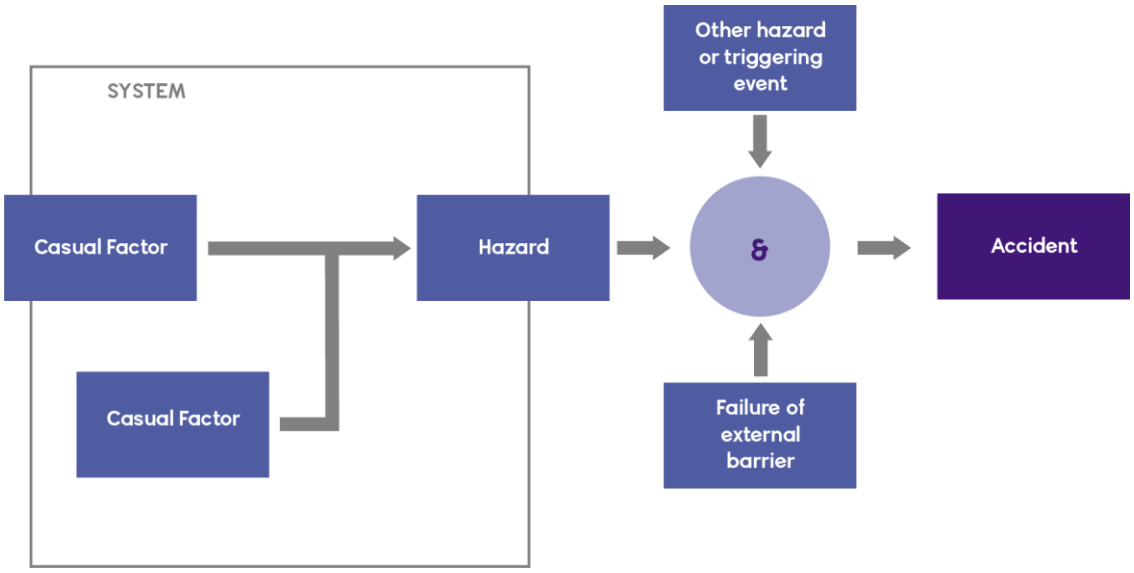


Figure 2-2: Systems, Hazards and Causal Factors

As Figure 2-2 illustrates, once we have defined a system, then we can say that a hazard *of that system* is a state *of that system* which can contribute to an accident. By drawing the hazard on the boundary of the system, we indicate that the hazard occurs at the point where the accident sequence ceases to occur within the system. If you are changing the railway then you should scope the system you consider to represent the extent of your responsibility. With that definition, the hazard is the point at which you cease to be able to affect the course of events.

A new railway can be regarded as a system and the final output of a project which changes the railway will be the system that contains all the changed parts. However some projects develop generic **products** which will be applied by later projects to create new systems.

We refer to both systems and products throughout this handbook. A product can become a system or a part of a system but first it must be applied**,** that is installed at one or more places on a railway and, often, configured for this application.

Once it is applied then the product may be considered as a system and we can identify its hazards and the accidents which they may lead to. These hazards and accidents may vary from application to application and so can only be definitively established for a **specific application**.

© Abbott Risk Consulting Ltd. 2022

However, by making assumptions about the operational environment in which their product will be applied, the product supplier can identify the hazards which are likely to be associated with the product and design the product to control them. The product supplier may do this for all applications of the product but sometimes more progress can be made by dividing these applications into classes (for instance electrified and non-electrified railways) and considering them separately. We describe the former as work to ensure the safety of the **generic product** and the latter as work to ensure the safety of a **generic application** of the product

To ensure that a specific application of a product is safe, it will always be necessary to consider the specific circumstances of this application – if only to confirm that the assumptions made in previous work hold in this application. However if thorough work has been done to ensure the safety of the generic product or a relevant generic application of the product, the additional work to confirm the safety of the specific application may be reduced.

2.3 A generic engineering safety management process

In volume 1 of this handbook, we presented a generic ESM process which contains the most important ESM activities and the most important flows of information between them. That generic process is repeated in Figure 2-3, below. The activities are represented by rectangles which are collected in five groups.

The most important flows of information between activities are indicated by arrows but there are other flows of information which are not shown. An arrow from activity A to activity B does not imply that A must finish before B can start – on the contrary it is usual for the activities to be repeated as new information comes to light.

The activities in the central boxes represent the main flow of the ESM process while the activities in the boxes on either side represent supporting activities that are performed throughout the durations of the activities in the central boxes.

© Abbott Risk Consulting Ltd. 2022

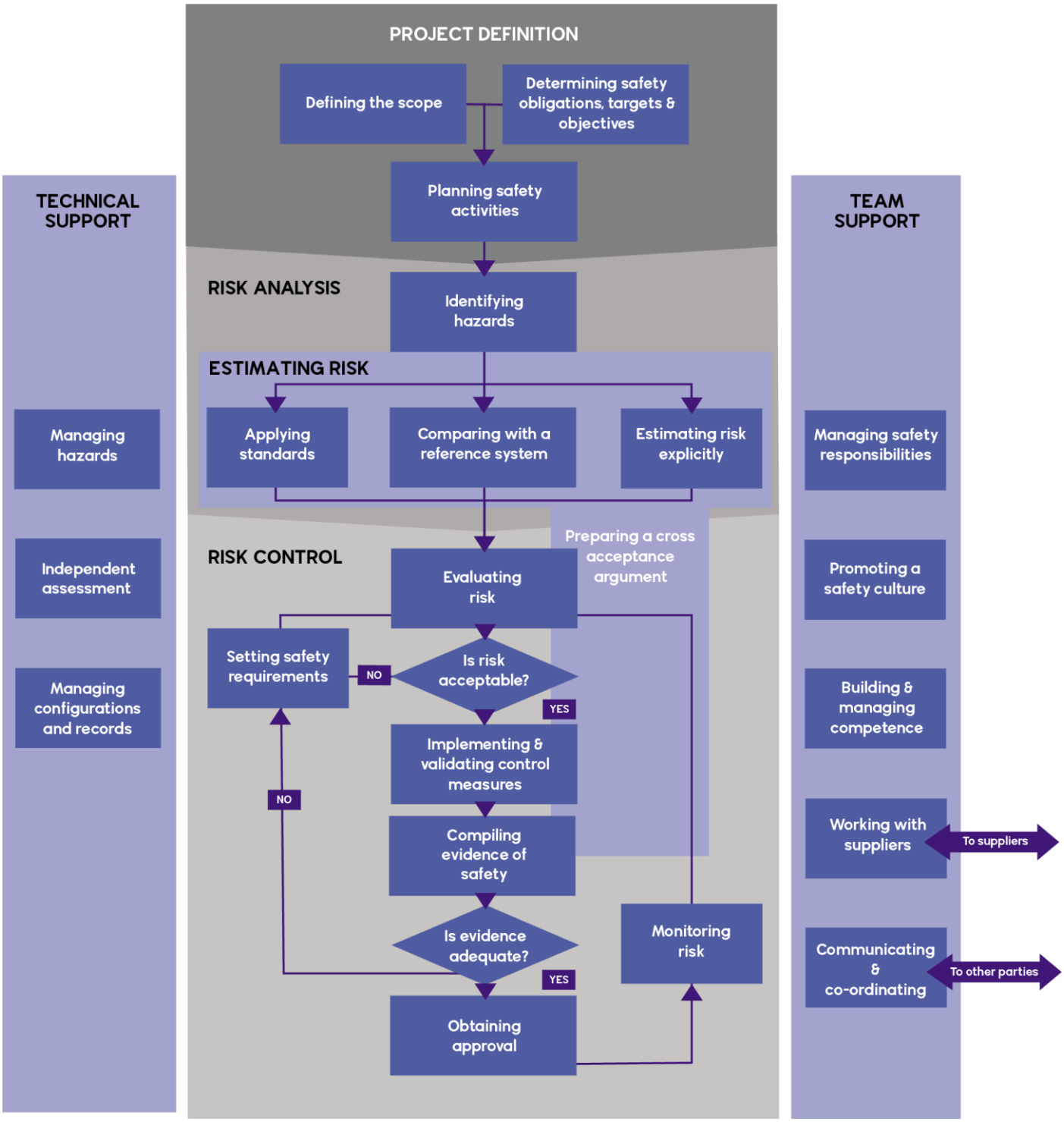


Figure 2-3: A Generic Process for ESM

© Abbott Risk Consulting Ltd. 2022

2.4 Taking decisions about safety

ESM contributes to increased safety by supporting better decisions about the system being built or the work being done – decisions which decrease risk compared with the alternatives.

Before a decision on whether risk is acceptable is made, you will have to establish relevant facts about the system or product being delivered, its users and its operational environment and to use these to assess the risk associated with the system or product. After the decision is made, you will have to confirm that the measures agreed upon to control risk are fully implemented and effective. Figure 2-4 illustrates these different activities, showing that decisions must be taken at several points in the project.

Figure 2-4: Decision Making

2.5 Obtaining approvals

Before a new system is brought into service, someone should review the evidence that risk has been controlled and decide whether or not the system may be brought into service. In this guidance we refer to this process as **approval**.

In some cases you may have to seek approval from someone outside your organization such as a government agency, the organization that manages the infrastructure or the organization that operates the trains. However, this is not necessarily the case: your organization may approve its own work. It is possible that you will require approval from more than one party.

In some cases you may obtain approval for specific procedures that you use to carry out the work. In such cases the work may be approved by an authorized and competent person, such as a supervisor, who will grant approval on the basis of evidence that the procedures have been correctly followed.

Note. You will also need to establish the terminology that your organization uses. The process that we refer to as 'approval may be described as 'acceptance' or 'endorsement' or something else.

© Abbott Risk Consulting Ltd. 2022

3 PLANNING A PROGRAM OF ESM ACTIVITIES FOR A PROJECT

3.1 The System Lifecycle

A railway system can be regarded as passing through the following generic **System Lifecycle**:

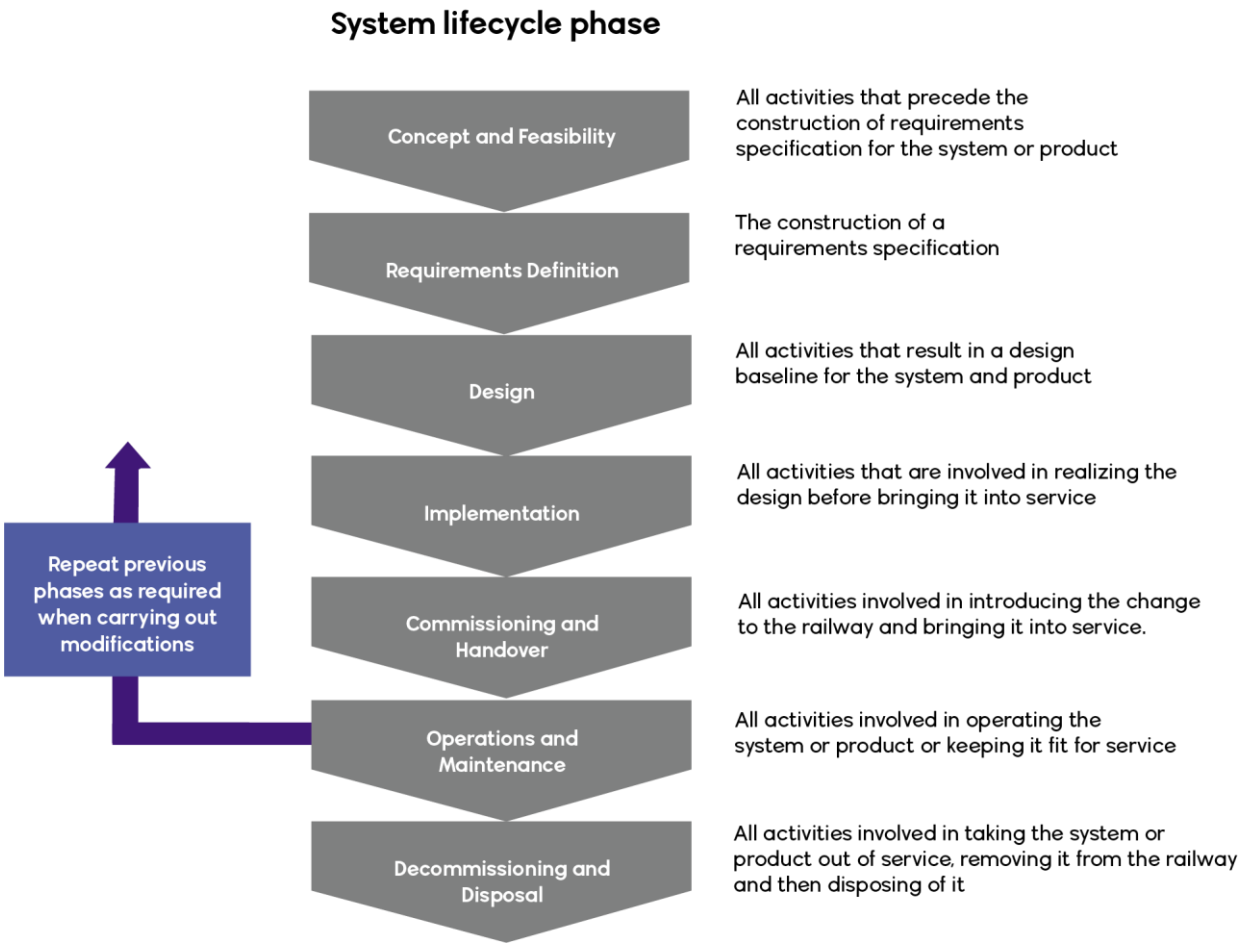


Figure 3-1: The System Lifecycle

The first four phases of this lifecycle may also be executed when developing new products.

This is not a business lifecycle or a project lifecycle. It simply represents the phases through which the system itself passes. A typical system will be worked on by more than one organization during its life.

The system lifecycle above relates to the system lifecycle in EN 50126 [50126-1] as follows:

- The **Concept and Feasibility** phase of the lifecycle above corresponds approximately to EN 50126 phase 1, **Concept.**
- The **Requirements Definitions** phase of the lifecycle above corresponds approximately to EN 50126 phases 2, **System Definition & Operational Context**, phase 3, **Risk Analysis and Evaluation** and phase 4, **Specification of System Requirements**
- The **Design** phase of the lifecycle above corresponds approximately to EN 50126 phase 5, **Architecture and Apportionment of System Requirements** and part of phase 6, **Design and Implementation.**
- The **Implementation** phase of the lifecycle above corresponds approximately to part of EN 50126 phase 6, **Design and Implementation,** phase 7, **Manufacture,** phase 8, **Integration** and phase 9, **System Validation.**

© Abbott Risk Consulting Ltd. 2022

- The **Commissioning and Handover** phase of the lifecycle above corresponds approximately to EN 50126 phase 10, **System acceptance.**
- The **Operations and Maintenance** phase of the lifecycle above corresponds to EN 50126 phase 11, **Operation, Maintenance and Performance Monitoring**.
- The **Decommissioning and Disposal** phase of the lifecycle above corresponds approximately to EN 50126 phase 12, **Decommissioning.**

This volume of the handbook is concerned with projects. The project part of the System Lifecycle comprises all phases apart from Operations and Maintenance. The project may be building something (and active in some or all of the Concept and Feasibility; Requirements Definition; Design; Implementation and Commissioning and Handover phases) or getting rid of something (and therefore active in the Decommissioning and Disposal phase). Moreover, some projects may be replacing one system with another and active in all of these phases.

In this chapter, we take each of the project phases, list the principal activities from the generic ESM process in volume 1 which need to be carried out in this phase and describe the specific tasks that the generic activities are likely to give rise to.

Note when reading this chapter that:

- The full guidance on the topics mentioned is provided in later chapters. This chapter provides a summary which may be useful for initial orientation but there is not enough space to deal with the topics fully. You should read the later chapters before trying to put this guidance into practice or you may miss some important points.
- You should check whether or not the activities recommended for the previous phases have been carried out; if they have not then you should consider remedial work to deal with this.
- It will generally be necessary to maintain the outputs of work carried out in previous phases; that is to update this work if something material should change.
- There are other ESM activities which are performed throughout the lifecycle and are not associated with any particular phase. You should make sure that you perform these as well.

Note: it is often the case, particularly with infrastructure projects, where access to the railway may only be possible overnight and at weekends, that the Implementation phase may be carried out in a series of small steps. Some people refer to this as carrying out ‘stage-works’, others refer to a ‘migration’ from the initial state of the railway to its final state. It is also common for a system to enter a period of interim operation, perhaps to carry out controlled trials, before it enters full service.

If the system is being implemented in stages or it has a period of interim operation , you need to assure yourself that risk has been controlled to an acceptable level whenever the railway is returned to service after an intermediate stage. This may be relatively straightforward compared with showing that risk has been controlled to an acceptable level in the final railway, in which case it can be demonstrated using simpler processes. However, you cannot ignore this issue and need to include it in your planning from the outset.

© Abbott Risk Consulting Ltd. 2022

3.2 The Concept and Feasibility phase

This phase covers activities that precede the construction of a requirements specification for the system or product. The generic ESM activities listed below are typically started during this phase in the manner described below.

Defining the scope

You should attempt to obtain a clear understanding of the aims of the project and of the extent of the system or product that it will deliver. If you are pursuing more than one option for the system or product then you should attempt to obtain a clear understanding of the extent of each option.

Determining safety obligations, targets and objectives

You should establish what legal framework you are working within; the role of standards in the legal framework and approval regimes; and the standards that are applicable to your work.

You should outline at a high level your objectives for safety.

Planning safety activities

You should prepare a short, high-level plan for the ESM program which will describe the overall strategy and approach to reducing safety risks.

Identifying hazards

You should carry out an initial search for hazards associated with the system or product, including hazards specific to intermediate stages, if there are any. You should also look for hazards concerned with the process of building the system or installing the product. This handbook is primarily designed to help with the former but we recommend that you co-ordinate the two hazard identification activities.

Estimating risk

You should annotate identified hazards with an initial appraisal of their severity and likelihood and use this to decide where further analysis is required in later phases.

© Abbott Risk Consulting Ltd. 2022

Independent assessment

If you are appointing an independent assessor (see section 17.2.3 for guidance on when you need to do this) you should identify the people who will provide independent assessment and ask them to review the outputs from the activities above.

3.3 The Requirements Definition phase

This phase covers activities that are associated with the construction of a requirements specification for the system or product. The generic ESM activities listed below are typically advanced during this phase in the manner described below.

Defining the scope

You should obtain a clear understanding of the system or product and its boundaries during this phase. You should also make sure that you are clear about the responsibilities for safety that you have as well as the responsibilities for safety of other people with whom you will be working.

You should clarify the aims, extent and context of your work.

If there is not sufficient information available to completely define the system or product, then you should make explicit assumptions, to be confirmed later.

Determining safety obligations, targets and objectives

If you did not do it in the previous phase, you should establish the obligations for safety arising from the legal framework you are working within and applicable standards.

You should determine precisely your targets and objectives for safety.

You should identify who will approve your work and agree with them how you will present the evidence for safety. In some cases you may obtain approval for specific procedures that you use to carry out the work. In such cases authority for the work may be an authorized and competent person, such as a supervisor, who will grant approval on the basis of evidence that the procedures have been correctly followed.

© Abbott Risk Consulting Ltd. 2022

Planning safety activities

You should plan the ESM program.

The size and depth of your plans will depend on the complexity and level of risk presented by the project. For simple and low-risk projects a brief plan defining the project personnel and justifying a simple approach may be sufficient.

If you assume a project is low-risk, you should make this assumption explicit and plan action to confirm it.

The plan may permit reliance on previous work to demonstrate acceptable risks if the previous work used good practice; it covered all of the project risk; and there is little novelty in development, application or use.

You should integrate your ESM plans with plans for managing human factors.

The plan should be approved by people who will approve the system or product.

Identifying hazards

You should refine your understanding of the hazards of the system or product and the system's or product's effect on overall risk on the railway, taking into account the effects of the operational environment on the system.

Estimating risk

You should decide for each hazard that you have identified which of the following methods will be used to address the risk associated with it (or at least show that the risk is likely to be acceptable):

- Applying standards;
- Comparison with a reference system; or
- Explicit estimation of the severity and likelihood of accidents.

These methods are described further in section 8.2.6.

You should use the understanding of the hazards of the system or product to estimate the risk associated with the system or product using these risk principles. You should take account of human error in performing this estimation. Note that "estimating risk" is a phrase used in Europe [CSM-RA] to give a guide to the level of risk involved. It doesn't provide any objective measure of the actual risk associated with the hazard.

© Abbott Risk Consulting Ltd. 2022

Setting safety requirements
Evaluating risk

You should set safety requirements to control the risk which are consistent with agreed targets for safety.

Good engineering practice for defining integrity requirements for components, such as software and complex electronics, for which systematic failure is a particular concern, is to use Safety Integrity Levels (SILs).

If you set quantitative safety targets, this is normally done by working from a fault tree (or similar representation of cause and effect logic) and the event probabilities to:

A. derive numerical accident targets which conform to the legal criteria for acceptable risk;
B. derive hazard occurrence rate and/or unavailability targets which are consistent with (A); and
C. if applicable, derive SILs that are consistent with (B) for the system's or product's function.

The requirements may be apportioned further to sub-systems of the hierarchy and aligned with the system or product design. Any functional requirements on the system or product that are necessary to reduce risk to an acceptable level should be incorporated as qualitative safety requirements.

Safety requirements to conform to standards should be defined whenever such conformance is assumed in the calculation of safety targets or such conformance is otherwise required to control risks to an acceptable level.

Safety requirements may also arise from relevant regulations, standards and codes of practice.

If your system or product includes software and the software might contribute to risk then you should derive software safety requirements from the system or product safety requirements.

Independent assessment

If you have not already identified the people who will provide independent assessment, you should do so at this stage. You should ask them to review the outputs from the activities above.

© Abbott Risk Consulting Ltd. 2022

3.4 The Design phase

This phase covers activities that are associated with the construction of a design baseline for the system or product. The generic ESM activities listed below are typically advanced during this phase in the manner described below.

Planning safety activities

The ESM plans should be updated as necessary.

Identifying hazards
Estimating risk
Setting safety requirements
Evaluating risk
Implementing and validating control measures
Managing hazards

The ESM activities and the design should contribute to each other. As the design proceeds it will produce additional information which may extend or replace the basis on which the risk estimation was originally done, allowing the risk estimation to be refined and corrected. The risk estimation should be an input to the design, and decisions taken to reduce risk further should be captured as additional safety requirements.

Consideration should be given to controlling risks which may be faced during construction, installation, commissioning, decommissioning and disposal as well as those which may be faced during operations and maintenance.

Any changes to the requirements or design of the system or product should be analyzed for effects on safety. The risk estimation should be adjusted to keep it accurate and safety requirements should be adjusted, if necessary, to ensure that the system or product will still meet its safety obligations, objective and targets.

Compiling evidence of safety

You should define the scope and format of the final report in which you will present evidence of safety with the people who will approve this report. If you have not already done so, you should start to compile evidence of safety into this format. This evidence will include a description of the activities described immediately above and a summary of the main results of these activities.

Independent assessment

Independent assessment will continue.

© Abbott Risk Consulting Ltd. 2022

3.5 The Implementation phase

This phase covers activities that are involved in realizing the design before bringing it into service. The generic ESM activities listed below are typically advanced during this phase in the manner described below.

Activities associated with the decommissioning and disposal of a system being replaced may be incorporated into this phase.

Planning safety activities
Identifying hazards
Estimating risk
Setting safety requirements
Evaluating risk

The risk estimation, safety requirements and ESM plans should be updated as necessary.

Any changes to the requirements or design of the system or product should be analyzed for effects on safety. The risk estimation should be adjusted to keep it accurate and safety requirements should be adjusted, if necessary, to ensure that the system or product will still meet its safety obligations, objective and targets.

Managing hazards

The progress on analyzing hazards, estimating the risk associated with hazards and putting in place control measures which are sufficient to control risk to an acceptable level should be actively tracked.

Implementing and validating control measures
Compiling evidence of safety

Compilation of the safety report will continue.

An Operational and Maintenance Plan should be produced covering:

- Start up, maintenance, changeover and shut down;
- Specified maintenance activities and tools;
- Maintenance competence requirements; and
- Operations competence requirements.

Independent assessment

Independent assessment will lead to a judgment by the independent assessor as to whether risk has been reduced to an acceptable level.

© Abbott Risk Consulting Ltd. 2022

3.6 The Operations and Maintenance phase

This phase covers activities involved in operating the new or changed railway, keeping it fit for service and adjusting it in responsible to changes in the operational environment and the railway's needs. The following generic ESM activities listed below are typically advanced during this phase in the manner described below.

Monitoring risk
Identifying hazards
Estimating risk
Evaluating risk
Implementing and validating control measures

The occurrence of incidents and faults on the railway should be monitored and, if this shows that risk had become or is becoming unacceptable, further control measures will be selected, implemented and validated in order to ensure that the risk remains acceptable.

If major changes to the system or product are required, the activities to make these changes should be organized as a project and the system lifecycle should be restarted.

With this exception, the ESM activities in this phase are outside the scope of this volume, which is focused upon projects. It is intended to provide guidance on ESM activities in this phase in another volume of this handbook.

3.7 The Commissioning and Handover phase

This phase covers activities involved in building a new railway or introducing a change to the railway and bringing the new or changed railway into service. The generic ESM activities listed below are typically advanced during this phase in the manner described below.

Planning safety activities
Identifying hazards
Estimating risk
Setting safety requirements
Evaluating risk

The risk estimation, safety requirements and ESM plans should be updated as necessary.

© Abbott Risk Consulting Ltd. 2022

Compiling evidence of safety

The compilation of evidence for safety into a report should be concluded and the report submitted to those providing safety approval.

The size of the safety report will depend on the risks and complexity of the project. For example, the safety report for a simple and low-risk project should be a short document with brief arguments justifying that the risk is acceptable. A safety report should always be kept as concise as possible but, for a high-risk or complex project, it may have to be longer to present the safety arguments satisfactorily.

The safety report should demonstrate that the system or product complies with its safety requirements and that risk has been reduced to an acceptable level.

The safety report should identify and justify any unresolved hazards, any non-conformances with the safety requirements specification and any departures from the ESM plans, should show that sufficient temporary controls are in place to reduce risk to an acceptable level and should described long term plans for resolving these issues.

The safety report should present or reference evidence to support its conclusions.

The safety report should be consistent with the actual system or product and with other project documentation.

Obtaining approval

A complete version of the safety report should be submitted and approved before a new railway is brought into service or a change is introduced to an existing railway. If the project is making staged changes then several versions may need to be submitted and approved, each covering one or more stages.

Independent assessment

Independent assessment will continue in order to provide assurance that Commissioning and Handover is proceeding as required by the safety report and that any unresolved hazards and any non-conformances with the safety requirements specification are resolved.

© Abbott Risk Consulting Ltd. 2022

3.8 The Decommissioning and Disposal phase

This phase covers all activities involved in taking a system or product out of service, removing it from the railway and then disposing of it.

Most commonly, the decommissioning and disposal of one system will occur during the implementation of another. In this case, the necessary activities to ensure safe decommissioning and disposal may be combined with those for the project producing the new system.

If this is not the case, then the decommissioning and disposal of the system may be regarded as a project in its own right.

For some systems the risks associated with decommissioning and disposal may be small and the guidance should be adjusted accordingly.

You may find it convenient to combine the activities which you carry out to ensure that disposal is carried out safely, with activities to ensure that it is carried out in an environmentally acceptable manner.

The ESM activities associated with decommissioning and disposing of a system or product should be subject to independent assessment in just the same way as the ESM activities associated with creating a system or product.

© Abbott Risk Consulting Ltd. 2022

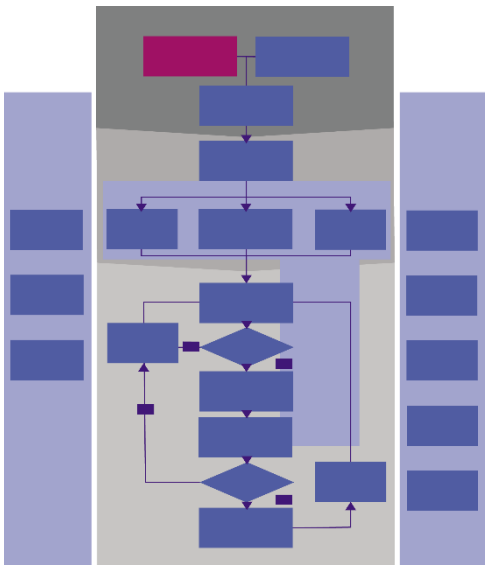
Part II: Project Definition

© Abbott Risk Consulting Ltd. 2022

4 DEFINING THE SCOPE

4.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. This is the starting point for the process. It involves establishing clearly the system or product that is to be delivered and details of the operational environment.



Your organization must define the extent and context of any activity that it performs which affects safety-related systems or products.

If there is uncertainty about any of these things, it will weaken any claims you make for safety.

If you are changing the railway or developing a product, these things are often defined in a requirements specification.

4.2 Guidance

4.2.1 Systems and their environment

Understanding the extent and context of your activities is fundamental to successful ESM. Any railway project can be associated with a system: introducing a new system or changing an existing one. Understanding the boundary between this system and its operational environment is a prerequisite to understanding how the system might contribute to an accident (that is, understanding what its hazards are).

Figure 4-1 illustrates the relationship between the system, hazards and accidents.

Some people use “systems” to refer to electrical components of a railway. iESM uses a broader definition. We define a system to be collection of equipment, people and procedures which are intended to work together to accomplish some function. By this definition an entire railway is a system, and so is a tunnel, a station, a train and a signaling system.

© Abbott Risk Consulting Ltd. 2022

The operational environment consists of anything that could influence, or be influenced by, the system. This will include anything to which the system connects mechanically, electrically or by radio, but may also include other parts of the railway with which there is interaction in other ways, such as through electromagnetic interference, or thermal interchange. The operational environment will also include people and procedures that can affect, or be affected by, the operation of the system.

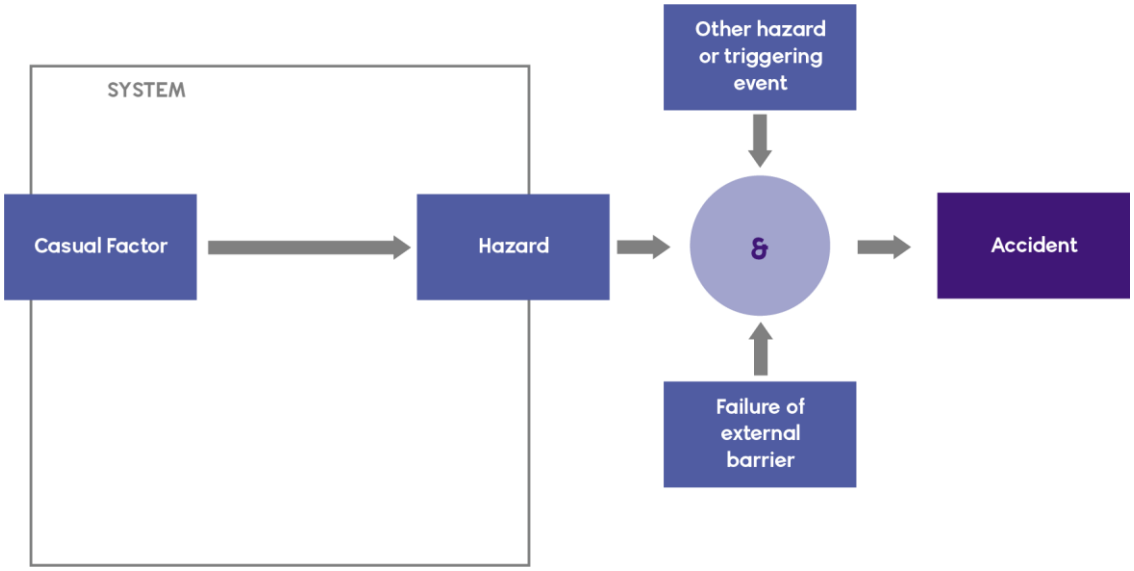


Figure 4-1: Systems, Hazards and Accidents

4.2.2 Systems within systems

Any railway will rely upon a supply chain. Figure 4-2 shows an example of this state of affairs. A train operator relies on a train supplier to provide it with trains. The train supplier, in turn, relies on other companies to supply train equipment, such as the driver's display. Of course this is just a small fragment of a much more complex network of suppliers.

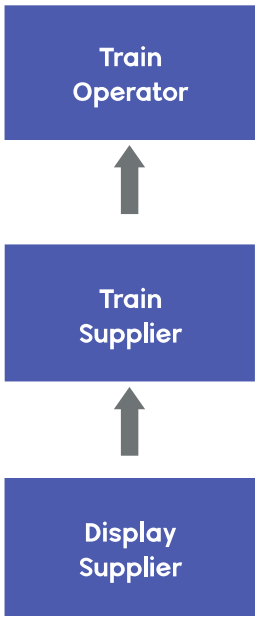


Figure 4-2: A Railway Supply Chain

© Abbott Risk Consulting Ltd. 2022

There is a hierarchy of systems associated with this network of suppliers, as illustrated in Figure 4-3. This shows that System B (a train, perhaps) is part of the railway as a whole and System A (the driver's display, perhaps) is part of System B.

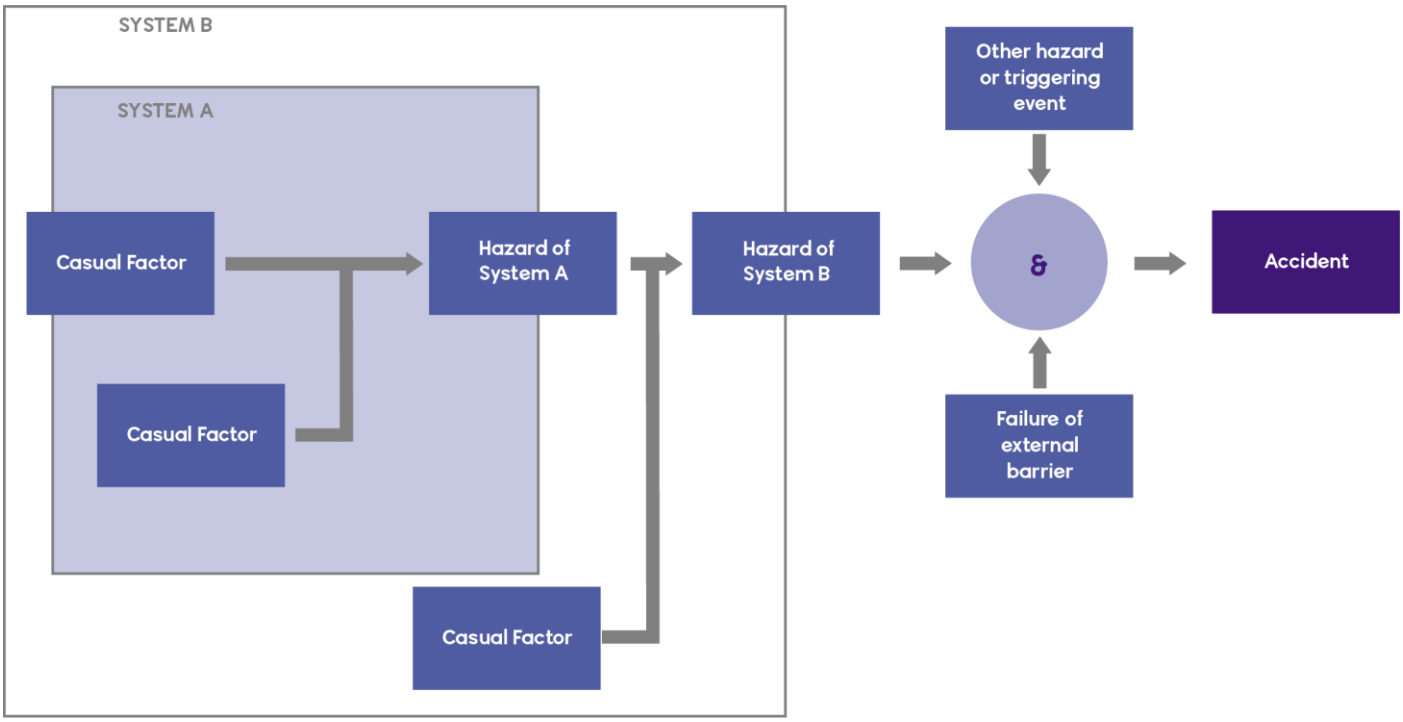


Figure 4-3: The Systems Hierarchy

The suppliers of both system A and system B need to carry out ESM but they will use different system boundaries and, as a result, concentrate on different hazards.

4.2.3 Products and their environments

A product manufacturer may not know all the operational environments in which its product may be considered for application. In general, it proceeds by making informed assumptions (from its own knowledge and by talking to likely customers) about the operational environment that its product will experience and then confirming these assumptions when the product is applied.

Hazards that the product might exhibit in this operational environment are then identified and the product can be designed so that these hazards are eliminated or controlled so that they occur very infrequently. General safety arguments can then be made that the product will be associated with low risk in the assumed operational environment which can be refined into specific arguments that the product will be associated with low risk in the actual operational environment when the product is applied.

© Abbott Risk Consulting Ltd. 2022

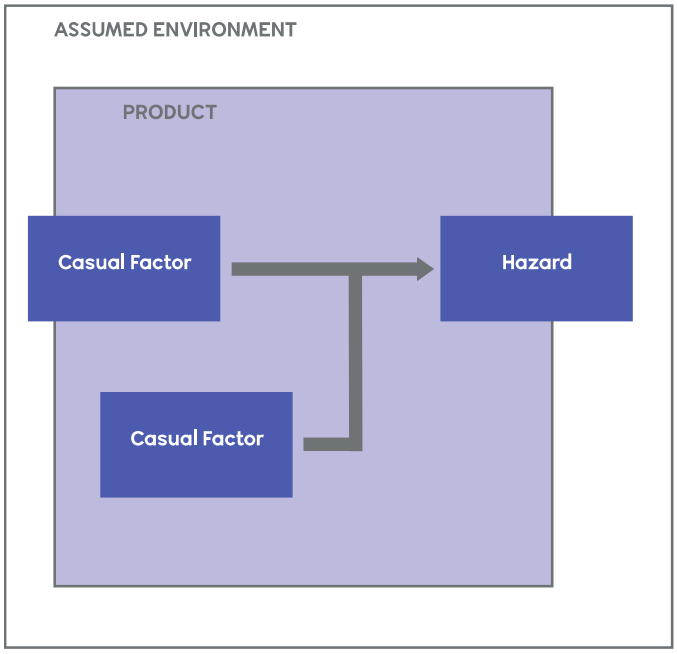


Figure 4-4: Product Development

4.2.4 Introduction to the guidance

This chapter is written for people starting to develop safety-related systems or products.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should define that system or product.
B. If you are delivering a system or product, you should define the operational environment in which that system or product will operate.
C. If you are delivering a system or product, you should monitor the aims, extent and context of your system or product and react to any changes.
D. You should establish the legal framework and acceptance regime within which you are working.

© Abbott Risk Consulting Ltd. 2022

4.2.5 Defining the system or product

A. If you are delivering a system or product, you should define that system or product.

You should attempt to define all relevant parameters of your system or product. If you cannot do this completely at the outset, you should record assumptions and refine the definition of the system or product later. When doing this you should consider the following things:

- **The function of the system or product**
  Not just what it does, but also what it must not do, in normal and degraded modes. Users are often more likely to make mistakes in these modes because they are unfamiliar and the tasks that they have to perform may be more difficult. It is important that the transitions between modes should be well-managed, and human factors will influence your ability to achieve this.

  It may be useful to construct a function list or a function breakdown – further guidance on doing this may be found in EN 50126 [50126-1].

- **How novel it is**
  You should look for systems or products that are similar to or related to the system or product that you are delivering. You should identify aspects of the system or product that you are delivering that are new or being applied in a new context. Similar and related systems and products may also provide useful information that you can use to design safety into your system or to show that it is safe.

- **The quality of the service it must provide**
  The standard to which the functional requirements are to be fulfilled. Relevant criteria include:
  - safety;
  - reliability;
  - availability;
  - maintainability;
  - economy;
  - service life (stating how this will be accepted);
  - industry and other standards and norms (themselves functional);
  - train service quality management;
  - targets (train paths provided, delays, recovered energy, efficiency, costs);
  - public perception; and
  - additionally, for adapting existing railways while traffic continues to run, the quality of the service provided (operated and supported by staff of stated competence) during the staged introduction of new systems or products.

- **Other contractual and related issues**
  If you do not take these into account you may find that they limit your ability to react to problems in the future. Relevant issues include:
  - patents and copyright;
  - licenses (jigs, tools, templates, software use and alteration);
  - spares and special test/diagnostic equipment;
  - documentation and manuals;

© Abbott Risk Consulting Ltd. 2022

- certification; and
- training.

4.2.6 Defining the environment

B. If you are delivering a system or product, you should define the environment in which that system or product will operate.

You should attempt to define all relevant parameters of the operational environment. If you cannot do this completely at the outset, you should record assumptions and refine the system definition later.

When doing this you should consider the following things:

- **How the system or product will be used and maintained**
  It may be useful to construct operational and maintenance scenarios, accounts of typical periods in the operation and maintenance of the system or product – further guidance on doing this may be found in EN 50126 [50126].

- **The people who will use the system or product and other stakeholders**
  For example operators, passengers, maintainers, installers, those responsible for decommissioning, regulators, and management. You should assess both the required and existing competency of staff using the system or product.

- **The interfaces between the system or product and other technical systems. For example:**
  - trains (human drivers or automatic systems, train protection, vehicle health monitoring);
  - permanent way (train detection, points, indicators, bridges, tunnel ventilation and so on);
  - electrical traction power (supply distribution control);
  - neighbors (level crossings, other railways);
  - station and terminal services, depots, technical (positional references, loadings, earthing policy, heat dissipation);
  - chemical interfaces – (dissimilar metals); and
  - data formats and information flow.

- **Other aspects**
  Relevant considerations may include:
  - staff competence
  - railway rules and procedures;
  - weather;
  - shock and vibration;
  - electromagnetic interference;
  - noise;
  - local conditions and lighting;
  - faulting and maintenance support policy; and
  - vandalism/terrorism/malicious acts.

Guidance on notations for representing the components of a system and their interfaces is provided in iESM Application Note 3.

© Abbott Risk Consulting Ltd. 2022

4.2.7 Monitoring for change

C. If you are starting to produce a system product, you should write down any assumptions that you make about the operational environments in which your system or product will run.

The checklist above is relevant to this guidance again but, as you may not know all the operational environments in which your product will run you will need to make assumptions. These assumptions should be made explicit and written down. When it comes to preparing a safety report for a specific application, a large part of the work required will be to confirm that these assumptions hold in the application in question.

D. If you are delivering a system or product, you should monitor the aims, extent and context of your system or product and react to any changes.

The aims, extent and context may change during the life of the system or product. If they do change, you should review all affected ESM activities and rework them as necessary.

4.2.8 Establishing the legal framework and acceptance regime

E. You should establish the legal framework and acceptance regime within which you are working.

You should establish:

- who will approve your work;
- what legal framework you are working within;
- the role of standards in the legal framework and approval regimes; and
- the standards that are applicable to your work.

There is further guidance in section 14.2.2 on establishing who will approve your work. There is further guidance in section 8.2.7 on the role that standards can play in estimating and controlling risk.

4.3 Sources of further guidance

Section 8.2.7 provides guidance on the role that standards can play in estimating and controlling risk.

Section 14.2.2 provides guidance on establishing who will approve your work.
Chapter 19 provides guidance on safety roles and responsibilities.

Section 22.2.6 provides guidance on the information that should be provided to suppliers, to allow them to carry out effective safety analysis.

iESM Application Note 3 provides guidance on notations for representing the components of a system and their interfaces.

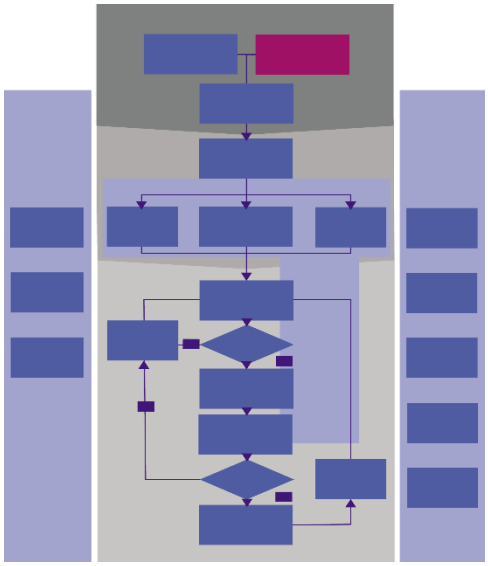
EN 50126 [50126] provides more guidance on system definition, including guidance on drawing up function lists, function breakdowns and operational scenarios.

© Abbott Risk Consulting Ltd. 2022

5 DETERMINING SAFETY OBLIGATIONS, TARGETS AND OBJECTIVES

5.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. Having established the scope for the project, it is necessary to determine clearly what obligations your organization has which are relevant to safety and to set clear objectives for the safety of the delivered system or product.



Your organization must establish the obligations that are relevant to the safety of its systems or products.

You may have obligations to meet certain criteria before you can accept the risk. You may also have obligations to perform certain tasks.

Your organization must define objectives and targets for safety that are consistent with its obligations.

The objectives for safety will be primary objectives for the organization but it will have other objectives. You should consider all objectives together. You may find conflicts between these objectives, in which case you will need to find a rational resolution of these conflicts.
The people leading your organization should allocate the resources needed to meet the objectives for safety.

© Abbott Risk Consulting Ltd. 2022

5.2 Guidance

5.2.1 Introduction to the guidance

This chapter is written for people starting to develop safety-related systems or products.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should establish the obligations that are relevant to the safety of the system or product.
B. If you are delivering a system or product, you should define objectives and targets for safety that are consistent with your obligations.
C. If you are delivering a system or product, you should ensure that your project works towards its obligations, objectives and targets.

5.2.2 Determining safety obligations

A. If you are delivering a system or product, you should establish the obligations that are relevant to the safety of the system or product.

You should search for these obligations in the laws of the states in which the system or product will be developed and used, in your own organization's procedures and, if you are working for a customer, in any contract that you have signed with a customer.

You may have obligations to:

- Follow defined processes;
- Produce defined deliverables;
- Ensure that your system or product meets certain defined standards; and
- Ensure that risk meets certain acceptability criteria.

You should write down these obligations and communicate them to the people who need to know.

5.2.3 Determining safety objectives and targets

B. If you are delivering a system or product, you should define objectives and targets for safety that are consistent with your obligations.

Objectives and targets may include maximum rates of occurrence of failures or hazards.

© Abbott Risk Consulting Ltd. 2022

5.2.4 Working towards safety obligations, objectives and targets

C. If you are delivering a system or product, you should ensure that your project works towards its obligations, objectives and targets.

The objectives and targets and any obligations which are not fully covered by objectives and targets, should be regarded as project requirements. The plans for the project should be designed to meet these obligations, objectives and targets. You should put in place activities to confirm that the obligations, objectives and targets are being met.

5.3 Sources of further guidance

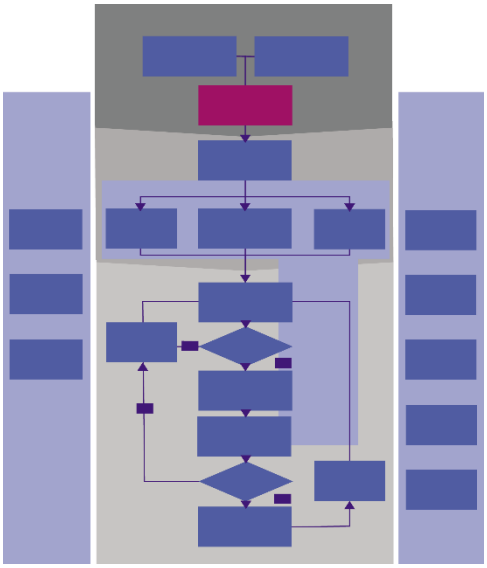
Chapter 6 provides guidance on planning ESM activities.

© Abbott Risk Consulting Ltd. 2022

6 PLANNING SAFETY ACTIVITIES

6.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. Having clarified objectives and scope, as they relate to safety, it is necessary to plan out a program of ESM activities to deliver them.



Your organization must plan out a program of ESM activities that will deliver the safety objectives and targets.

You may cover all ESM activities in one plan but you do not have to. You may write different plans for different aspects of your work at different times, but you should plan each activity before you do it. Your plans should be designed to deliver your safety objectives and targets and you should review your plans periodically to check that they are consistent with your safety objectives and targets.

Your plans should be enough to put this generic process into practice. Your plans for ESM should be integrated with other plans for the project.

If there is a possibility that you may become involved in an emergency on the railway, you should have plans to deal with it. You should adjust the extent of your plans and the ESM activities you carry out according to the extent of the risk. You should review your plans in the light of new information about risk and alter them if necessary.

You may include ESM activities in plans that are also designed to achieve other objectives. The output of this planning process may be called something other than a ‘plan’ – for example, a ‘specification’ or a ‘schedule’. This does not matter as long as the planning is done.

© Abbott Risk Consulting Ltd. 2022

You may have plans at different levels of detail. You may, for example, have a strategic plan for your project that sets out a program of activities to achieve your objectives for safety. You may then plan detailed ESM activities for individual tasks.

If you intend to use cross acceptance in your program of ESM activities, your plans should make clear what part cross acceptance will play in that program.

Your organization must carry out activities that affect safety by following systematic processes that use recognized good practice. Your organization must write these processes down beforehand and review them regularly.

The project should use good systems engineering practice to develop safety-related systems and products.

When choosing methods, you should take account of relevant standards. You should confirm that a method is appropriate to the task in hand before applying it. You should keep your processes under review and change them if they are no longer appropriate or they fall behind good practice.

The people leading your organization should be aware of good practice and encourage staff to adopt it.

6.2 Guidance

6.2.1 Introduction to the guidance

This chapter describes the different types of plans that may be required for ESM during a project and provides guidance on the production of these plans and their content.

Whatever type of planning you are going to do, the objective will be the same, that is to set down all of the things that need to be done to ensure that the work is done safely and efficiently so that it can be agreed and communicated to those who need to know. There are seven basic criteria for a good plan:

- **what**: describes what the work involves, including details of the tasks that need to be completed and the records required. The level of detail should reflect the needs of the people using the plan and the consequence of doing the wrong thing.
- **how**: describes the method, often referring to a specification.
- **where**: describes the locations that the work will take place.
- **when**: describes the overall timescales and the times that parts of the work have to take place, including sequences of actions and periodicities of repetitive tasks.
- **who**: allocates tasks to individuals and names the people responsible for doing and checking the work.
- **with**: describes the resources to be used (tools, materials, plant, supplier resources and so on).
- **why**: describes the rationale for the work so that it can be related back to your company goals and the overall railway goals that need to be managed.

Your plans for safety should meet these criteria. All of your plans should be co-ordinated.

Your plans should be consistent with good practice. What constitutes good practice is relative and depends on:

© Abbott Risk Consulting Ltd. 2022

- the type of work that you are doing;
- the level of integrity that you are designing into 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 people planning the development of safety-related systems or products.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should plan a program of activities which is designed to deliver your safety obligations, targets and objectives.
B. If you prepare plans for a project, your plans should be appropriate to the nature of the project.
C. If you are delivering a system or product, you should submit your plans for ESM to the authorities who will approve the system or product.
D. If you are delivering a system or product, you should prepare preliminary plans for your ESM activities before you carry out any significant ESM activities.
E. If you are delivering a system or product, you should prepare comprehensive plans for your ESM activities as soon as you have sufficient information to do so.
F. If you are delivering a system or product, you should keep your plans up-to-date if you change your approach.
G. If you are delivering a system or product which contains software, you should plan to ensure that the software is of sufficient integrity.

6.2.2 Preparing and obtaining approval of plans

A. If you are delivering a system or product, you should plan a program of activities which is designed to deliver your safety obligations, targets and objectives.

For guidance on establishing your safety obligations, targets and objectives, see chapter 5.

The construction of a new railway or any significant change to an existing railway should be run as a project. You should prepare plans for the ESM activities on this project. The plans should justify the ESM approach to be followed, so that it may be considered and approved.

Your plans should meet the criteria presented above, in the introduction to this section.

B. If you prepare plans for a project, your plans should be appropriate to the nature of the project.

The size of the plans will depend on the complexity and level of risk presented by the project. For simple and low-risk projects a brief plan defining the project personnel and justifying a simple approach may be sufficient. If you assume a project is low-risk, you should make this assumption explicit and take action to confirm it.

The plans may permit reliance on previous work to demonstrate acceptable risks. You would not normally do this unless:

© Abbott Risk Consulting Ltd. 2022

- the previous work used good practice;
- 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.

The plans should be scoped according to the information available and the organization 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 some plan.

The plans for ESM may be combined with other project plans.

If the work you are doing comes within your organization's Safety Management System then you may be able to make your plans shorter by referring to the requirements of this system.

You should search for good practice for the delivery of similar systems and products in local and international standards and in authoritative text books and ensure that the processes that you plan to use are at least as effective as relevant good practice.

C. If you are delivering a system or product, you should submit your plans for ESM to the authorities who will approve the system or product.

You should do this regardless of the level of complexity or risk.
The primary purpose of your plans for ESM is to plan out a program of activities to control risk. However it is also an opportunity to inform authorities who will approve the system or product of the project's intentions and to obtain their feedback on them. Therefore the plans should normally be submitted to these authorities for approval.

D. If you are delivering a system or product, you should prepare preliminary plans for your ESM activities before you carry out any significant ESM activities.

You may have insufficient information at an early stage in your project to prepare comprehensive plans. In that case you should prepare preliminary plans to cover the first stages of your project.

The preliminary plans will be short, high-level version of the full planning documents, produced as early in the project as possible, and describing the overall strategy and approach to reducing safety risks.

The next guidance point suggests a list of topics to be treated comprehensive safety plans. The preliminary plans should concentrate on the topics which are most relevant to the early stages of the project, These are likely to include:

- The definition of the system or product;
- The life cycle to be followed
- The safety objectives and targets for the system or product;
- Hazard identification;

© Abbott Risk Consulting Ltd. 2022

- Risk estimation and evaluation;
- Establishing safety requirements;
- Managing hazards and assumptions; and
- The authorities to whom the safety report should be submitted.

It may be convenient to present the preliminary plans in the format chosen for the comprehensive plans with some sections containing a note that they will be completed later.
Each section of a preliminary plan should be brief; detailed planning will be carried out after safety requirements have been set, and documented in a more comprehensive plan.

E. If you are delivering a system or product, you should prepare comprehensive plans for your ESM activities as soon as you have sufficient information to do so.

Your plans should cover the following topics:

- Scope of the plan including definition of the system or product;
- Interfaces to other work;
- Life cycle to be followed;
- Safety objectives and targets for the system or product;
- Engineering safety organization and responsibilities, including subcontractors;
- Hazard identification;
- Hazard Log management;
- Risk estimation and evaluation;
- Establishing and maintaining safety requirements;
- Validation of safety requirements;
- Managing human factors and how this is integrated with ESM;
- Managing hazards, assumptions and application conditions;
- Identification of safety-related deliverables;
- Format of the safety report that will be prepared and the authorities to whom it should be submitted;
- Independent assessment and audit arrangements;
- Configuration management;
- Quality management; and
- Assumptions and constraints made in the plan.

If any of these topics is dealt with in another plan or procedure, your plans for safety may summarize the topic and refer to the other document for more detail.

A suggested outline for a Safety Plan which covers these topics is provided in iESM Application Note 2 but many other formats are also effective.

It is often the case, particularly with infrastructure projects where access to the railway may only be possible overnight and at weekends, that the Implementation phase may be carried out in a series of steps. Some people refer to this as carrying out ‘stage-works’, others refer to a ‘migration’ from the initial state of the railway to its final state. If this is the case, you need to assure yourself that risk has been controlled to an acceptable level whenever the railway is returned to service after

© Abbott Risk Consulting Ltd. 2022

an intermediate stage. This may be relatively straightforward compared with showing that risk has been controlled to an acceptable level in the final railway, in which case it can be demonstrated using simpler processes. However, you cannot ignore this issue and need to deal with it in your planning from the outset.

You should ensure that the system is designed to reduce the potential for human error to cause accidents and to increase the potential for human action to prevent accidents.

6.2.3 Keeping plans up to date

F. If you are delivering a system or product, you should keep your plans up-to-date if you change your approach.

The plans 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 revised plans should be re-submitted to the people who approved the original plans for re-approval.

6.2.4 Planning for software integrity

G. If you are delivering a system or product which contains software, you should plan to ensure that the software is of sufficient integrity.

If the system that you are building contains software, then you will have to provide assurance that:

- the software does not contribute to a hazard; and
- where the system relies on the software to control hazards, the software does this successfully.

You should consider how you will provide this assurance from the outset when designing the system and the software. Generally, to do this, you will need to show that:

- the software safety requirements are sufficient;
- the software meets its software safety requirements; and
- if the software is configurable, that configuring it has not introduced risk (or, if it has, that this risk has been controlled).

The software safety requirements will specify the behavior of the software and its safety integrity, which is a measure of the confidence that the software will behave safely.

Section 13.2.4 provides guidance making a safety argument for software which has already been developed.

We consider that EN 50128 [50128] represents good practice for development of railway software for railway control and protection systems. For rolling stock on-board software EN 50657 [50657] is very similar, even down to the section numbering.

© Abbott Risk Consulting Ltd. 2022

There are other programmable devices, whose programming data are sufficiently similar to software that they deserve to be treated in a similar manner. For example, Field Programmable Gate Array (FPGA) devices are reconfigurable logic gate networks. They are programmable, may have internal states and have complex software-like functions, and are configured using something that looks very much like a programming language. Further details on the safe application of such hardware-based logic devices can be found in EN 50129 Appendix F [50129].

Other systems have behavior that is defined by configuration data, which may have many of the features of software. Where programming data and configuration data has the complexity of software, then some at least of the guidance in EN 50129 and IEC 61508 [61508] is likely to be useful. However, this guidance may not be applicable without modification. In these cases, EN 50128 / EN 50675 and IEC 61508 may be useful as a guide, but you will have to replace inapplicable requirements with other tools, techniques and measures that meet the same underlying need.

6.3 Sources of further guidance

Chapter 5 provides guidance on establishing your safety obligations, targets and objectives.
Section 13.2.4 provides guidance making a safety argument for software which has already been developed.

iESM Application Note 2 contains a suggested outline for a Safety Plan.

EN 50128 [50128], EN 50657 [50657] and IEC 61508 [61508] provide guidance on developing safety-related software.

© Abbott Risk Consulting Ltd. 2022

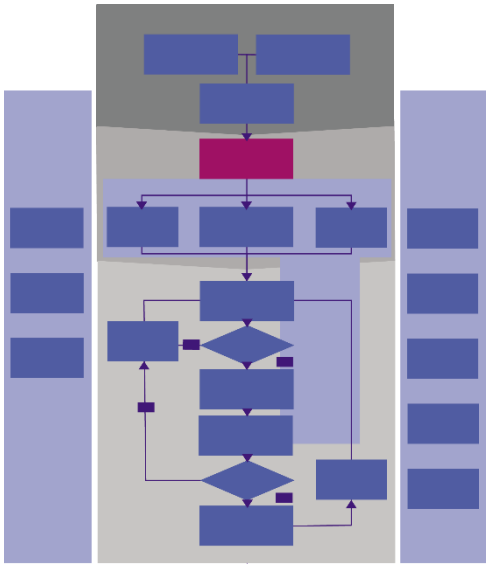
Part III: Risk Analysis

© Abbott Risk Consulting Ltd. 2022

7 IDENTIFYING HAZARDS

7.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. Hazards are initially identified from the definition of scope. The Hazard Log is reviewed throughout the life of the system and product and new hazards may be identified as additional information becomes available.



Your organization must make a systematic and vigorous attempt to identify all possible hazards related to its systems or products.

Identifying hazards is the foundation of ESM. You may be able to take general actions, such as introducing safety margins. However, if you do not identify a hazard, you can take no specific action to eliminate it or control the risk relating to it.

When you identify a hazard relating to your activities and responsibilities, you should make sure that you understand how your activities might contribute to the hazard and the risk arising from it.

You should not just consider accidents that might happen during normal operation. You should also consider accidents that might happen at other times, such as installation, testing, commissioning, maintenance, decommissioning, disposal and degraded operation, or when operations are not normal.

The focus of ESM is on hazards associated with the systems or products being delivered. There may be also hazards associated with the work that is being done. For example, the workers performing installation may be exposed to electrocution hazards. These are normally controlled by separate processes but it may make sense to integrate these processes with ESM processes.

When identifying hazards, you should consider the interfaces between the system or product that you are delivering and other people, organizations and systems.

© Abbott Risk Consulting Ltd. 2022

You should look for hazards associated with any changes in the way the railway is operated and maintained.

You should not ignore hazards that happen extremely infrequently. You should record these hazards together with the reasons for believing that they happen very infrequently.

When identifying hazards, make sure that you take proper account of the effects of human behavior. Even the most highly automated systems are designed, installed, operated and maintained by people. Everybody makes errors. People's behavior plays a part in most, if not all, accidents.

7.2 Guidance

7.2.1 Introduction to the guidance

Hazard identification is fundamental to the risk estimation process. Absence of a systematic and comprehensive hazard identification phase can severely undermine the risk estimation process. In the worst case this can create an illusion of safety and a false sense of confidence.

Although hazard identification can and should be started as soon as an initial description of the system or product is available, accurate and comprehensive identification of the hazards of a system or product can only be completed with an accurate and precise characterization of the system and its operational environment. This activity therefore relies upon the **Defining the scope** activity.

Once the hazards have been identified, it becomes possible to estimate the risk associated with a system or product. This activity therefore supports the **Estimating risk** activity. In fact, in some cases this activity may overlap the **Estimating risk** activity.

As the hazards are identified, they should be recorded and tracked in a register of hazards. This is part of the **Hazard management** activity.

This chapter is written for people identifying the hazards associated with a system or product or reviewing the results of these activities.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should consider all phases of the lifecycle of the system or product at which it is present on the railway when identifying hazards.
B. If you are delivering a system or product, you should check that you have a workable understanding of the system or product and its operational environment.
C. If you are delivering a system or product, you should use previous knowledge to identify hazards.
D. If you are delivering a system or product, you should carry out a preliminary hazard analysis early in the project.
E. If you are delivering a system or product, you should carry out a thorough search for hazards as soon as this becomes possible.
F. If you are delivering a system or product, you should carry out analysis to identify hazards in any areas of novelty.
G. If you are delivering a system or product, you should take account of human factors when identifying hazards.
H. If you are delivering a system or product, you should document the results of hazard identification.
I. If you are delivering a system or product, you should structure the list of hazards and avoid unnecessary duplication.
J. If you are delivering a system or product, you should keep the Hazard Log up-to-date.

© Abbott Risk Consulting Ltd. 2022

K. If you are delivering a system or product, you should look for opportunities to integrate the identification of hazards of the system or product with the identification of hazards associated with the construction and installation of the system or product.
L. If you are delivering a system or product, you should make sure that the people identifying hazards collectively have sufficient knowledge and expertise to do the work competently.

7.2.2 Preparing to identify hazards

A. If you are delivering a system or product, you should consider all phases of the lifecycle of the system or product at which it is present on the railway when identifying hazards.

When identifying hazards, you should not restrict yourself to steady-state operation, but consider all aspects of the System Lifecycle from the point at which it is installed on the railway to its final decommissioning, including maintenance and upgrade.

B. If you are delivering a system or product, you should check that you have a workable understanding of the system or product and its operational environment.

Before identifying hazards, you need to understand the system or product and its interactions with its operational environment. For further guidance on achieving this understanding, see chapter 4.

If there are significant aspects of the system or product or its operational environment that you cannot establish, you should make an explicit assumption and make sure that it is confirmed later. For further guidance on managing assumptions, see section 16.2.3.

You should identify any interactions between the system or product and its operational environment that have not previously been identified and consider whether they could cause hazards.

C. If you are delivering a system or product, you should use previous knowledge to identify hazards.

If your system or product is a variant of a previous system or product for which hazards were identified then you should review the hazards of the previous version and carry them forward where they still apply.

Otherwise, you should look for similar systems or products for which hazards were identified and review these.

In any case, you should look for relevant standard lists of hazards and review these. Your organization or your customer may have such lists.

There is a general checklist which you may use for identifying hazards in iESM Application Note 1.

© Abbott Risk Consulting Ltd. 2022

7.2.3 Preliminary hazard identification

D. If you are delivering a system or product, you should carry out a preliminary hazard analysis early in the project.

Safety analysis is iterative: as the design progresses, the analysis should be repeated to take account of change and extended to cover the extra detail. By doing this, hazards can be identified early and the design can be modified to eliminate or mitigate them while it is still at an early stage, avoiding expensive rework later.

A **Preliminary Hazard Analysis** (PHA) should be carried out early in the project. The PHA combines a first-pass hazard identification with a first-pass risk estimation (see chapter 8). The risk estimation should consist of annotating the hazards with an initial appraisal of their severity and likelihood.

Preliminary Hazard Analysis is intended to determine:

- the scope and extent of risk presented by a system or product, so that ESM may be applied to an appropriate depth; and
- a list of potential hazards that may be eliminated or controlled during initial design activity.

Preliminary Hazard Analysis should be carried out as soon as an initial description of the function of the system or product and of its interfaces to people and other systems is available and before any significant design work is done. To focus later effort upon the most significant hazards, the hazards should be ranked.

The findings of Preliminary Hazard Analysis should be documented.

7.2.4 Comprehensive hazard identification

E. If you are delivering a system or product, you should carry out a thorough search for hazards as soon as this becomes possible.

A more thorough search for hazards should be carried out when the system or product and its operational environment is fully specified.
You should not exclude hazards just because they are very unlikely to occur, particularly if they could lead to catastrophes, but events which are impossible or completely incredible should be excluded from the list. The risk of a signaling system in Berlin being damaged by a tsunami may be excluded, for example.

F. If you are delivering a system or product, you should carry out analysis to identify hazards.

Unless the system and product is well understood and you are sure that all its hazards are controlled by standards, you should analyze the system or product from first principles to search for hazards.

Your analysis should take account of the following aspects of the system or product:

- Its functionality, including the time that it takes to perform functions;
- Its physical structure;

© Abbott Risk Consulting Ltd. 2022

- Its interfaces with other systems, including environmental interactions such as temperature and humidity; and
- Its interfaces with people.

For simple systems or products, informal brainstorming may be sufficient.

The following methods may also be used:

- A **System Hazard Analysis (SHA)** is a systematic, creative brainstorm examination of a technical design by a multi-disciplinary team. The design needs to be well developed (but not necessarily complete) for it to be effective.
- An **Interface Hazard Analysis** (**IHA**) is a systematic, creative brainstorm examination of a design by a multi-disciplinary team. It focuses on the hazards associate with the interfaces which could be technical, with users, operators and maintainers and external parties e.g. emergency services.
- A **Hazard and Operability Study (HAZOPS)** (see iESM Application Note 3) is a systematic, creative brainstorm examination of a design by a multi-disciplinary team. It is a general-purpose technique but quite labor-intensive and difficult to carry out before design information is available.
- **Functional Hazard Analysis** is a systematic analysis of the effects of misbehaviors of a system in which each of the system's functions is taken in turn and consequences of that function failing to operate, operating incorrectly or operating at the wrong time are considered. For further information, see '*Hazard Analysis Techniques for System Safety*' [Ericson].
- **Failure Mode and Effects Criticality Analysis (FMECA)** (see iESM Application Note 3) is an analysis of technical failures that allows the effects of these failures to be identified and their implications for safety and reliability to be estimated. However, it is of limited use in identifying hazards with human or environmental causes. It is also of limited use in identifying hazards arising from multiple technical failures. FMEA supports risk estimation as well as reliability and maintainability analysis in addition to hazard identification.

Further, more specialized techniques are described later in this chapter. EN 50129 [50129] provides a comprehensive bibliography of safety engineering techniques, including techniques which are useful for hazard identification.

Techniques for analyzing the interfaces with people are described in the next point.

G. If you are delivering a system or product, you should take account of human factors when identifying hazards.

Identifying, assessing and reducing the risk associated with human error should be part of any safety process.

It is possible to identify, model and control human error, and human reactions to failure. There are useful human reliability techniques that allow a practitioner to identify human contribution to hazards, assess that risk, and devise methods to reduce that risk. You should ensure that appropriate human reliability techniques are used and that they are used correctly.

In order to identify sources of human error, you should first understand the tasks that are being carried out. If you do not fully understand the tasks that people will perform, and the manner in which they are to be carried out, you cannot comprehensively identify where hazards may originate.

© Abbott Risk Consulting Ltd. 2022

The possible sources of error can be identified using methods that use the results of the task analysis. A variant of HAZOPS (see above) may be applied to the task analysis, with an adapted set of for dealing with the classes of errors that people make. Alternatively, a variant of FMEA (see above) can be used.

The following specialized techniques may also be used:

- **Task Analysis** for man-machine interfaces (see *'Human-Computer Interaction'* [Preece]). This is of value in identifying hazards which may be caused by human error.
- **Operating and Support Hazard Analysis** The Federal Aviation Administration *System Safety Handbook* [DoT] and '*Hazard Analysis Techniques for System Safety'* [Ericson] provide guidance on this technique.

You should integrate the process of human error identification with the general process of hazard identification within the project.

7.2.5 Keeping records of hazard identification

H. If you are delivering a system or product, you should document the results of hazard identification.

Once identified, the hazards should be documented. A Hazard Log is usually created (see section 16.2.2).

I. If you are delivering a system or product, you should structure the list of hazards and avoid unnecessary duplication.

A hazard usually has several causes. If you have identified a large number of hazards, you should check to see that you have not separately identified multiple causes of a single hazard. It is generally a good idea to define hazards so that they occur on the boundary of the system, as the last event within the system in the potential line of cause and effect leading to the accident to occur.

Many legal frameworks require no action for risks of the sort that are routinely accepted in ordinary life. These are sometime referred to as 'broadly acceptable' or 'broadly accepted' risks. The risk of passengers cutting themselves on the edges of paper timetables might be such a risk. Hazards associated with risks of this nature may be excluded from the list. The risk of a passenger falling into a significant gap between the train and the platform would however not currently be considered broadly acceptable.

7.2.6 Keeping the Hazard Log up-to-date

J. If you are delivering a system or product, you should keep the Hazard Log up-to-date.

As more design information becomes available you should review it to see whether it reveals a new hazard or whether it shows that a previously identified hazard cannot occur and, if so, you should update the Hazard Log accordingly.

If the system or product or its operational environment changes during the project, you should analyze this change and update the Hazard Log if necessary.

© Abbott Risk Consulting Ltd. 2022

7.2.7 Co-ordination with other safety activities

K. If you are delivering a system or product, you should look for opportunities to integrate the identification of hazards of the system or product with the identification of hazards associated with the construction and installation of the system or product.

The focus of ESM is on hazards associated with the systems or products being delivered. There may be also hazards associated with the construction and installation of the system or product. For example, the workers performing installation may be exposed to hazards that could lead to electrocution. These are normally identified and controlled by separate processes but it may make sense to integrate the identification of both sorts of hazards.

7.2.8 Competence

L. If you are delivering a system or product, you should make sure that the people identifying hazards collectively have sufficient knowledge and expertise to do the work competently.

Identifying hazards requires knowledge and expertise of both:

- the system or product, including its function and design; and
- the operational environment in which the system or product will run.

Typically, the former is provided by the system or product supplier and the latter is provided by the organization that will use the system or product.

The person or persons leading the analysis should have received training in ESM or have had experience of successfully delivering a program of ESM activities or both. They should also have received training in the analysis techniques employed or have had experience of successfully applying them or both.
For further guidance on competence management, see chapter 21.

7.3 Sources of further guidance

Chapter 4 provides guidance on defining the boundaries of a system or product

Chapter 8 provides guidance on estimating risk.

Chapter 16 provides guidance on maintaining a Hazard Log, which can act as a repository for risk estimation data, and on managing assumptions.

Chapter 21. provides further guidance on competence management.

iESM Application Note 1 contains a general checklist which you may use for identifying hazards.

iESM Application Note 3 describes some relevant techniques.

EN 50129 [50129] provides a comprehensive bibliography of safety analysis techniques, including techniques which are useful for hazard identification.

© Abbott Risk Consulting Ltd. 2022

For further guidance on Task Analysis for man-machine interfaces see '*Human-Computer Interaction'* [Preece]).

For further guidance on Operating and Support Hazard Analysis, see the Federal Aviation *Administration System Safety Handbook* [DoT] and *'Hazard Analysis Techniques for System Safety'* [Ericson].

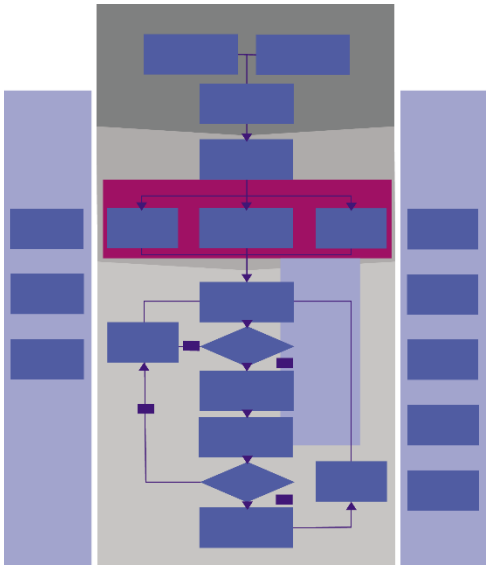
© Abbott Risk Consulting Ltd. 2022

8 ESTIMATING RISK

8.1 Principles from Volume 1

The risk associated with each hazard is estimated and aggregated to estimate the risk associated with the system or product. This estimation may later be reduced as control measures are introduced.

The acceptability of this risk is not evaluated in this activity; it is done in the **Evaluating risk activity**, which is described below.



Your organization must assess the effect of its work on the overall risk on the railway.

In most countries, you will have a legal duty to assess risk.

Risk depends on the harm that could arise and the likelihood that an accident will happen. You should consider both factors. Your organization should also consider *who* is affected and verify that no-one is exposed to an unacceptable level of risk.

You may make an explicit estimation of the risk, that is, you may estimate the frequency with which incidents will occur and the harm done, either as numbers or by selecting from a number of categories.

There are two other accepted ways of addressing the hazards, or at least of showing that the risk associated with them is below an acceptable threshold, that may support sound decisions with considerably less effort.

Firstly, if a hazard is fully addressed by accepted standards[1] that define agreed ways of controlling it, showing that you have met these standards may be enough to control the hazard or to meet your legal obligations or both. For example, the electrical safety of ordinary office equipment is normally shown by meeting electrical standards.

[1] We use the word 'standard' in this volume to include other forms of authoritative guidance such as rules and codes of practice.

© Abbott Risk Consulting Ltd. 2022

Secondly, if you can show that your system is sufficiently similar to a **reference system,** another system that is known to be safe, and that the risk associated with some hazards of your system is no more than that associated with the reference system, then you may be able to conclude that this risk is acceptable.

In both cases, there may be occasions when a limited increase in risk may be accepted for a change if that change delivers significant benefits and no group of people experiences an unfair increase in risk. This may be the case, for example, for a project to increase the speed at which trains can run.

While following both of these alternative methods will generally give a strong indication that the risk is acceptable, the final decision is still taken later in the process, during the **Evaluating risk** activity. This allows other factors, such as risk that is not addressed by standards or differences between the system being built and the reference system, to be taken into account.

Some things are done with the aim of making the railway safer, that is to reduce overall railway risk, for example installing automatic train protection. You should still assess them in case they introduce other risks that need to be controlled.

You should consider people's behavior, when estimating the risk. Understanding how people behave when things go wrong is important in understanding the risk. People prevent accidents as well as contributing to them, and you should also take this into account.

Your estimation of risk should take account of any relevant output from the **Monitoring risk** activity described below.

8.2 Guidance

8.2.1 Introduction to risk estimation

Most railway work is associated with risk; that is, the potential for harm to people. The risk can vary from negligible to totally unacceptable.

Risk can generally be reduced, although usually at a cost.

Risk estimation entails a systematic analysis of the severity and likelihood of accidents arising from the work.

Risk estimation is tightly coupled with hazard identification and risk reduction. The hazards of a system or product have to be identified before an accurate assessment of risk can be made. Risk estimation provides, throughout the lifecycle of a system or product, both input to risk reduction and feedback on its success.

The guidance in this chapter will help you to establish the facts on which you have to take a decision that involves risk. Guidance on taking that decision is provided in chapter 10.

When you assess risk you will often find that you have to make assumptions. There is guidance on managing these assumptions in section 16.2.3.

Risk estimation is focused on demonstrating compliance with legal safety obligations and these are phrased in terms of harm to people. These obligations place constraints on the alternatives that may be followed.

© Abbott Risk Consulting Ltd. 2022

In broader decision making, it is appropriate to consider non-safety losses, such as environmental and commercial harm, as well as the opportunities for reaping benefits of many different sorts. The practices described in this chapter can be extended to estimate such non-safety losses but that is beyond the scope of this guidance. Techniques such as Weighted Factor Analysis, (see '*Risk – A Missed Opportunity?*' [Hessami]) provide a basis for balancing the factors in such decision making.

8.2.2 Three methods of risk estimation

This handbook follows the example set by the European Common Safety Method on Risk Evaluation and Assessment [CSM-RA] in identifying three main methods of risk estimation.

- You may make an explicit estimation of the risk, that is, you may estimate the frequency with which incidents will occur and the harm done.
- If a hazard is fully addressed by accepted standards that define agreed ways of controlling it, showing that you have met these standards may be enough to demonstrate that the risk has been reduced to an acceptable level.
- If you can show that your system is sufficiently similar to a reference system, another system that is known to be safe, and that the risk associated with your system is no more than that associated with the reference system, then you may be able to demonstrate that the risk has been reduced to an acceptable level.

Strictly only the first method delivers an actual estimation of risk; the last two methods only show that the risk is below an acceptable threshold. However, in many circumstances it is not necessary to deliver a precise estimate of risk and it is sufficient to show that risk is below a maximum acceptable value. The second two methods do this and we follow the usage established by the European Common Safety Method.

A more accurate title of this chapter and the process which it describes would be "Estimating risk (or demonstrating that it is below an acceptable threshold)". We hope that the reader will accept the title of "Estimating risk" as a practical abbreviation.

It is acceptable to use different approaches for different risks.

8.2.3 Introduction to the guidance

The following three sub-sections provide guidance specific to each of the three risk assessment methods described above, including guidance on when each approach is appropriate.

This chapter is written for people estimating the risk associated with a system or product or reviewing the results of these activities.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should consider all phases of the lifecycle of the system or product at which it is present on the railway when identifying hazards.
B. If you are delivering a system or product, you should check that you have a workable understanding of the system or product and its operational environment.
C. If you are delivering a system or product, you should carry out a preliminary hazard analysis early in the project.
D. If you are delivering a system or product, you should decide upon your approach to risk estimation early in the project.
E. If you are delivering a system or product, you should select appropriate methods to support your approach to risk estimation.
F. If you are delivering a system or product, you should carry out a thorough risk estimation as soon as this becomes possible.
G. If you are delivering a system or product, you should keep the risk estimation up-to-date.
H. If you are delivering a system or product, you should document the results of risk estimation.

© Abbott Risk Consulting Ltd. 2022

I. If you are delivering a system or product, you should take account of human and organizational factors when estimating risk.
J. If you are delivering a system or product and a hazard comes completely within accepted standards that define agreed ways of controlling it, you may be able to control the risk associated with that hazard and show that you have done so by showing that you have complied with these standards.
K. If you are delivering a system or product and controlling risk by applying a standard, you should record which hazards are controlled by which standards and the reasons for believing that this is the case.
L. If you are delivering a system or product, you may be able to demonstrate that the risk associated with some or all hazards of a product or system has been reduced to an acceptable level by comparing with a reference system or product.
M. If you are demonstrating that the risk associated with some or all hazards of a product or system has been reduced to an acceptable level by comparing with a reference system or product, you should record the grounds for believing that risks have been controlled.
N. If you are performing explicit risk estimation for a system or product, you may estimate risk qualitatively or quantitatively. You should make a reasoned choice between the two approaches.
O. If you are performing explicit risk estimation for a system or product, you should use historical data to support risk estimation where available but you should use it with caution.
P. If you are performing explicit risk estimation for a system or product, you should consider whether the uncertainties in your estimation of risk might lead to different conclusions and if so you should try to reduce this uncertainty.
Q. If you are performing explicit risk estimation for a system or product, you should carry out causal analysis - analysis of the causes of hazards - to a level which is sufficient to support robust risk estimates.
R. If you are performing explicit risk estimation for a system or product, you should carry out consequence analysis - analysis of the consequences of hazards - to a level which is sufficient to support robust risk estimates.
S. If you are performing explicit risk estimation for a system or product, you should use the results of causal and consequence analysis to support a rational estimation of the severity and likelihood of accidents.
T. If you are performing explicit risk estimation for a system or product, likelihood-severity matrices may provide a practical method of performing qualitative risk estimation but you should use them with caution.
U. If you are performing quantitative risk estimation, you should establish conventions for severity assessment.
V. If you are performing explicit risk estimation for a system or product, you may need to model parts of the railway in order to estimate the effect of your system or product on overall risk.
W. If you are performing explicit risk estimation for a system or product, you should take account of the potential for people to cause and to prevent accidents.
X. If you are delivering a system or product, you should make sure that the people estimating risk collectively have sufficient knowledge and expertise to do the work competently.

8.2.4 Preparing to assess risk

A. If you are delivering a system or product, you should consider all phases of the lifecycle of the system or product at which it is present on the railway when identifying hazards.

When estimating risk, you should not restrict yourself to steady-state operation, but consider all aspects of the System Lifecycle from the point at which it is installed on the railway to its final decommissioning, including maintenance and upgrade.

© Abbott Risk Consulting Ltd. 2022

B. If you are delivering a system or product, you should check that you have a workable understanding of the system or product and its operational environment.

Before estimating risk, you need to understand the system or product and its interactions with its operational environment. For further guidance on achieving this understanding, see chapter 4.

If there are significant aspects of the system or product or its operational environment that you cannot establish, you should make an explicit assumption and make sure that it is confirmed later. For further guidance on managing assumptions, see section 16.2.3.

8.2.5 Preliminary risk estimation

C. If you are delivering a system or product, you should carry out a preliminary hazard analysis early in the project.

A preliminary hazard analysis combines preliminary hazard identification and preliminary risk estimation. It is described in section 7.2.3.

8.2.6 Risk principles and methods

D. If you are delivering a system or product, you should decide upon your approach to risk estimation early in the project.

You should decide for each hazard that you have identified which of the following risk principles will be used to estimate the risk associated with it:

- Applying standards;
- Comparison with a reference system; or
- Explicit estimation of the severity and likelihood of accidents.

This sub-section provides general guidance on risk estimation. The following three sub-sections provide guidance specific to each of the three approaches described above, including guidance on when each approach is appropriate.

E. If you are delivering a system or product, you should select appropriate methods to support your approach to risk estimation.

There are a number of formal safety methods available for risk estimation or aspects of risk estimation and we describe some of these below.

It is not always necessary to employ formal safety methods. The purpose of ESM – to foresee and forestall hazards – parallels mainstream engineering and mainstream engineering methods may be focused upon safety issues.

Some aspects of risk estimation may rely on expert judgment. This is appropriate in cases where the risks are low or the decision which risk estimation will support is straightforward.

© Abbott Risk Consulting Ltd. 2022

When risk estimation is being done by expert judgment, it is good practice to ensure that there is documented consensus from a group of experts whose knowledge covers the area being assessed and who share a common understanding of the assessment process.

F. If you are delivering a system or product, you should carry out a thorough risk estimation as soon as this becomes possible.

A thorough estimation of risk becomes possible when a stable outline design has been created. Risk estimation should be carried out as soon as it becomes possible so that it can have the greatest influence on the evolving design at the least cost.

G. If you are delivering a system or product, you should keep the risk estimation up-to-date.

If the system or product or its operational environment changes during the project, you should analyze this change and update the Hazard Log if necessary.

Once the system or product has entered service, you should also monitor risk. Chapter 15 provides guidance on monitoring risk.

H. If you are delivering a system or product, you should document the results of risk estimation.

The results of a risk estimation study may be compiled into a report so that they can be reviewed and, if required, approved.

Risk estimation results should also be incorporated into the Hazard Log. See section 16.2.2 for guidance on maintaining a Hazard Log.

I. If you are delivering a system or product, you should take account of human and organizational factors when estimating risk.

The effects of human error should be integrated with other aspects of risk estimation.

You should note that socio-organizational factors contribute to accidents as well as direct physical causes. For example, while the direct physical cause of an incident may be a maintenance error, this may in turn be the result of an organizational culture in which deviations from agreed procedures are routine and accepted.

Current practice in risk estimation often does not take these factors into account and, instead, deals with them separately (see for example chapter 20 of this volume which deals with promoting a safety culture).

Techniques are emerging to include socio-organizational factors within risk estimation.
For further details, see "*Engineering a Safer World: Systems Thinking Applied to Safety*" [Leveson2].

© Abbott Risk Consulting Ltd. 2022

8.2.7 Risk estimation by applying standards

This method of risk estimation is appropriate when there are authoritative standards that control one or more risks and your work is compliant with these standards. This can be difficult as most standards are not written in a way that makes it clear which risk is being addressed by each requirement.

We use the word 'standard' in this section to include other forms of authoritative guidance such as rules and codes of practice.

J. If you are delivering a system or product and a hazard comes completely within accepted standards that define agreed ways of controlling it, you may be able to control the risk associated with that hazard and show that you have done so by showing that you have complied with these standards.

Standards may be associated with the legal framework in which you are working. You may be legally required to comply with certain standards. In some cases, it may also be illegal to require someone to go beyond certain standards. In the European Union, there are circumstances in which both these things are true for 'Technical Specifications for Interoperability', standards associated with European railway interoperability directives.

However, standards and other authoritative sources of good practice play a role in decision-making that goes beyond the requirements of the law.

As we said in volume 1, '*if a hazard is fully addressed by accepted standards that define agreed ways of controlling it, showing that you have met these standards may be enough to control the hazard or to meet your legal obligations or both*.'

Before you decide that just referring to standards is enough, make sure that:

- the standards are acknowledged to represent good practice in the railway sector;
- all of the risk associated with the hazard is covered by the standards;
- the standards cover your situation; and
- there are no obvious and straightforward ways of reducing risk further.

If a standard does not completely cover the risk associated with the hazard, its provisions may still provide a useful starting point for measures that do cover the risk. Hence, you will need to make sure that you are familiar with the standards that are relevant to your work.

K. If you are delivering a system or product and controlling risk by applying a standard, you should record which hazards are controlled by which standards and the reasons for believing that this is the case.

These reasons, along with evidence that the standards were in fact applied, will form the main inputs to the evaluation of whether risk has been satisfactorily controlled.

© Abbott Risk Consulting Ltd. 2022

8.2.8 Risk estimation by comparison with a reference system or product

This method of risk estimation is appropriate when there is a similar system or product which is known to be associated with an acceptable level of risk.

Normally, if you use this method, you will estimate that the risk associated with a new system is acceptable if it is no greater than the risk associated with the reference system. However, if you have targets to improve safety compared with current levels then this may not be sufficient. This method of risk estimation can still be used under these circumstances but you may need to set more stringent criteria.

L. If you are delivering a system or product, you may be able to demonstrate that the risk associated with some or all hazards of a product or system has been reduced to an acceptable level by comparing with a reference system or product.

You will need to decide whether you are going to use this approach for all hazards of your system or product or a subset of them.

For each hazard for which you use this approach, will need to show that:

- the risk associated with this hazard in the reference system or product is acceptable;
- there are no differences between your system and product and the reference system or product that could cause a significant increase in this risk; and
- there are no between the operational environment of your system or product and the operational environment of the reference system and product that could cause a significant increase in this risk.

This approach to risk estimation has some similarities with cross-acceptance as described in chapter 12. Both use the fact that one system or product is found to be safe as part of the evidence that another system or product may be regarded as safe.

Cross-acceptance is generally applied to the whole system or product. It is supported by explicit risk estimation, which is used to show that the effect of differences between the two systems or products does not result in acceptable risk.

This approach to risk estimation is generally applied to individual hazards. It is an alternative to explicit risk estimation: if it is not possible to show that a hazard is satisfactorily controlled by comparing with a reference system or product, then it will be necessary to show this by explicit risk estimation or by arguing that the hazard is controlled by standards.

M. If you are demonstrating that the risk associated with some or all hazards of a product or system has been reduced to an acceptable level by comparing with a reference system or product, you should record the grounds for believing that risks have been controlled.

These grounds will form the main inputs to the evaluation of whether risk has been satisfactorily controlled. They will include:

- The evidence that the risks associated with the reference system or product are acceptable;

© Abbott Risk Consulting Ltd. 2022

- The differences that you have identified between your system and product and the reference system and product and between the operational environment of your system and product and the operational environment of the reference system and product; and
- The reasons for believing that none of these differences causes an unacceptable increase in risk.

8.2.9 Explicit risk estimation

Explicit risk estimation should be used for risks for which the other two approaches are not suitable.

N. If you are performing explicit risk estimation for a system or product, you may estimate risk qualitatively or quantitatively. You should make a reasoned choice between the two approaches.

Qualitative risk estimation relies mainly upon expert judgment and past experience.

It can be done with less effort than quantitative risk estimation and does not need as much data but it produces results that are less precise and more subjective.

Qualitative risk estimation is likely to suffice for most hazards. However, hazards with the potential to lead to major or catastrophic consequences, may require quantitative risk estimation. A quantitative approach may also be needed for novel systems or products where there is insufficient experience to support an empirical, qualitative approach but should only be applied if it is justified by the increased confidence achieved.

O. If you are performing explicit risk estimation for a system or product, you should use historical data to support risk estimation where available but you should use it with caution.

Risk estimation always relies on some form of extrapolation from the past to the future. This may be the result of expert judgment but may also include data derived from industry-standard handbooks and published statistics and data from other sectors.

Historical data is very valuable but it should be used with care. The reasons for this include the following:

- Insufficient information may be available to determine whether historical figures are relevant to the circumstances of concern, particularly regarding rare major or catastrophic accidents and the circumstances surrounding previous incidents.
- Secondary effects arising from an incident are likely to be difficult to reliably determine (for example fires, derailment or exposure to harmful substances).

Inappropriate use of historical data can undermine the analysis, and significantly reduce the accuracy of risk estimation.

Where historical data is employed in an assessment, a clear argument should be presented that its use provides an accurate forecast of the losses associated with the particular circumstances under study.

© Abbott Risk Consulting Ltd. 2022

P. If you are performing explicit risk estimation for a system or product, you should consider whether the uncertainties in your estimation of risk might lead to different conclusions and if so you should try to reduce this uncertainty.

There are always uncertainties in any risk estimation. You should recognize this when performing the estimation and when presenting the results.

Your estimation does not need to be precise if the uncertainties would not affect the decisions that you make.

It is acceptable to make approximations, provided that they are conservative, that is, that they do not underestimate risk.

There are circumstances in which you can make very broad approximations without affecting your conclusions and it is generally sensible to do this and put effort into reducing uncertainty elsewhere.

Q. If you are performing explicit risk estimation for a system or product, you should carry out causal analysis - analysis of the causes of hazards - to a level which is sufficient to support robust risk estimates.

You should determine those factors contributing to the occurrence of each hazard, in order to enable accurate assessment of the likelihood of occurrence of each hazard and help identify measures to reduce the likelihood of its occurrence.

You may find it most efficient to perform consequence analysis (see next point) before starting causal analysis in order to establish which hazards are most likely to lead to an accident. If a hazard is very unlikely to lead to an accident, it may be possible to show that the risk associated with it is acceptable with limited causal analysis. Performing consequence analysis before causal analysis can therefore help to avoid performing unnecessary work.

Causal analysis requires knowledge of the system or product. Causal analysis generally assumes that the system or product is organized as a hierarchy of components.

Casual analysis can start with an outline description of the system but, before it can be completed, the analyst should have seen a complete set of design material.

Most causal analysis techniques employ a diagrammatic representation of the errors and failures leading to a hazard. This helps to understand and communicate the relationships between the causes of a hazard and is therefore recommended.

Since the causal models are usually generated with the assistance of individual domain experts, they should be subject to peer review in order to enhance confidence in their integrity and correctness.

Fault Tree Analysis and FMEA are techniques which may be used to perform causal analysis. They are described in iESM Application Note 3. EN 50129 [50129] provides a comprehensive bibliography of safety analysis techniques, including causal analysis techniques. EN 50126 [50126] also provides guidance on identifying the failure modes of hardware items which may support these or other techniques.

Causal analysis may be done qualitatively or quantitatively.

© Abbott Risk Consulting Ltd. 2022

Qualitative causal analysis should be done to a depth sufficient to enable a realistic subjective estimate to be made of the likelihood or frequency of the hazard. It may not be necessary to go to the level of detail of failures in basic system or product components in order to do this.

Fault Tree Analysis can support qualitative causal analysis. One qualitative method of analyzing fault trees is to compute **minimal cut sets**, that is the smallest sets of basic events in the fault tree which are sufficient to cause the hazard to occur. The minimal cut sets indicate possible accident scenarios.

Quantitative causal analysis of a hazard should continue until all the fundamental causal factors have been identified, or until there is insufficient reliable data to go further. Fundamental causal factors include basic component failures and human errors.

Accurate quantification of causal models requires an objective assessment of the frequency or probability of occurrence of fundamental causal factors. These are then combined in accordance with the rules of probability calculus to estimate the frequency or probability of occurrence of the hazard.

Key issues are:

- obtaining reliable and accurate data;
- dealing with uncertainty in the data;
- sensitivity analysis; and
- ensuring that probabilities and frequencies are combined correctly (for example ensuring that two frequencies are not multiplied to yield units in terms of per time squared).

Quantitative causal analysis techniques are generally based upon formal mathematical foundations and are supported by computer-based tools.

If a particular hazard occurs frequently, and reliable statistics are available concerning the probability of its occurrence, detailed quantitative causal analysis may not be necessary, but it may still be useful in determining the causes of the hazard and helping to identify potential hazard prevention measures.

R. If you are performing explicit risk estimation for a system or product, you should carry out consequence analysis - analysis of the consequences of hazards - to a level which is sufficient to support robust risk estimates.

Consequence analysis involves determining the possible effects of each hazard. The results of consequence analysis should provide an estimate of the likelihood of occurrence of each incident following realization of the hazard in order to:

- support accurate assessment of the likely losses associated with a hazard; and
- help identify control measures for the hazard.

Consequence analysis requires knowledge of the system's or product's operational environment and how the system or product will be used. It is generally applied to each hazard.

Key issues are:

- developing a clear understanding of the hazard; and

© Abbott Risk Consulting Ltd. 2022

- determining existing physical, procedural and circumstantial barriers to the escalation of the hazard.

Most consequence analysis techniques employ a diagrammatic representation of the lines of cause and effect and this is encouraged.

Consequence analysis techniques typically present the results of analysis in the form of a logic tree structure. Event Tree Analysis and Cause Consequence Diagramming are such techniques. The latter is described in iESM Application Note 3. EN 50126 [50126] provides a comprehensive bibliography of safety analysis techniques, including consequence analysis techniques.
Consequence analyses should be subject to peer review in order to enhance confidence in their integrity and correctness.

It is important in consequence analysis to consider the full range of consequences. Do not assume that because a failure is described as failing to a safe state that it cannot contribute to an accident. Typically, even 'fail-safe' failures lead to alternative, temporary methods of working, which increase risks.

Consequence analysis may be done qualitatively or quantitatively.

Qualitative consequence analysis should be conducted to a depth sufficient to enable a realistic subjective estimate to be made of the likelihood of occurrence of an incident or accident. As a general rule, the analysis should be continued until all potential incidents arising from a hazard have been identified.

Quantification of consequence trees requires an assessment of the probability of each accident trigger occurring or of each barrier preventing an accident. Such assessment may be based upon historical data, the results of specific causal analysis such as Fault Tree Analysis or, where no objective data can be obtained, on the basis of expert opinion.

Key issues are:
- obtaining reliable and objective data sources for the assessment of barrier strengths;
- appropriate treatment of uncertainty in the data sources; and
- sensitivity analysis of barrier strengths.

Quantitative consequence analysis techniques are generally based upon formal mathematical foundations and are supported by a suite of computer-based tools.

S. If you are performing explicit risk estimation for a system or product, you should use the results of causal and consequence analysis to support a rational estimation of the severity and likelihood of accidents.

For each accident that a hazard may cause, an estimate should be made of the likelihood that the accident will occur as a result of that hazard and the severity of the consequences.

© Abbott Risk Consulting Ltd. 2022

Sometimes a hazard may have the potential to lead to a range of accidents with different severities and likelihoods. To obtain a wholly accurate estimate of the risk, it is necessary to consider the risk associated with each type of accident and then combine these estimates. Considering the likelihood that *any* accident will occur with the severity of *the worst case* accident is a conservative approximation which is often acceptable. However, you should be careful if you do this as sometime it can result in an estimate of the risk which is excessively high.

This may be done qualitatively or quantitatively.

T. If you are performing explicit risk estimation for a system or product, likelihood-severity matrices may provide a practical method of performing qualitative risk estimation but you should use them with caution.

If you have to carry out a series of risk estimations of applications of similar systems or products, then you may find that a **likelihood-severity matrix** can save repeating the same work.

A likelihood-severity matrix has the general format shown below:

Likelihood	Severity			
	Insignificant	Marginal	Critical	Catastrophic
Frequent				
Probable				
Occasional				
Remote				
Improbable				
Incredible				

Table 8-1 Example format of likelihood-severity matrix
Table 8-1 is only an illustrative example. Other headings may be used.

The two components of risk – frequency (or likelihood) and consequence (or severity) – are partitioned into broad order of magnitude categories which are then used to index the rows and columns of a matrix. Each cell within the matrix then represents a broad region of risk. The example above is empty but, in a real matrix, a risk category is written into the cell.[2]

A matrix of this sort may be used for prioritizing hazards for action, in which case it will normally be applied to the initial estimation of the risk and the cells in the matrix will contain a number indicating the priority.

When using the matrix, the basis on which each risk is classified should be recorded (for example whether it is based upon experience or expert judgment).

[2] It is also possible to split the frequency or likelihood into two components: the frequency or likelihood of a hazard occurring and the likelihood of an accident occurring given that the hazard has occurred. This can remove some excessive conservatism for hazards that are unlikely to lead to an accident but the table become more complex.

© Abbott Risk Consulting Ltd. 2022

A matrix of this sort may also be used to support decisions on risk acceptability, in which case it will be applied to risk before and after mitigation and the cells in the matrix will contain an indication of the acceptability of risk. In this case, the definitions of the categories are normally chosen such that there is a constant factor of increase in either likelihood or severity as one moves from one category to the next (often a factor of 10 or 5). The benefit of doing this is that if one moves diagonally from one cell to one which is one category more likely and one category less severe, the overall risk will remain comparable. It can also help when establishing SILs when a risk reduction factor of for example ten is needed. We note that the example matrix published in EN 50126 Annex C [50126-1] is not structured like this and therefore is not recommended.

Using a matrix to support decision on risk acceptability will naturally also support the process of setting safety requirements by providing feedback. Where risk is not acceptable additional safety requirements will be added and the risk re-estimated until it is found to be acceptable.

You should be cautious about using a likelihood-severity matrix as the only method of assessing the acceptability of risk because it is imprecise and subjective. If a risk is given a very low classification of both likelihood and severity then this classification may be enough to conclude that it is acceptable. However, as the risk rises towards the upper threshold of acceptability, further analysis will normally be required before it can be concluded that the risk is acceptable. Moreover, some risk acceptance criteria in use cannot be tested using a likelihood-severity matrix. For example, a requirement to reduce risk as low as reasonably practicable can only be demonstrated by considering the options available which are not shown on the matrix.

It is not possible to create one general-purpose matrix that will suit all railway applications. A matrix should be designed with likelihood, severity and risk acceptability categories that are appropriate to the situation in hand. The matrix should be associated with:

- definitions of the categories used;
- an explanation of how the risk acceptability categories relate to the legal criteria for acceptable risk and to any agreed overall safety targets;
- assumptions on which the matrix is based; and about the system or product, its hazards, its operational environment and its mode of use;
- a clear statement of the population to which the matrix applies, that is, whether the likelihood categories are the likelihood of an accident caused by a single system or product or the likelihood of an accident caused by a defined number of systems or products; and
- guidelines for the use of the matrix.

To avoid possible later problems with use of the matrices, you should submit the matrix with your justification that it meets these criteria for approval by any authority whom you may later ask to approve a Safety Case which uses the matrix.

© Abbott Risk Consulting Ltd. 2022

U. If you are performing quantitative risk estimation, you should establish conventions for severity assessment.

When performing quantitative risk estimation, likelihoods are usually presented as probabilities or frequencies.

Severities may be expressed in terms of a sum of fatalities and weighted injuries. The terminology used and the weighting vary from railway to railway. If you use this method then you should find out how the railway that you are working on uses it. One convention that is used is as follows:

- 1 major injury is equivalent to 0.1 fatalities
- 1 minor injury is equivalent to 0.01 fatalities

It is possible, but not essential, to assign a monetary value to losses expressed as fatalities and weighted injuries. This is most useful in supporting decisions on expenditure to reduce risk, in which case it is common to use an indication of what level of expenditure is considered to be necessary, if it would reduce risk by one fatality. Such a figure is often referred to as a **Value of Preventing a Fatality (VPF)**. The VPF is a parameter intended only for supporting decisions on whether risk has been controlled to an acceptable level. It is not an estimation of the commercial loss that might follow from such a fatality and so cannot be used for purposes such as arranging insurance cover.

The total estimated number of fatalities and weighted injuries is multiplied by the VPF to yield a monetary loss, for decision-making purposes.

Further guidance on one method of performing these calculations is published in “Taking Safe Decisions” [RSSB1].

Be aware that all benchmarks are only rough reflections of the values held by society at large. If there is significant public concern about a hazard, then you should take this into account in your decision making and it may justify precautions that would not be justified otherwise. In some countries, for instance, a risk associated with an accident in which many people might die is considered to require more effort to control than a risk associated of several single-fatality accidents, even if the statistical estimate of the number of fatalities is the same for both risks.

V. If you are performing explicit risk estimation for a system or product, you may need to model parts of the railway in order to estimate the effect of your system or product on overall risk.

Many hazards are caused by failures that put the railway into a dangerous state. There are almost always mechanisms to detect the failure and mitigate the danger. Usually, for instance if both filaments of the red aspect of a signal fail, this is detected by the interlocking which will almost immediately set other signals red.

The fact that railway systems and products mitigate each other’s hazards provides network resilience: the railway as a whole is safer and more reliable than any of the individual systems.

It is possible to inadvertently degrade this network resilience if this is not recognized. For example, if an emergency is reported using a mobile telephone rather than a railway telephone, then the recipient may not have confirmation of the location of the person reporting the emergency. This effect may be outweighed by the advantages of using a mobile telephone but it should not be forgotten.

© Abbott Risk Consulting Ltd. 2022

You need to take account of failure detection in two ways to assess the effect of a system or product on overall risk.

- Firstly, you need to understand how the railway can detect and respond to hazardous failures of your system or product in order to estimate the time at risk, the time between entering and leaving the dangerous state. You should do this as part of consequence analysis.
- Secondly, you need to understand how your system or product can reduce risk arising from other causes by detecting or mitigating hazards elsewhere.

You can reduce overall risk by increasing the system's or product's ability to detect hazards in the rest of the railway. However, when you replace an old system or product, you may also inadvertently reduce the ability of the railway to detect failure. Any loss of failure detection should be weighed against possible improvements in safety that may result in an overall improvement.

Where an existing system or product is being replaced, it may be possible to use the results of hazard analysis carried out on the original in order to understand how it relates to other systems in the event of a hazard. You should examine the interfaces of the existing system or product to identify the systems (including such things as track) with which it interacts, and identify the failure modes of these systems.

You should take account of any assumptions or application conditions associated with the system or product (see sections 16.2.3 and 16.2.4). Through them you can identify the manner in which it interacts with the other parts of the railway.

Failure scenarios can be complex. The railway may pass through several unsafe states, before returning to a safe one. State-transition diagrams and the Unified Modeling Language (UML) can provide useful notations for capturing these scenarios. For further information on state transition diagrams, see iESM Application Note 3.

In some cases, it may be sufficient to make a single point estimate of the time at risk, based upon the most likely scenario for making the railway safe.

If you have modeled failure scenarios using state transition diagrams, you can use these to estimate time at risk. In the simple case where there is only one sequence of events, a single estimate of the time spent in each state may be calculated. Markov models may be used to make a statistical estimate of time at risk in more complex situations.

W. If you are performing explicit risk estimation for a system or product, you should take account of the potential for people to cause and to prevent accidents.

Many hazards will have both human and technical causes. In order to model the causes of hazards, it is necessary to consider both classes, and the manner in which they interact.

Standard notations for representing cause and effect, such as event and fault trees, can be used to describe the sequences of events that lead to, and from, a hazard. Human error events can be integrated into these descriptions.

With human error represented within the overall model of errors for a system or product, it is possible to assess the likelihood of an error occurring, and of it leading to a hazard and an accident. In order to do this you will need to assess the likelihood of human actions being carried out incorrectly. Likelihood of human error can be expressed either qualitatively or quantitatively.

© Abbott Risk Consulting Ltd. 2022

There are many methods for assigning human failure probabilities to human actions. Most use some mix of recorded probabilities of errors from a database, and expert assessment, to reason about and simulate human behavior and the likelihood of an error. Experts and data sampling are subject to bias, and techniques exist that attempt to minimize this bias.

You should understand dependencies between human actions.

One human error may make others more likely. A person may, knowing the correct value, mistakenly enter an incorrect value into a single system. Having committed this error, then they may enter the same incorrect value into multiple systems. Similarly, a mistake by an operator that results in a hazardous situation may cause them to be more stressed, impairing their thought processes and making further errors more likely. An inadequate understanding of dependencies between human actions can lead to a significant underestimation of risk.

See '*Incorporating Human Dependent Failures in Risk estimations to Improve Estimates of Actual Risk*' [Hollywell] for more information on dependencies between human actions.

When human error is considered within the context of technical failures, it is possible to use methods such as calculating the minimal cut sets for fault trees to identify those events that have the most impact on the likelihood of a hazard, identifying how the risk can be reduced most effectively.

As with technical failures, such as mechanical breakdown, the likelihood of human error is affected by environmental, physical and organizational factors. Human reliability techniques exist that allow you to model the effect that these factors have on the likelihood of human error. It is possible by improving an environmental or organizational factor, that the likelihood of error at several stages in a chain of events leading to a hazard can be reduced, leading to a significant reduction in risk. Human reliability tools exist to allow you to model these effects in order to identify those factors that have most impact on the likelihood of error.

8.2.10 Competence

X. If you are delivering a system or product, you should make sure that the people estimating risk collectively have sufficient knowledge and expertise to do the work competently.

Estimating risk requires knowledge and expertise in both:

- the system or product, including its function and design; and
- the operational environment in which the system or product will run.

Typically, the former is held by the system or product supplier and the latter is held by the organization that will use the system or product.

The person or persons leading the estimation should have received training in ESM or have had experience of successfully delivering a program of ESM activities or both. They should also have received training in the estimation techniques employed or have had experience of successfully applying them or both.

For further guidance on competence management, see chapter 21.

© Abbott Risk Consulting Ltd. 2022

8.3 Sources of further guidance

Chapter 4 provides guidance on understanding a system or product and its interactions with its operational environment.

Section 7.2.3 provides guidance on preliminary hazard analysis.

Chapter 10 describes how the results of risk estimation are used to reach a decision on whether risk is acceptable or not

Chapter 15 provides guidance on monitoring risk.

Chapter 12 provides guidance on cross-acceptance.

Chapter 16 provides guidance on maintaining a Hazard Log, which will act as a repository for risk estimation data, and on managing assumptions.

Chapter 20 provides guidance on promoting a safety culture.

Chapter 21 provides further guidance on competence management.

iESM Application Note 3 describes some relevant techniques. '*Hazard Analysis Techniques for System Safety*' [Ericson] provides further description of some of these techniques plus description of additional relevant techniques.

EN 50129 [50129] provides a comprehensive bibliography of safety analysis techniques, including techniques which are useful for hazard identification.

European Union Commission Regulation (EU) No 402/2013 on the Common Safety Method (CSM) for Risk Assessment and Evaluation [CSM-RA] and its guidance

'*Risk – A Missed Opportunity?*' [Hessami] describes techniques for balancing safety with factors in broader decision making.

'*Incorporating Human Dependent Failures in Risk estimations to Improve Estimates of Actual Risk*' [Hollywell] provides information on dependencies between human actions.

"Taking Safe Decisions" [RSSB1] contains guidance on one method of performing quantitative severity calculations.

© Abbott Risk Consulting Ltd. 2022

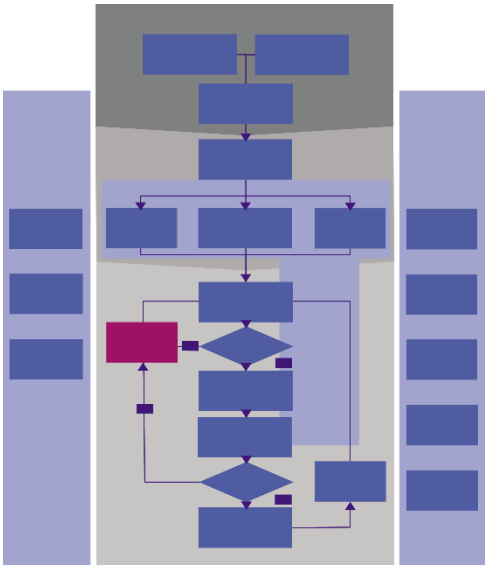
Part IV: Risk Control

© Abbott Risk Consulting Ltd. 2022

9 SETTING SAFETY REQUIREMENTS

9.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. Safety requirements are requirements to put in place measures to control risk. They will be derived from the safety obligations and targets established at the outset of the process. Some safety requirements will be derived directly from the safety obligations; other safety requirements will arise from the **Evaluating risk** activity and will be formulated in order to reduce risk to an acceptable level.



Your organization must set safety requirements which are sufficient to meet its safety obligations and targets.

Safety requirements may specify:

- specific functions or features of a railway product or a part of the railway;
- features of design and build processes;
- actions to control risk;
- features of maintenance or operation practices; and
- tolerances within which something must be maintained.

You may have requirements at different levels of detail. For example, you may set overall targets for risk within your area of responsibility and then define detailed technical requirements for individual pieces of equipment.

You should make sure that your safety requirements are realistic, clear, comprehensive and accurate and that you can confirm that they have been met.

© Abbott Risk Consulting Ltd. 2022

Some of the ways people behave and some of the reasons for their errors are understood. Writers such as James Reason [Reason], for instance, draw a distinction between deliberate violations of rules, mistakes (which are the result of erroneous reasoning) and simple slips and lapses. Some ways of preventing or controlling these errors are known. You should consider setting safety requirements to help people avoid errors.

For the purposes of this activity, a 'safety requirement' is any written commitment to implement a control measure whose completion is tracked. It does not matter what these commitments are called. An action in a Hazard Log may serve the function of a safety requirement.

9.2 Guidance

9.2.1 Introduction to the guidance

The activity of establishing safety requirements follows and builds on the **Determining safety obligations, targets and objectives** activity described in chapter 5 and the **Evaluating risk** activity described in chapter 10. This activity consolidates information from the other two activities into specific requirements, which will, if complied with, ensure that the safety obligations, targets and objectives will be met and that risk will be controlled to an acceptable level. Safety requirements provide the basis against which the safety of the system is tested and assessed.

This chapter is written for people writing or reviewing safety requirements.

Guidance is structured under the following checklist items:

A. If you are developing a system or product, you should establish safety requirements for it which are sufficient to meet your safety obligations, objectives and targets.
B. If you are formulating safety requirements, you should follow good practice in writing requirements.
C. If you are formulating safety requirements, you should consider setting requirements to reduce the chance of a hazardous error being made when the system or product is built, installed or commissioned.
D. If you are formulating safety requirements, you should ensure that they are kept up-to-date.
E. If you developing a system or product, you should establish safety requirements for its safety integrity.
F. If you are delivering a system or product which contains software, you should establish safety requirements for the functionality and integrity of the software.
G. If you are delivering a system or product which contains complex components you should take steps to control the risk of systematic failures within these components.
H. If you are formulating safety requirements, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

9.2.2 Types of safety requirement

Safety requirements may be divided into categories in a number of different ways.

Firstly, safety requirements may be quantitative or qualitative.

Secondly, EN 50126 [50126] draws a distinction between three types of safety requirement:

- **Functional requirements**: which are requirements to perform functions that are fundamental to the system or product, including associated requirements on reliability and other attributes of the performance of these functions

© Abbott Risk Consulting Ltd. 2022

- **Contextual requirements**, which concern the relation between the system and its operational environment
- **Technical requirements**, requirements which derive from the way in which the system is built.

It may also be useful to categorize requirements according to the aspect of the system or product which they constrain. EN 50126 requires that requirements should be set in the following areas:

- functional requirements and supporting performance requirements, including safety;
- functional requirements and safety integrity requirements for each safety-related function;
- logistic support requirements;
- interfaces;
- operational environment and mission profile;
- tolerable risk levels for the consequences arising from the identified hazards;
- external measures necessary to achieve the requirements;
- system support requirements;
- details of the limits of the analysis;
- details of any assumptions made;
- identification of technology related standards;
- scope of diagnosis and monitoring.

In some areas, such as software, where systematic failure is a particular issue, good engineering practice for meeting integrity requirements is to use Safety Integrity Levels (SILs). SILs are described below.

9.2.3 General guidance

A. If you are developing a system or product, you should establish safety requirements for it which are sufficient to meet your safety obligations, objectives and targets.

Safety obligations, objectives and targets are discussed in chapter 5.

A safety requirement should be a specific and testable requirement on the system or product. Any requirement on the system or product that is necessary to close a hazard or otherwise to reduce risk to an acceptable level should be incorporated as a safety requirement.

In some cases, safety obligations, objectives and targets may be transcribed directly as safety requirements. For example an obligation to comply with a standard may give rise directly to one or more requirements.

In other cases, requirements may be derived from the obligations, objectives and targets.

One case where this is necessary is where numerical targets are set for the maximum level of risk. Safety requirements may be set on the occurrence of hazards and failures that may contribute to the hazards.

If you set numerical safety targets, this is normally done by working from a fault tree (or similar representation of cause and effect logic) and the event probabilities to:

A. derive numerical accident targets which conform to legal criteria for acceptable risk;
B. derive hazard occurrence rate and/or unavailability targets which are consistent with (A);

© Abbott Risk Consulting Ltd. 2022

C. if applicable, relate hazards to system functions and derive SILs for the system functions that are consistent with (B).

The targets may be apportioned further to failures of sub-systems of the hierarchy and aligned with the system design. In general, targets for systematic failure should not be set below sub-system function level. Refer to IEC 61508 [61508] or EN 50126 [50126] for further guidance on this decomposition.

You should always consider safety requirements across the life of the system or product. You should check that your safety requirements are sufficient to ensure that it is practical to maintain the system or product in a safe state and to maintain and operate it safely. You may need to set maintainability requirements on the design and/or requirements on the provision of maintenance resources, such as procedures, test equipment, training and spares.

It is generally a good idea to co-ordinate the setting of safety requirements with the setting of requirements on operability and maintainability such as application conditions.

Safety requirements arising from human factors analysis should be integrated with other safety requirements.

B. If you are formulating safety requirements, you should follow good practice in writing requirements.

In any safety requirements specification, and indeed in any well-written specification of any sort:

- Every requirement should be unambiguous, that is admitting only one possible interpretation.
- The requirements should be complete. It should include all the customers' and other stakeholders' requirements and those required by the context (standards, legislation and so on). Each requirement should be stated in full and any constraints or process requirements that affect the design should be completely specified. The requirements should define both what the system must do, and what it must not do.
- The requirements should be correct: they should correctly reflect what the stakeholders need.
- The requirements should be consistent. There should be no conflict between any requirements in it, or between its requirements and those of applicable standards.
- Every requirement should be capable of being validated. There should be some process by it can be checked that the requirement has been met.

When you set a requirement, it is a good idea to define acceptance criteria for it, that is criteria on the successful performance of test, inspections and analyses which will be sufficient to conclude that the requirement has been met.

- The specification should be modifiable. Its structure and style should be such that any necessary changes to the requirements can be made easily, completely and consistently in a controlled and traceable manner.
- Every requirement should be traceable. Its origin should be clear and it should have a unique identifier so that it can be referred to.

In addition, safety requirements should reflect the safety obligations, targets and objectives such that any system that meets the requirements will meet the safety obligations, targets and objectives. You should verify that this is the case and document the evidence for believing that this is the case.

It is acceptable to maintain some safety requirements as actions in a Hazard Log provided that they are expressed precisely and treated as requirements.

© Abbott Risk Consulting Ltd. 2022

C. If you are formulating safety requirements, you should consider setting requirements to reduce the chance of a hazardous error being made when the system or product is built, installed or commissioned.

Measures which may reduce the chance of a hazardous error being made when the system or product is built, installed or commissioned include:

- Ensuring that elements of the system or product are clearly labeled;
- Designing self-test facilities capable of detecting errors; and
- Designing items such that some assembly errors are impossible, for instance, using cables that have connectors shaped so that they cannot be inserted into the wrong socket or the wrong way around.

D. If you are formulating safety requirements, you should ensure that they are kept up-to-date.

The activity of establishing requirements in general, and safety requirements in particular, is iterative. As further analysis or further design work reveals the need for different or additional safety requirements, the requirements should be updated.

9.2.4 Safety integrity

In section 2.1, we drew a distinction between random and systematic failures.

There are well-established techniques for assessing and controlling the risk arising from random failures. The risk arising from systematic failures is controlled in many engineering activities through rigorous checking and the application of standards, codes and accepted good practice.

However, as the complexity of designs increases, Systematic failures contribute a larger proportion of the risk. For software, all failures are systematic. In software and some other areas where designs may be particularly complex, such as electronic design, current best practice is to make use of Safety Integrity Levels (SILs) to control systematic failures.

SILs are described in a number of widely-used standards, including EN 50126 [50126], EN 50128 [50128], EN 50657 [50657] and IEC 61508 [61508] and we recommend defining SILs for systems or parts of systems for which the guidance on SILs in such standards is applicable. Otherwise, we recommend that you should use other means, such as rigorous checking, to control the risk arising from systematic failure.

Even in complex systems, SILs are not the only means of controlling systematic failures; they may be controlled through architectural design features as well.

SILs represent different levels of rigor in the development process and are related to approximate probability targets. Five levels of integrity are defined in EN 50128 [50128], ranging from SIL 4, the most stringent, to SIL 0, the least stringent. Below SIL 0 no SIL is required, meaning that the function is not relied upon to control risk at all and so no conceivable failure of the function could ever be blamed for any harm.

© Abbott Risk Consulting Ltd. 2022

Four levels of integrity are defined in EN 50126 [50126-2], EN 50129 [50129] and EN 50657 [50657] ranging from SIL 4 to SIL 1 with a level of "basic integrity" defined below (less dependable than) that. Basic integrity is either not relied upon to control risk or the contribution that failure of the function could make to risk is so indirect that a failure rate above 10^{*-5} per hour would be tolerable.

Functions which are not relied upon at all to control risk have no SIL. This is where the Tolerable Functional Failure Rate (TFFR) is less demanding (more frequent) than 10^{-5} per hour. Each level is populated with increasingly stringent processes and techniques as the integrity requirement increases. Note that the processes and techniques for basic integrity in EN 50657 [50657] are reduced compared with those for SIL0 in EN 50128 [50128].

Each integrity level is associated with a target rate of occurrence of failure, although there is no causal connection. One widely accepted association is shown in
Table 9-1, which is derived from EN 50129 [50129].

The TFFR may be a specified target or may be derived from a THR by identifying the functional failure associated with the hazard (if there is one). For each hazard with related quantitative target, the quantitative safety integrity requirement (the THR) is allocated to the function that protects against that hazard (the TFFR). Beware however that the relationship may not be one-to-one as hazards may result from a combination of functional failures (or none at all). In such cases, the THR shall be apportioned and converted to TFFR for each of the functions. An example analysis is shown in EN50129 [50129] Appendix A4.5.

Note that TFFR is a rate. In the event of a probability on demand being specified it needs to be changed into an appropriate continuous demand equivalent.

Tolerable Functional Failure Rate (TFFR) (per hour)	Safety Integrity Level
10^{-9} … 10^{-8}	4
10^{-8} … 10^{-7}	3
10^{-7} … 10^{-6}	2
10^{-6} … 10^{-5}	1
>=10^{-5}	0 / Basic Integrity

Table 9-1 Safety Integrity Levels

EN 50129 [50129] provides guidance for safety-related functions having quantitative requirements more demanding (lower) than 10^{-9} per hour, but this is seldom (if ever) useful for railway projects.

Target probabilities of failure for systematic functions should be set to achieve an acceptable level of risk for the overall system.

A system will generally take the maximum SIL of all the functions that it implements.

SILs for the functions of a sub-system may generally be set according to the target rates of failures of the system and this may allow some sub-systems to be provided a lower SIL than that of the overall system. However, EN 50126 [50126] recommends restrictions on assigning a lower SIL to sub-systems in the case where the functions of two sub-systems control the same hazard and there is some interaction between the two functions.

© Abbott Risk Consulting Ltd. 2022

It is very difficult to prove functional independence within a sub-system and so it is important to take care in assigning functions to sub-systems. If possible, functions with differing SILs should be segregated either physically or logically.
Practitioners have successfully justified designs with software functions of different SIL on the same processor, although EN 50126 does not provide any support for this practice. To be able to use software functions of varying SIL on the same processor, you must be able to produce a safety argument that demonstrates that the lower SIL functions cannot influence the behavior of those with higher SILs. This may be through mechanisms that prevent interference such as memory protection or shown by analysis of the code, for example by demonstrating that no part of the code will write to memory outside of its designated area. However, this can be difficult to do, and the effort required may be excessive compared with other solutions to the same problem.

E. If you are developing a system or product, you should establish safety requirements for its safety integrity.

You should establish requirements for safety integrity for the system or product and significant sub-systems using a recognized process such as that described above, setting requirements for the safety integrity of the functions of the system, product or sub-system first and then establishing the safety integrity of the system, product or sub-system itself.

Once the SIL for a sub-system has been established, then appropriate techniques to develop the sub-system to that level can be established by reference to tables in standards, including EN 50126 and IEC 61508.

9.2.5 Software safety requirements

This guidance is applicable to any railway system containing software, including embedded systems such as programmable logic controllers.

F. If you are delivering a system or product which contains software, you should establish safety requirements for the functionality and integrity of the software.

For programmable systems, it is normal to derive a Software Requirements Specification (although other titles may be used). This should define the functions that the software must perform which, taken together with the capabilities of the hardware, will allow the overall system to meet its requirements.

In just the same way as safety requirements are set at the system level and form part of the overall system requirements, it is usual to establish a Software Safety Requirements Specification, either as a subset of the Software Requirements Specification or as a separate document.

The software safety requirements will normally include requirements for features which can tolerate faults, as well as requirements for dependability of the software. EN 50128 [50128] and EN 50657 [50657] provide guidance on fault-tolerant features.

© Abbott Risk Consulting Ltd. 2022

All software failures are systematic. Software does not wear out or break. Most software failures are the result of errors in the software which themselves result from failures in the development process, such as incorrect specification (for instance specifying the wrong behavior in the event of an error), or a mistake when implementing this specification.

Generally speaking, if a system includes software, then the Safety Integrity of the system will depend upon the Safety Integrity of the software. Dependability should be treated by specifying the SIL of the software. This will be the same as the SIL for the system unless it has been explicitly apportioned as described in the previous section.

Guidance on the development of software for safety-related railway applications can be found in EN 50128 [50128] for control and protection systems and EN 50657 [50657] for on-board rolling stock systems, which also describe techniques appropriate to each SIL.

EN 50128 [50128] and EN 50657 [50657] require that software safety requirements be included within Software Requirements Specification.

The software safety requirements will play a pivotal role in demonstrating the safety of the system or product. You will need to show that:

- the software safety requirements are sufficient; and
- the software meets its software safety requirements.

To support this, the software safety requirements must be complete, precise, and intelligible to both those developing the software and those applying it. It is also desirable for other software requirements to have these attributes.

There is no consensus within the software engineering community on methods of predicting the probability of software failures or even whether it is valid to assign a probability to these failures at all.

EN 50128 [50128] and EN 50657 [50657] provide no method for estimating the probability of software failure. The practice of using the worst-case probability associated with the SIL of the software is not supported by the standard. We do not endorse this practice, although we do not consider it to be a completely unreasonable approach as the requirements of the standard would be open to challenge if they routinely resulted in software that failed more often than this limit.

Without estimating the probability of software failure it is not possible to estimate the probability of failure of a system containing software. It is possible, however, to estimate the probability of system failure from non-software causes and to present this figure, carefully explained, together with the SILs of the system function in the safety report. If you are using fault trees, the probability of system failure from non-software causes can be calculated by setting the probabilities of software failure to zero, although it must be understood that this is a device for excluding software failure from the calculation, not an assumption that software does not fail.[3]

[3] Be careful however if the software includes functions that protect against other hazard causes. Setting the probability of failure of such functions to zero can result in a zero estimate for the probability of the hazard. In these circumstances you may need to provide probabilities for nodes in the fault tree below the top event, if you are to provide the reader with useful information.

© Abbott Risk Consulting Ltd. 2022

9.2.6 Requirements for the integrity of complex, non-software components

Although safety integrity levels are often associated with software, they are also applicable to non-software components with significant complexity, such as some electronic components, where this complexity requires that steps be taken to control the risk of systematic failures.

G. If you are delivering a system or product which contains complex components you should take steps to control the risk of systematic failures within these components.

These steps may include additional analysis, testing and review.

It may be useful to define a SIL for a complex components. EN 50126 [50126] provides guidance on the design of electronic sub-systems at different SILs.

9.2.7 Requirements for the integrity of software tools

For all but the simplest software systems the use of tools to develop and test software will be necessary. EN 50128 [50128] and EN 50657 [50657] classifies them into three groups:

- T1 tools generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software (e.g. a text editor).
- T2 tools help to test or verify the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software (e.g. a static analysis tool)
- T3 tools generate outputs which can directly or indirectly contribute to the executable code (including data) of a safety related system (e.g. a compiler)

H. If you are delivering a system or product which relies on software tools their selection should be justified and they should form part of the safety justification for that system or product.

For those tools that affect safety EN 50129 [50129] states that one of the following shall be done:

- verification of the output from the tool through a combination of tests, analyses and checks;
- a proven in use claim made with sufficient evidence to show that the tool can be trusted;
- proving of the tool by analysis and testing;
- use of tool diversity
- evidence that the tool has been designed, implemented and validated to achieve the safety integrity level needed for the application

9.2.8 Competence

I. If you are formulating safety requirements, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

The person or persons writing the safety requirements should have received training in ESM or have had experience of successfully delivering a program of ESM activities or both. They should also have received training in writing requirements or have had experience of writing good quality requirements, or both.

© Abbott Risk Consulting Ltd. 2022

For further guidance on competence management, see chapter 21.

9.3 Sources of further guidance

Section 2.1 provides definitions of random and systematic failures

Chapter 5 provides guidance on determining safety obligations, targets and objectives.

Chapter 10 provides guidance on evaluating risk.

iESM Application Note AN8 provides more detailed guidance on accounting for human factors within ESM

IEC 61508 [61508], EN 50126 [50126], EN 50128 [50128] and EN 50657 [50657] provide guidance on setting and meeting requirements on safety integrity.

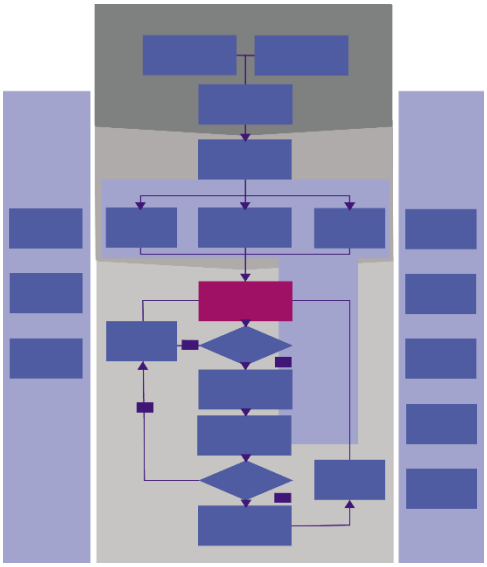
IEC 61508 [61508] provides guidance on setting and meeting software safety requirements in general.

© Abbott Risk Consulting Ltd. 2022

10 EVALUATING RISK

10.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. This activity involves applying the risk acceptance criteria established when carrying out the **Establishing safety obligations** activity to the estimated risk and concluding whether or not it can be accepted.



Your organization must evaluate the risk associated with each of its systems or products against the criteria for safety that it is obliged to use. If the risk associated with a system or product cannot be reduced to an acceptable level, then it must be abandoned.

This activity may come to one of the following conclusions:

1. The risk can be accepted as it is (the "OK" arrow on the diagram); or
2. The risk requires reduction (the "Not OK" arrow on the diagram); or
3. The risk cannot be accepted and cannot be reduced to an acceptable level and the system or product must be abandoned (this is a rare situation and not shown on the diagram).

If you need to reduce risk then, in order of priority, you should look for opportunities to:

1. Eliminate the hazard;
2. Make the hazard less likely to occur, for example by eliminating causes of the hazard;
3. Replace the hazard with something less hazardous;
4. Move the hazard away from the people who might be harmed;
5. Introduce technical measures to make the hazard less likely to result in harm to people or to limit that harm; or
6. Introduce procedures to make the hazard less likely to result in harm to people or to limit that harm.

When searching for measures to reduce risk, you should bear in mind that safety is highly dependent on how well people and equipment do their job. You should avoid relying completely for safety on any one person or piece of equipment.

© Abbott Risk Consulting Ltd. 2022

You should look for ways of controlling hazards introduced by your work as well as hazards that are already present in the railway. Even if your work is designed to make the railway safer, you should still look for measures you could take to improve safety even further.

10.2 Guidance

10.2.1 Introduction to the guidance

Risk evaluation is the process of taking an estimation of risk (see chapter 8) and deciding whether the risk may be accepted or not. If it cannot be accepted then additional control measures are introduced until the risk becomes acceptable.

A final evaluation of risk cannot be performed until the system is built and ready to enter service but provisional risk evaluation is performed from the point at which the system starts to be specified in order to provide feedback on whether the current specification and design will lead to acceptable risk. When the design is stable, it may be possible to reach a conditional evaluation that the risk will be acceptable provided that there is no departure from plan and that a list of other conditions are met, in which case, the final evaluation of risk may be restricted to confirming that these conditions are in fact met.

Three methods of estimating risk were defined in previous chapters:

- Applying standards;
- Comparison with a reference system; or
- Explicit estimation of the severity and likelihood of accidents.

If the first method is being used then the evaluation of risk just requires confirmation that the risk is in fact covered by the standards and that the standards have been applied. In the other cases, the results of risk estimation will need to be considered in the light of the safety obligations, objectives and targets (see chapter 5) to see whether these obligations, objectives and targets have been met.

This chapter is written for anyone responsible for deciding whether the risk associated with a system or product is acceptable and anyone reviewing such a decision.

Guidance is structured under the following checklist items:

A. If you are estimating risk by applying standards, you should check that the risk is covered by the standards and that the standards have been applied before accepting it.
B. If you are estimating risk by comparison with a reference system, you should check that comparison shows that your system or product is consistent with your safety obligations, targets and objectives before accepting the risk.
C. If you performing explicit estimation of the risk, you should check that the estimation of risk is consistent with your safety obligations, targets and objectives before accepting the risk.
D. If you find that risk is unacceptable or that there is doubt about whether risk is acceptable or not, you should take action to rectify the situation.
E. If you are estimating risk, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

© Abbott Risk Consulting Ltd. 2022

10.2.2 Risk evaluation when the risk is covered by standards

A. If you are estimating risk by applying standards, you should check that the risk is covered by the standards and that the standards have been applied before accepting it.

This will normally have been checked during risk estimation and so can be double-checked by reviewing the documentation produced by risk estimation.

10.2.3 Risk evaluation by comparison with a reference system

B. If you are estimating risk by comparison with a reference system, you should check that comparison shows that your system or product is consistent with your safety obligations, targets and objectives before accepting the risk.

You should confirm that the risk associated with the reference systems is consistent with your safety obligations, targets and objectives and that the differences between the reference system and your system or product have not introduced unacceptable risk.

10.2.4 Risk evaluation when performing explicit estimation of risk

C. If you are performing explicit estimation of the risk, you should check that the estimation of risk is consistent with your safety obligations, targets and objectives before accepting the risk.

The precise manner in which you will do this will depend upon your safety obligations, targets and objectives.

If these include numerical targets for the maximum acceptable risk then you will compare the estimate risk with these targets.

Risk evaluation generally requires an element of expert judgment. When risk evaluation relies on expert judgment, there should documented consensus from a group of experts whose knowledge covers both the system or product and the operational environment in which it is being applied and who share a common understanding of the evaluation process.

10.2.5 The 'Precautionary Principle'

D. If you find that risk is unacceptable or that there is doubt about whether risk is acceptable or not, you should take action to rectify the situation.

In evaluating risk, you should take account of the fact that all estimates of risk are uncertain. You should consider whether this uncertainty casts doubt on whether the targets have been met.

It is good practice to follow the 'Precautionary Principle', which requires that uncertainty over risk should not prevent action from being taken. If there is doubt over whether risk is acceptable or not, you should initiate action, either to reduce the uncertainty in the estimates or to reduce the risk.

© Abbott Risk Consulting Ltd. 2022

If you need to reduce risk then, in order of priority, you should look for opportunities to:

1. Eliminate the hazard;
2. Make the hazard less likely to occur, for example by eliminating causes of the hazard;
3. Replace whatever is causing the hazard with something less hazardous;
4. Move the hazard away from the people who might be harmed;
5. Introduce technical measures to make the hazard less likely to result in harm to people or to limit that harm; or
6. Introduce procedures to make the hazard less likely to result in harm to people or to limit that harm.

EN 50126 [50126] describes a number of design strategies which may be used to control risk.

Some actions to control risk may be taken by the system or product supplier alone but other actions may require co-operation with other parties, such as the system's or product's operator or maintainer, or may be taken entirely by other parties.

These actions should be agreed between the parties. EN 50126 [50126] provides guidance on the division of responsibilities between the parties involved in procuring a new system
or product.

10.3 Sources of further guidance

Chapter 5 provides guidance on establishing safety obligations, objectives and targets.

Chapter 8 provides guidance on estimating risk.

EN 50126 [50126] describes design strategies which may be used to control risk and provides guidance on the division of responsibilities between the parties involved in procuring a new system or product.

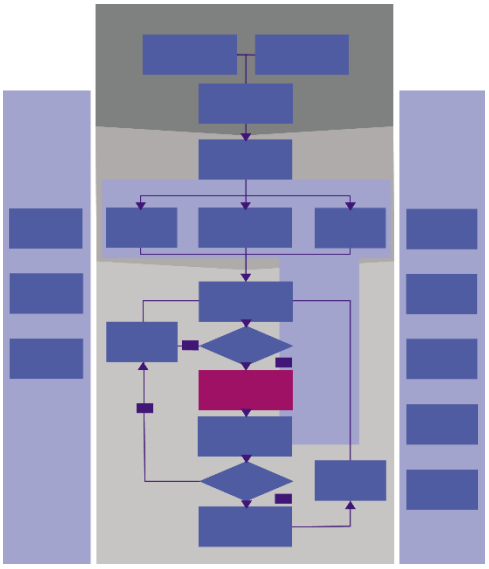
The European Commission Regulation on the adoption of a Common Safety Method on Risk Evaluation and Assessment [CSM-RA] sets mandatory requirements on methods of evaluating risk. These requirements are only applicable within the European Union. However, the requirements are consistent with the approach described in this handbook and may be a useful source of guidance to readers who are not required to follow them.

© Abbott Risk Consulting Ltd. 2022

11 IMPLEMENTING AND VALIDATING CONTROL MEASURES

11.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. This activity involves implementing the control measures defined in the previous activity and confirming that they have been implemented and that the safety requirements set in the previous section have been met.



Your organization must design its systems or products to meet its safety requirements and all control measures must be implemented.

The control measures will be implemented and validated as an integral part of the implementation and validation of the system or product as a whole, using the methods appropriate to the technology being used.

The continued effectiveness of the control measures will be continually revalidated as part of the **Monitoring risk** activity described below.

© Abbott Risk Consulting Ltd. 2022

11.2 Guidance

11.2.1 Introduction to the guidance

The previous steps in the process are essential parts of their process but they are theoretical and, on their own, will have no effect on safety. It is the implementation of control measures which will reduce risk to an acceptable level. The validation that these control measures have been correctly implemented is essential if assurance that risk has been reduced to an acceptable level is to be provided.

This chapter is written for anyone responsible for implementing or validating control measures or for reviewing the results of these activities.

Guidance is structured under the following checklist items:

A. If you are developing a system or product, you should design it to implement all control measures and comply with all safety requirements.
B. If you intend to bring a system or product into interim use before all the control measures for final use are implemented and validated then you should introduce temporary control measures.
C. If you are developing a system or product, you should verify that the design implements all control measures and all safety requirements.
D. If you are developing a system or product, you should validate that all control measures and all safety requirements have been implemented in the final system or product.

11.2.2 Implementing control measures

A. If you are developing a system or product, you should design it to implement all control measures and comply with all safety requirements.

You should make sure that the designers are given the details of all control measures and all safety requirements and are informed that a decision has been taken to implement them.

Control measures will generally require that the system or product should perform specified functions or contain certain design features. Safety requirement may also require these things but they may also require:

- specified levels of safety integrity, that is that the likelihood that the system or product will malfunction hazardously is sufficiently low; or
- resilience, that is that the system or product will continue to avoid hazards even in the presence of failures or external influences.

Integrity requirements may be specified in terms of maximum probabilities of rates of hazardous failure or in terms of Safety Integrity Levels (SILs) as described in section 9.2.4.

Some safety requirements may be met by removing the source of a hazard. For example, a requirement to avoid electrocution hazards may be met by ensuring that lethal voltages are not present in the system.

© Abbott Risk Consulting Ltd. 2022

Integrity and resilience requirements may also be achieved by including architectural design features such as:

- designing a system to be fail-safe, so that certain types of failure will always leave the system in a safe state;
- ensuring that a safety-related function can be performed by more than one sub-system so that, if one sub-system fails, the other can take over; or
- having one sub-system check for hazardous behavior in another sub-system so that it can intervene, if necessary, in order to prevent hazards.

These architectural design features will generally increase the complexity of the system and so will increase the number of failure modes that it can exhibit. This will make it harder to analyze all failure modes and to provide assurance that the design is safe. The benefits of these features will not always outweigh the disadvantages of increased complexity; a balance must be struck between the two.

EN 50126 [50126] provides guidance on architectural design features including guidance on establishing sufficient evidence between functions where this is relied upon to deliver sufficient safety integrity.

B. If you intend to bring a system or product into interim use before all the control measures for final use are implemented and validated then you should introduce temporary control measures.

A system or product may be brought into use before all the control measures for final use are implemented and validated for trials, which may form part of the validation of the control measures, or to meet an urgent operational need.

In this case, you should introduce temporary control measures, which may include temporary restrictions upon the way in which the system or product may be operated until all the control measures for final use are implemented and validated in order to ensure that risk during this initial period of use is acceptable.

11.2.3 Verifying that control measures have been included in the design

C. If you are developing a system or product, you should verify that the design implements all control measures and all safety requirements.

Some of the techniques which were introduced in chapter 7 and chapter 8 for hazard identification and risk estimation may also be used for this purpose. In particular Fault Tree Analysis and Failure Modes, Effects and Analysis (FMEA) may be used to show that there are no single points of failure or to show that the probability of certain hazards is below a specified threshold.

Further information on Fault Tree Analysis and FMEA is provided in iESM Application Note 3 and in EN 50126 [50126].

Other techniques that may be used to identify and remove hazardous design flaws include:

- **Design analysis,** which is used to look at constraints, internal or external interactions, and the logic flow within a design.
- **Sneak circuit analysis**, which is used to look for interactions between parts of the system or between the system and other things which might lead to unexpected and hazardous behavior.

Further information on Design Analysis and Sneak circuit analysis is provided in EN 50126 [50126].

© Abbott Risk Consulting Ltd. 2022

11.2.4 Validating that control measures have been implemented

D. If you are developing a system or product, you should validate that all control measures and all safety requirements have been implemented in the final system or product.

Validation may be achieved by inspecting, testing or analyzing the final system or product or by some combination of these.

You should decide how you will validate a control measure of safety requirement when you specify it. As stated in section 9.2.3, it is a good idea when you specify a safety requirement, to specify 'acceptance criteria' for it, that is, criteria on the inspection, test or analysis of the system or product which will allow you to conclude that the requirement has been met. Specifying acceptance criteria will make the validation process more efficient and may also reveal flaws in the requirement which can be corrected before they cause problems.

After the requirements definition phase EN 50126 [50126-2] allows for those responsible for validation to report to the project manager if the function to be validated has been identified as SIL2 or lower or if no fatality can arise from a credible accident. We cannot see any safety or commercial advantage to this and recommend that validation is always performed independently of the line management.

11.3 Sources of further guidance

Chapter 7 provides guidance on identifying hazards.

Chapter 8 provides guidance on estimating risk.

Chapter 9 provides guidance on safety integrity levels and defining acceptance criteria.

iESM Application Note 3 provides further guidance on Fault Tree Analysis, and FMEA.

EN 50126 [50126] and IEC 61508 [61508] provide guidance on complying with SILs.

EN 50126 [50126] provides further guidance on Fault Tree Analysis, FMEA, Design Analysis and Sneak Circuit Analysis.

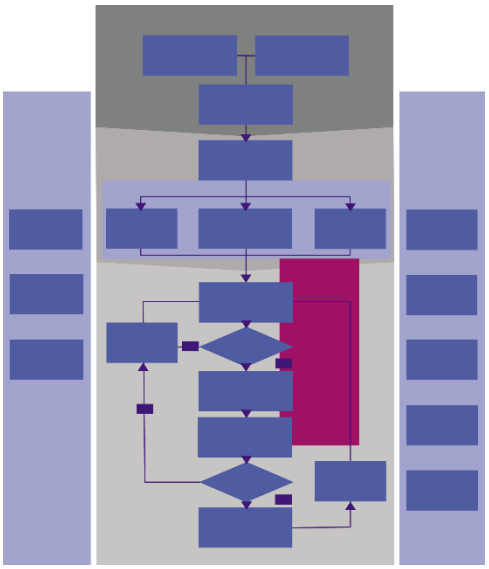
© Abbott Risk Consulting Ltd. 2022

12 PREPARING A CROSS-ACCEPTANCE ARGUMENT

12.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. For some products, some of the evidence for the safety of their application may derive from the approval of a similar product in a similar operational environment. It is common to refer to the application that has already been approved as the **native** application and to refer to the new application as the **target** application.

By **cross acceptance,** we mean using the approval to bring the native application into service directly as part of the evidence for the safety of the target application rather than reusing the detailed evidence behind the original acceptance. It is also possible, and often sensible, when performing ESM on one project to reuse and adapt work done on a previous project but that is better considered as part of other ESM activities such as **Identifying hazards** or **Estimating risk.**



Where a similar product has been found safe in a similar operational environment and approved for use in that operational environment, your organization may use that approval as evidence for the safety of new products and new applications of products but it must identify and allow for the differences between the products and between their operational environments.

If the native and target products and their operational environments are similar and the safety of the native application has been established to the satisfaction of a reputable authority then you may use the approval for that native product as part of the evidence for the target product. However you should identify all material differences between the native and target products and their operational environment, because each of these differences may mean that the risk associated with the two products is different. Having done this you should establish that none of these differences results in unacceptable risk, using the activities described above.

© Abbott Risk Consulting Ltd. 2022

Cross acceptance offers the possibility of saving time and money by avoiding the repetition of work done before. It should be performed with care as assumptions may have been made about the native product or the way in which it was applied when compiling evidence for the native product which may not be true for the target product or the way in which it is being applied. All these implicit assumptions should be identified and checked.

There is a guide on cross-acceptance associated with EN 50126 [50126] that is numbered PD CLC/TR 50506-1: 2007 [50506] and that provides further useful advice.

12.2 Guidance

12.2.1 Introduction to the guidance

The basic idea behind cross-acceptance is illustrated in Figure 12-1. The target system or product (the yellow rectangle) is the system or product on which ESM is being performed and the objectives of ESM are to ensure and to demonstrate that the risk associated with the target system or product is acceptable, which, in the figure, is indicated by the fact that the yellow rectangle is below the acceptable threshold.

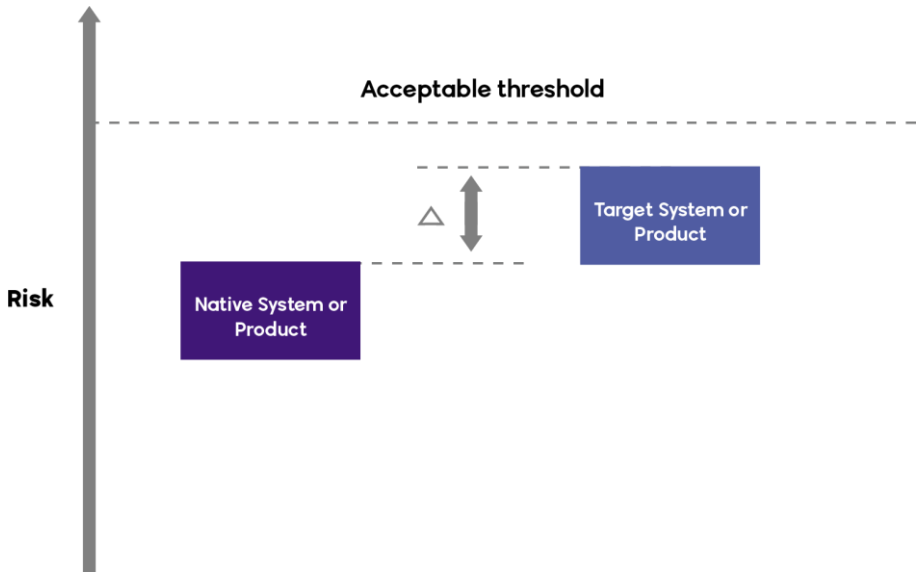


Figure 12-1: Cross Acceptance

Normally ESM is performed by considering the target system or product on its own. Cross acceptance involves considering another system or product which is known to be associated with acceptable risk (indicated by the blue rectangle on the figure), considering the differences between the two systems, including any differences between their operational environments and applications (indicated by Δ on the figure) and showing that these differences do not change level of risk associated with the target system in a way that could make it unacceptable.

Cross acceptance may allow the safety of a system or product to be ensured and demonstrated with lower cost than working from first principles but this is not necessarily the case – the effort involved in identifying and analyzing the differences between two systems is significant and, in some cases, cross acceptance may take more effort than working from first principles. Cross acceptance should not generally be attempted unless the differences between the native and target systems or products are small.

© Abbott Risk Consulting Ltd. 2022

Moreover, cross acceptance relies upon accurate, comprehensive information about the way in which the native product and system has been used and, in some case, its performance. If this information is unavailable, cross acceptance will not be possible.

If you use cross acceptance, you will still need to perform all the other ESM activities but will affect what is done when performing the **Identifying hazards, Estimating risk, Setting safety requirements, Evaluating risk, Implementing and validating control measures** and **Compiling evidence of safety** activities.

Internationally agreed guidance on cross acceptance is published by IEC in a technical report, CLC/TR 50506-1 [50506]. The guidance in this section is generally in line with CLC/TR 50506-1 but does follow current practice in allowing cross acceptance between two specific systems, where CLC/TR 50506-1 only provides for cross acceptance of generic products and generic applications of a product.

CLC/TR 5056-1 uses the following sequence of steps as a framework for providing guidance:

1. Establish a credible case for the native (baseline) application
2. Specify the target operational environment and application
3. Identify the key differences between the target and native cases
4. Specify the technical, operational and procedural adaptations required to cater for the differences
5. Assess the risks arising from the differences
6. Produce a credible case for the adaptations adequately controlling the risks arising from the differences
7. Develop a generic or specific cross-acceptance case

This chapter is written for anyone considering embarking on cross acceptance.

Guidance is structured under the following checklist items:

A. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should establish that the native system or product meets the risk acceptance criteria applicable to the target system or product.
B. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should establish the differences between the systems or products and between their operational environments.
C. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should analyze the differences between the two.
D. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should compile evidence that the cross acceptance process has been carried out satisfactorily and that risk has been controlled to an acceptable level.
E. If you are compiling evidence of safety in order to seek cross acceptance, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

The relationship between these checklists items and the steps in the CLC/TR 50506-1 framework is as follows:

- Item A covers step 1.
- Item B covers steps 2, 3 and 4.
- Item C covers step 5.
- Item D covers steps 6 and 7.

© Abbott Risk Consulting Ltd. 2022

12.2.2 Establishing the safety of the native system or product

A. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should establish that the native system or product meets the risk acceptance criteria applicable to the target system or product.

This is normally done by establishing that the native system or product has been accepted for use by a recognized authority using risk acceptance criteria that are the same as or more stringent than those that apply to the target system.

Evidence that such acceptance has been granted is normally sufficient to complete this step.

Where the native system or product has a long service record from which it is possible to argue statistically that it meets the relevant risk acceptance criteria, the service record may be used even if no record of formal acceptance against the criteria is available.

12.2.3 Establishing the differences between the native and target systems or products

B. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should establish the differences between the systems or products and between their operational environments.

Differences between the systems or products will include any differences in construction and functionality, including any differences in software.

Differences between the operational environments will include differences in:

- Interfaces and in other systems with which the target system or product interfaces;
- Operating and maintenance practices;
- Environmental conditions, such as temperature and humidity; and
- The patterns of usage of the systems or products.

You may need to specify adaptations to operating and maintenance practices in order to cater for the other differences.

12.2.4 Confirming that the differences do not introduce unacceptable risk

C. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should analyze the differences between the two.

You should ensure that the differences between the systems or products and between their operational environments do not cause the risk associated with the target system or product to become unacceptable.

© Abbott Risk Consulting Ltd. 2022

Showing that differences between the systems or products and between their applications do not cause the risk associated with the target system or product to become unacceptable will generally require you to show that the differences do not increase the risk. Some risk acceptance criteria may require more. For example, if you are working in a country where you are obliged to do everything reasonably practicable to reduce risk, you will also need to show that any reasonably practicable opportunities to reduce risk introduced by the differences have been taken.

Performing this step may require you to change the system or product or to introduce new application conditions in order to reduce risk.

To carry out this task, you can use the guidance for the **Identifying hazards, Estimating risk, Setting safety requirements, Evaluating risk** and **Implementing and validating control measures** activities, focusing upon the differences between the systems or products.

D. If you are seeking cross acceptance for a target system or product with reference to a native system or product, you should compile evidence that the cross acceptance process has been carried out satisfactorily and that risk has been controlled to an acceptable level.

The guidance in this handbook on **Compiling evidence of safety** may be used to compile evidence associated with point (C), above, but the technical aspects of this evidence will be restricted to the differences between the native and target systems or products.

This evidence should be supplemented by evidence that points (A) and (B), above, have been satisfactorily completed, including the list of differences between the native and target systems or products.

12.2.5 Competence

E. If you are compiling evidence of safety in order to seek cross acceptance, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

The person or persons compiling evidence of safety in order to seek cross acceptance should have received training in ESM or have had experience of successfully delivering a program of ESM activities or both. They should also be familiar with good practice in preparing cross-acceptance safety arguments.

For further guidance on competence management, see chapter 21.

12.3 Sources of further guidance

Chapter 21 provides further guidance on competence management.

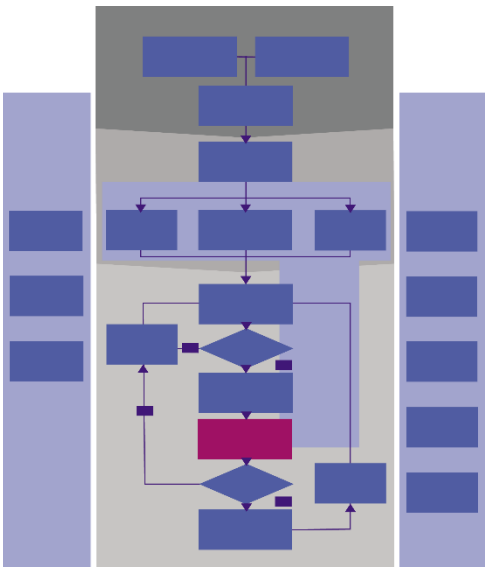
For further guidance on cross acceptance, see CLC/TR 50506-1 [50506].

© Abbott Risk Consulting Ltd. 2022

13 COMPILING EVIDENCE OF SAFETY

13.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. This activity involves compiling evidence of the satisfactory performance of the other activities in order to demonstrate that the system or product is or will be safe.



Your organization must demonstrate that risk has been controlled to an acceptable level. Your organization must support this demonstration with objective evidence, including evidence that all safety requirements have been met.

You should ensure and demonstrate that:

- you have accurately defined the scope of your work and your safety obligations and objectives;
- you have adequately assessed the risk associated with your activities;
- you have set adequate safety requirements and met them;
- you have carried out the ESM activities that you planned;
- all safety-related work has been done by people with the proper skills, experience, awareness and knowledge; and
- there are arrangements in place to make sure that the safety measures that have been implemented remain effective.

If, when compiling evidence of safety, you discover that one of the points above is not completely true, you should revise your estimation of the risk as necessary and take corrective action to ensure that the risk is returned to an acceptable level.

You should confirm that the evidence for your conclusions is reliable. You should record and validate any assumptions and conditions on which your conclusions are based. If you rely on other people to take action to support your conclusions, you should write these actions down. You should do what you reasonably can to make sure that the other people understand what they have to do and confirm that they have accepted responsibility for doing it.

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

© Abbott Risk Consulting Ltd. 2022

13.2 Guidance

13.2.1 Introduction to the guidance

This chapter provides guidance on compiling evidence of safety in most cases. However, chapter 12 provides guidance on 'cross acceptance', that is, using the approval to bring a previous system or product into service directly as part of the evidence for the safety of the target application rather than reusing the detailed evidence behind the original acceptance. If you are using cross acceptance then you should read chapter 12; cross acceptance is not covered in this chapter.

Evidence of safety will generally comprise direct evidence for a number of subordinate claims, for instance that tasks have been satisfactorily performed or that components are of satisfactory integrity, plus an argument that it follows from these claims that the obligations, objectives and targets for the system or product have been met.

This chapter is written for:

- anyone compiling a document presenting safety evidence; and
- anyone reviewing such a document.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product and controlling risk through the application of standards then you should compile evidence that the standards are sufficient to control the risk and that they have actually been followed.
B. If you are delivering a system or product and controlling risk other than by applying standards, you should compile evidence that you have carried out effective ESM and that risk is at an acceptable level.
C. If you are delivering a system or product which contains software, you should compile evidence that the software is of sufficient integrity.
D. If you wish to bring a system or product into use before all of its hazards are closed or all of its safety requirements are met then you should introduce temporary control measures.
E. If you are delivering a system or product, you should agree how you will present evidence of safety with the authorities who will approve the system.
F. If you are delivering a system or product, you should compile evidence for safety as the project proceeds.
G. If you are building a product. you may compile evidence for safety of the generic product or the product in a generic class of application rather then or as well as compiling evidence for each application of the product.
H. If you are compiling evidence of safety, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

13.2.2 Compiling evidence of safety when the risk is covered by standards

A. If you are delivering a system or product and controlling risk through the application of standards then you should compile evidence that the standards are sufficient to control the risk and that they have actually been followed.

Using standards to control risk is one of the risk estimation principles that you may use (see section 8.2.2)

You may use standards to control some or all of the hazards associated with your system. If you use standards to control some of the hazards then you will need to follow the guidance in the next point below for the other hazards.

© Abbott Risk Consulting Ltd. 2022

To show that standards are sufficient to control one or more hazards you will need to show that the standards fully cover the risk associated with these hazards and that the standards are being used as intended. A short report showing this which is compiled and checked by competent people will typically provide sufficient evidence.

Evidence that the standards have actually been followed will normally be accumulated by testing, analysis or inspection, following the checking process associated with the standard.

13.2.3 Compiling evidence of safety when the risk is not covered by standards

B. If you are delivering a system or product and controlling risk other than by applying standards, you should compile evidence that you have carried out effective ESM and that risk is at an acceptable level

You should compile one or more safety reports that provide assurance that risk has been reduced to an authorities to the project and to those who will approve the entry into service of a new railway or a change being made to an existing railway.

The evidence that you rely upon to provide this assurance may include safety cases, or other safety reports, for components of your system or product or previously-published safety cases related to your system or product as a whole.

The size of these reports will depend on the risks and complexity of the project. The reports for a simple and low-risk project should be short. The reports should always be kept as concise as possible but, for a high-risk or complex project, they may have to be longer to present sufficient justification of the conclusions.

The reports should provide evidence that:

- The system or product has been accurately defined.
- The safety objectives and targets for the system or product have been established.
- Safety requirements have been set for the system or product which are consistent with safety objectives and targets.
- The safety requirements have been met.
- Hazards associated with the system or product have been comprehensively identified.
- Risk associated with the system or product has been estimated and shown to be acceptable.
- Human factors have been satisfactorily considered
- Any assumptions made during the analysis have been confirmed.
- Any conditions on the application of the system or product have been accepted by people who are able to ensure that they are complied with.
- An effective program of ESM activities has been performed.
- The system or product was designed, built and installed within quality arrangements that are compliant with an ISO-9000 series standard.
- The system or product and its documentation are under effective configuration management.
- The risk associated with any unresolved issues (for instance hazards that are not closed, unresolved assumptions that have not been confirmed and safety requirements that have not been complied with) has been controlled and arrangements are in place to resolve these issues.
- It is practical to maintain the system in a safe state and to do maintain and operate it safely.

© Abbott Risk Consulting Ltd. 2022

If some hazards of the system or product are controlled entirely by the application of standards and some are not then the safety report should contain evidence that the points above are true in general but you may restrict the evidence for control of the hazards which are controlled by standards to that recommended in the previous guidance point.

The main sources of evidence called up by the safety report are the records that have been kept by the project and the checks that have been made by independent assessors.

The safety report 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.

Although the safety reports are primarily used to satisfy the project and approvers of the system or product, the safety report may have a wider readership, including independent assessors, and this should be taken into account when preparing them.

13.2.4 Compiling evidence that software is of sufficient integrity

C. If you are delivering a system or product which contains software, you should compile evidence that the software is of sufficient integrity.

Guidance on compiling evidence of software integrity is provided in iESM Application Note 3.

13.2.5 Dealing with omissions and non-compliances

D. If you wish to bring a system or product into use before all of its hazards are closed or all of its safety requirements are met then you should introduce temporary control measures.

Sometimes, it may be desirable to bring a system or product into use before all of its hazards have been closed and all of its safety requirements have been implemented and validated.

In this case, you should estimate the increased risk arising from the open hazards and non-compliances and introduce temporary control measures, which may include temporary restrictions upon the way in which the system or product may be operated in order to reduce the risk to an acceptable level. If you cannot reduce the risk to an acceptable level this way, you should not bring the system or product into service.

The temporary control measures should remain in place until any relevant hazards have been controlled and any relevant safety requirements have been implemented and validated.

There may not be time to formulate safety requirements to cover these temporary control measures but they should be defined and written down and someone should check that they have been implemented.

© Abbott Risk Consulting Ltd. 2022

13.2.6 Presenting evidence of safety

E. If you are delivering a system or product, you should agree how you will present evidence of safety with the authorities who will approve the system.

The format of the safety report should be agreed with the people who will approve it. This may be done by defining the format of the safety report in the safety planning documents and agreeing the safety planning documents with the people who will approve the safety report. See section 6.2.2 for further details.

One way of presenting a safety report is to prepare a Safety Case. EN 50126 [50126-1] requires the production of a Safety Case when seeking approval for train control and protection systems, electrification systems and rolling stock. iESM Application Note 2 provides a document outline for a Safety Case.

Goal Structuring Notation (GSN) has been found a useful technique for structuring and illustrating Safety Cases, if used correctly. For further information about GSN, see [Kelly].

13.2.7 Compiling evidence of safety as the project proceeds

F. If you are delivering a system or product, you should compile evidence for safety as the project proceeds.

However you present evidence for safety and whoever is approving it, you should collect this evidence and agree it with the approvers as the project proceeds. Ideally, you and the approvers will both be confident that your plans and designs will control risk before physical work starts and the final approval can be largely based on confirmation that the agreed arrangements for controlling risk are in place. This is generally a good idea as it makes it less likely that you will encounter unexpected objections at the end of the project.

The safety report can be prepared as an incremental document which will include evidence as it becomes available.

13.2.8 Structuring evidence of safety for products

G. If you are building a product you may compile evidence for safety of the generic product or the product in a generic class of application rather then or as well as compiling evidence for each application of the product.

EN 50126 [50126-2] and EN 50129 [50129] define three different types of Safety Case:

- A **Generic Product Safety Case** provides evidence that a generic product is safe. The conclusions of a generic product Safety Case will rely upon assumptions about the way in which the product will be applied and the operational environment in which it is applied which will have to be confirmed when the product is applied. There may also be omissions from the Safety Case which will have to be confirmed when the product is applied.
- A **Generic Application Safety Case** provides evidence that a generic product is safe in a specific class of applications. It will generally have more assumptions than a generic product Safety Case but fewer omissions.

© Abbott Risk Consulting Ltd. 2022

- A **Specific Application Safety Case** is relevant to one specific application at one location. It will address both the application design and physical implementation.

This division allows efficient re-use of safety evidence. For instance, a Specific Application Safety Case for a resignaling 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. In such cases there will be dependencies or application conditions between the safety cases that need to be respected.

You may find it useful to divide the evidence for the safety of a product and its applications in this way even if you are not following EN 50126 and even if you do not use the names above.

You do not normally have to use all three types of safety case.

13.2.9 Competence

H. If you are compiling evidence of safety, you should make sure that the people doing the work have sufficient knowledge and expertise to do it competently.

The person or persons compiling the safety evidence should have received training in ESM or have had experience of successfully delivering a program of ESM activities or both.

For further guidance on competence management, see chapter 21.

13.3 Sources of further guidance

Section 6.2.2 provides guidance on planning a program of ESM activities, which should include defining the format of the safety report.

Section 8.2.2provides guidance on risk estimation principles.

Chapter 12 provides guidance on cross acceptance.

Chapter 21 provides further guidance on competence management.

iESM Application Note 2 provides a document outline for a Safety Case, which is one way of presenting safety evidence.

iESM Application Note 3 provides guidance on compiling evidence of software integrity.

EN 50126 [50126-2] and EN 50129 [50129] provides guidance on producing Safety Cases and on different types of Safety Cases.

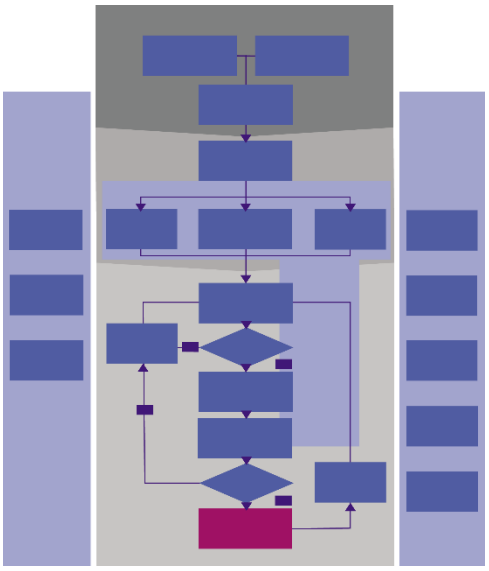
© Abbott Risk Consulting Ltd. 2022

14 OBTAINING APPROVAL

14.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. The evidence compiled in the previous activity is submitted to the necessary authorities in order to obtain approval to bring the system into service.

Note. We use the word ‘approval’ to cover any occasion when someone accepts that work done so far is satisfactory and work may continue to the next stage. Your organization may use other words such as ‘acceptance’, ‘authorization’, ‘endorsement’ or ‘consent’.



Your organization must obtain all necessary approvals before placing a system or product into service.

The body or bodies who need to approve your work may be defined in law, by the government or by the railway company. The approval may be made subject to restrictions on how the work is carried out or how the railway can be used afterwards.

In some cases, you may receive approval for your organization's overall processes and then uses the processes to approve the placing of some systems into service without seeking external approval.

If you are changing the railway, you may need approvals before you make the change or bring the change into service, or both. Some projects make staged changes to the railway, in which case each stage may need approval.

© Abbott Risk Consulting Ltd. 2022

14.2 Guidance

14.2.1 Introduction to the guidance

When creating a new railway system or product, it is necessary to gain approval from one or more authorities before placing the system or product in service. The authorities from whom you require approval may be within your organization or outside it, or both. You should make sure that you understand applicable legal and the requirements of the local railway authorities. These will take precedence over the guidance in this section.

One of the criteria that will have to be met before approval is granted will be that risk has been controlled to an acceptable level but there will usually be other criteria, for example that the system has acceptable reliability. This chapter provides guidance on this approval process as it relates to safety.

This chapter is written for anyone seeking or granting approval to bring a system or product into service.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should identify the authorities from whom you will have to obtain approval.
B. If you are delivering a system or product, you should agree with the authorities from whom you will have to obtain approval whether they will delegate any aspects of approval to you.
C. If you are delivering a system or product, you should agree with the authorities from whom you will have to obtain approval, the content and timing of submissions that you will make to them.
D. If you are delivering a system or product, you should obtain approval, from the necessary authorities before placing the system or product in service.

14.2.2 Planning to obtain approval

A. If you are delivering a system or product, you should identify the authorities from whom you will have to obtain approval.

You should do this early in the project. To do this, you should:

- Check your own organization's requirements.
- Consult the procedures which apply on the railway that you are changing.
- Consult the guidance provided on national and international approval requirements.

B. If you are delivering a system or product, you should agree with the authorities from whom you will have to obtain approval whether they will delegate any aspects of approval to you.

In some cases, the authorities may approve your own internal procedures and allow you to approve the system or product. In such cases the person who approves the system or product may be an authorized and competent person, who will grant approval on the basis of evidence that the procedures have been correctly followed.

© Abbott Risk Consulting Ltd. 2022

C. If you are delivering a system or product, you should agree with the authorities from whom you will have to obtain approval, the content and timing of submissions that you will make to them.

Approval will generally be granted on the basis of inspecting evidence for safety. See chapter 13 for guidance on compiling evidence of safety.

If the system or product is being brought into service in a number of stages then each stage should be covered by an explicit approval. It may be possible for the authorities concerned to grant approval for multiple stages at one time.

It is generally a good idea to compile evidence of safety incrementally as the project proceeds and submit early versions to the authorities granting approvals. This makes it less likely that they will raise unexpected objections at the end of the project. Ideally, you and authorities granting approvals will all be confident that your plans and designs will control risk before physical work starts and the final approval can be largely based on confirmation that the agreed arrangements for controlling risk are in place.

14.2.3 Obtaining approval

D. If you are delivering a system or product, you should obtain approval, from the necessary authorities before placing the system or product in service.

You should make the submissions as planned and respond to any objections or comments raised by the approving authorities.

14.3 Sources of further guidance

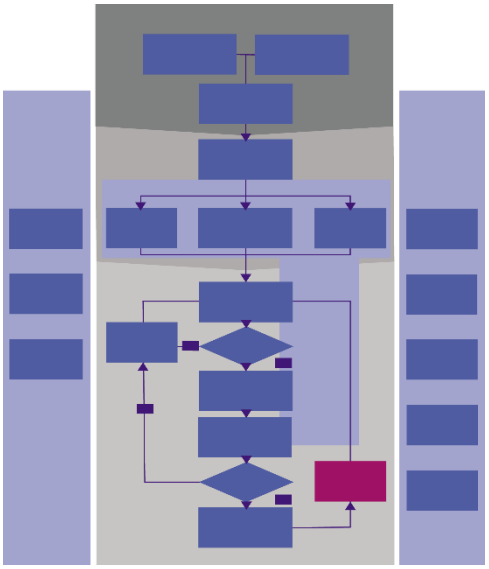
Chapter 13 provides guidance on compiling evidence of safety.

© Abbott Risk Consulting Ltd. 2022

15 MONITORING RISK

15.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. As soon as a system first enters service (or enters trial operation in an operational environment that approaches the real environment), its performance should be monitored in order to confirm and improve the estimation of risk. This may require that additional control measures should be put in place.



Your organization must take all reasonable steps to monitor and improve the management of risk. Your organization must identify, collect and analyze data that could be used to improve the management of risk, as long as it is has responsibilities for safety.

The type of monitoring you should perform depends on the type of safety-related work you do. To the extent that it is useful and within your area of responsibility, you should monitor:

- how safely and reliably the railway as a whole is performing;
- how safely and reliably parts of the railway are performing;
- whether the measures put in place to control risk remain operative and effective; and
- the circumstances within which the railway operates.

You should consider collecting and analyzing data about:

- incidents, including both accidents and near misses;
- suggestions and feedback from users of the system and your staff;
- failures to follow standards and procedures;
- faults and wear and tear; and
- anything else that may affect your work.

You should calculate statistics from these data and monitor the variation of these statistics with time.

© Abbott Risk Consulting Ltd. 2022

Where safety depends on assumptions and you have access to data that you could use to confirm these assumptions, then you should collect and analyze these data. If you analyze incidents you should look for their root causes because preventing these may prevent other problems as well.

You should ask users of the system and your staff to tell you about safety problems and suggest ways of improving safety.

You should look out for future problems which may arise because components of your system or product are becoming obsolete.

If you work for a supplier, you may not be able to collect all of these data yourself. If so, you should ask the organizations using your products to collect the data you need and provide them to you.

Your organization must take action where new information shows that this is necessary

This action will generally require performing some of the activities described above.

15.2 Guidance

15.2.1 Introduction to the guidance

Risk estimation, as described in chapter 8, delivers a forecast of the risk associated with a product and system. This forecast is generally based upon assumptions about the operational environment in which the system or product will operate and how it will be used.

Once the system or product enters service, statistics about its performance should be collected in order to find out if the forecast of risk was accurate and to detect any trends in the risk, particularly where risk is increasing. In addition data should be collected in order to establish whether the assumptions made are and remain true.

This chapter is written for anyone responsible for monitoring levels of risk associated with a system or product.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should initiate activities to collect data that could be used to improve the management of risk.
B. If you are delivering a system or product, you should define and initiate activities to analyze data that could be used to improve the management of risk and you should act on the results of the analysis where necessary.
C. If you are delivering a system or product, you should look out for components which may soon become obsolete and take steps to ensure that this does not result in increased risk.
D. If you are delivering a system or product and it is involved in a safety incident, you should play a full part in ensuring that the incident is investigated and you should act on the findings where necessary.

© Abbott Risk Consulting Ltd. 2022

15.2.2 Collecting data

A. If you are delivering a system or product, you should initiate activities to collect data that could be used to improve the management of risk.

The types of monitoring that you should do and the parts of the railway that you monitor should depend on the risk that your activities are designed to control.

There are two sorts of data that you may collect:

- You may collect data about your *processes,* in order to improve them. If your processes have the potential to expose people directly to hazards, then you may collect data such as the number of incidents. If your processes have the potential to introduce hazards, then you may collect data such as the number of mistakes made and/or faults introduced (including possibly non-hazardous ones). In either case you will need to collect data about the total volume of work done so that you can express statistics in units, such as 'Lost time incidents per million working hours' or 'Faults per million lines of software'.
- You may collect data about the *performance of the system* that you are responsible for in order to improve its behavior or to react to degradations in its behavior. This only becomes useful in projects from the point that an early version of the system, or maybe a prototype, starts to function but is always at the heart of data collection for maintenance. You may collect data about hazardous and non-hazardous events. You will probably also need to collect some data about the total volume of use that the system has had, so that you can express statistics in units such as 'Failures per million operational hours'.

Your organization should decide what things it needs to monitor and then continue to monitor them throughout the project and then as long as it is responsible for a part of the railway. You may need to change the way you monitor these things and change what you monitor as parts of the project. You should decide which other parts of the railway you need to monitor for changes as well.

Your organization should also collect data, so that you can confirm that the assumptions that you originally made are still valid. See section 16.2.3 for guidance on managing assumptions.

If your organization shares responsibility for the railway with other organizations, collecting some of the data that you will need in order to monitor risk is likely to require co-ordination between these organizations.

Guidance on risk monitoring during the Operations and Maintenance phase is published by the European Union [CSM-M] and provides some help in identifying what data may be relevant to collect.

You should collect the data that you have decided to collect.

15.2.3 Analyzing data

B. If you are delivering a system or product, you should define and initiate activities to analyze data that could be used to improve the management of risk and you should act on the results of the analysis where necessary.

You should decide how you are going to analyze the data and you should establish arrangements for performing the necessary analysis.

© Abbott Risk Consulting Ltd. 2022

The phrase 'Data Recording, Analysis and Corrective Action System' or DRACAS is used to describe such arrangements. Guidance on establishing a DRACAS is provided in iESM Application Note 3.

It is good practice to pro-actively review your safety record against your safety targets on a regular basis, for instance, annually or whenever there is a change that you think could affect the risks that you are managing (including changes to equipment, organizations and the way work is done). You should also review your safety record when you receive information about an incident to look for any additional control measures that might improve safety further.

The data you collect should be used to develop key safety and performance indicators. You should use these as part of the way you review your work and communicate how well you are doing to your personnel, your suppliers and your customers.

You should decide how you are going to use the results of your analysis and who will decide whether to act on the results.

You should communicate the information to others who need it to control risk. Chapter 23 provides guidance on communicating safety-related information.

The results of your analysis may be used to confirm that temporary control measures may be relaxed because risk would be acceptable without them.

15.2.4 Monitoring and reacting to obsolescence

C. If you are delivering a system or product, you should look out for components which may soon become obsolete and take steps to ensure that this does not result in increased risk.

You should perform an analysis of the likelihood of obsolescence of key components. You should then decide on your strategy for dealing with obsolescence. Possible strategies include performing periodic redesigns in which obsolescent components are replaced and stockpiling spare components.

You may be also able to reduce the likelihood of a component becoming obsolescent within a period of time by sourcing it from multiple vendors or by using components that conform to industry standards.

15.2.5 Investigating and learning from incidents

D. If you are delivering a system or product and it is involved in a safety incident, you should play a full part in ensuring that the incident is investigated and you should act on the findings where necessary.

The part that you will play in investigating an incident will depend upon the role that your organization plays in running the railway. It may take the lead or it may only be required to support someone else.

Whatever role your organization plays, it should do its utmost to help ensure that the root causes of any incident are understood. Even if no-one was hurt in the incident, if its occurrence shows that there is a possibility of someone being hurt in the future, steps should be taken to remove the root causes of the incident.
RSSB publishes advice on investigating incidents which may be useful to you [RSSB2].

© Abbott Risk Consulting Ltd. 2022

15.3 Sources of further guidance

Chapter 8 provides guidance on risk estimation.

Section 16.2.3 provides guidance on managing assumptions.

Chapter 23 provides guidance on communicating safety-related information.

iESM Application Note 3 provides guidance on establishing 'Data Recording, Analysis and Corrective Action System' or DRACAS.

RSSB publishes advice on investigating incidents [RSSB2].

European Union Commission Regulation (EU) N°1078/2012 on the Common Safety Method (CSM) for Monitoring [CSM-M] and its guidance

© Abbott Risk Consulting Ltd. 2022

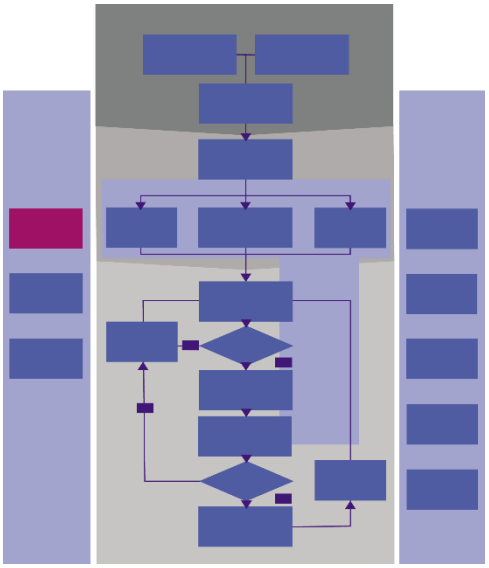
Part V: Technical Support

© Abbott Risk Consulting Ltd. 2022

16 MANAGING HAZARDS

16.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. Many of the activities described above will deliver additional information about hazards. This information needs to be compiled into some form of register so that the state of each hazard can be readily established at any time.



Your organization must track the analysis of hazards, the implementation of measures put in place to control hazards and the validation of such measures in order to confirm that the risk associated with each hazard is, and remains at, an acceptable level.

You should create a Hazard Log that records the hazards identified and describes the action to remove them or control risk to an acceptable level. You should keep this register up to date as long as you have responsibility for the system or product and hand it on if anyone else takes on that responsibility.

16.2 Guidance

16.2.1 Introduction to the guidance

This chapter describes how to set up and maintain a Hazard Log and how to use it to support the process of closing hazards and thereby controlling risk. It also describes how to manage the assumptions and application conditions upon which hazard management depends.

© Abbott Risk Consulting Ltd. 2022

This chapter is written for:

- 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.

Guidance is structured under the following checklist items:

A. If you are delivering a system or product, you should set up a Hazard Log containing information about each hazard.
B. If you are delivering a system or product, you should actively manage hazards to closure.
C. If you have set up a Hazard Log, you should keep it up-to-date as new information becomes available.
D. If you are delivering a system or product, you may find it useful to keep other information in the same place as the Hazard Log.
E. If you are delivering a system or product, you should make sure that the people who need to use the information in the Hazard Log can access it and, if they cannot, you should extract the information that they need and send it periodically to them.
F. If you are delivering a system or product, you should identify assumptions upon which the safety of the system or product relies.
G. If you are delivering a system or product, you should find out whether the assumptions that you have made are true and take action if they are not.
H. If you are delivering a system or product, you should identify assumptions which other people make about your system or product.
I. If you are delivering a system or product, you should either make sure that any assumptions that other people have made about it are true or inform them if they are not.
J. If you are delivering a system or product, you should track assumptions to closure.
K. If you are delivering a system or product, you should identify application conditions upon which the safety of the system or product relies.
L. If you are delivering a system or product, you should ensure that any application conditions that you define are passed to the people who have to respect them and that these people accept them.
M. If you are making use of someone else's system or product then you should identify any application conditions associated with it.
N. If you are making use of someone else's system or product then you should ensure that any application conditions associated with it are respected.
O. If you are delivering a system or product, you should track application conditions to closure.

16.2.2 Maintaining a Hazard Log

A. If you are delivering a system or product, you should set up a Hazard Log containing information about each hazard.

The Hazard Log should contain an unambiguous definition of the system or product to which it refers and should be capable of storing the following information for each hazard:

- A unique reference.
- A brief description of 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, including any application conditions on how the system may be used (see below).

© Abbott Risk Consulting Ltd. 2022

- The risk principle used to estimate risk for the hazard (see section 8.2.2), that is, one of the following
    - Applying standards;
    - Comparison with a reference system; or
    - Explicit estimation of the severity and likelihood of accidents.
- The estimated risk associated with the hazard (where the principle of explicit risk estimation is used).
- The status of the hazard (see below).
- A description of any actions identified to progress the hazard to closure and the names of the people or organizations responsible for carrying out these actions.
- A list of measures agreed to control the risk associated with the hazard, which may be provided by reference to relevant safety requirements (see chapter 9), noting whether each measure has been implemented and validated yet.

It may also be desirable to record possible measures to control the risk associated with the hazard that were considered and rejected. In some jurisdictions, records of this sort may be necessary in order to demonstrate that you have complied with the law.

The Hazard Log is best stored in some tool with an underlying database. Special purpose tools are available for this purpose, but it is also possible to store the Hazard Log in a general-purpose database or spreadsheet tool.

If a general purpose database is being used to store system requirements, then it may be convenient to store the Hazard Log in the same database.

It is not necessary to repeat detailed information documented elsewhere and so the Hazard Log should summarize this information and make reference to other project safety documentation for more detail.

The Hazard Log should be stored with the project file so that material referred to in the Hazard Log is easily accessible.

Adequate provision should be made for security and back-up of the Hazard Log.

B. If you are delivering a system or product, you should actively manage hazards to closure.

The possible statuses of a hazard will typically include 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); and
- closed (action to close the hazard has been completed).

Additional statuses may be useful. For example, it may be administratively convenient to record that a hazard is ‘conditionally closed’ or ‘resolved’ if the actions required to close it have been agreed but not all implemented. The hazard can be closed as soon as the outstanding actions are completed.

You should ensure that any hazard which is not closed or cancelled is associated with an action to progress it towards closure.

You should make sure that anyone who is shown in the Hazard Log as being responsible for an action, knows that they have this action and accepts it.

© Abbott Risk Consulting Ltd. 2022

You should monitor the status of actions and hazards and take action if necessary to ensure that progress is maintained.

C. If you have set up a Hazard Log, you should keep it up-to-date as new information becomes available.

The Hazard Log should be updated whenever:

- a new hazard is identified;
- further analysis is performed on a hazard;
- an action is assigned, completed, cancelled or transferred;
- a measure to control a hazard is agreed upon, implemented or validated;
- any other new information about a hazard comes to light; or
- an incident occurs in which the system or product is involved.

A process should be defined for updating the Hazard Log, which makes clear which staff are authorized to make changes.

A record should be kept of the changes made to the Hazard Log. If the Hazard Log is kept in a database, the database tool may record this information; otherwise some journal or document history should be set up and maintained.

D. If you are delivering a system or product, you may find it useful to keep other information in the same place as the Hazard Log.

Other records which it may be convenient to store in the same place as the Hazard Log, particularly if a database is being used, include:

- records of any incidents related to the system or product being delivered;
- records of the status of assumptions and application conditions; and
- a directory of the safety records produced by the project.

E. If you are delivering a system or product, you should make sure that the people who need to use the information in the Hazard Log can access it and, if they cannot, you should extract the information that they need and send it periodically to them.

The Hazard Log should be available for inspection by project staff, those performing independent assessment and those granting safety approval.

If there are people with actions or other stakeholders who need to use the information in the Hazard Log but who do not have access to the log, you should produce a report with the information that they need and send it periodically to them.

© Abbott Risk Consulting Ltd. 2022

16.2.3 Managing assumptions

The developers of systems and products find themselves making assumptions about the rest of the world, including the people and organizations with which the systems and products will interact, as well as the physical railway. For instance, when designing an electric train, certain tolerances on the supply voltage may be assumed. Someone will have to confirm that these assumptions are true when the system goes into service and remain true for the rest of its life (or deal with the situation if they do not).

Not all assumptions affect safety but many do. If they are not identified or are identified but not confirmed, a hazard may result.

If you are replacing an existing system or product, there may be assumptions that other systems make about the system or product that is being replaced that are recorded. Moreover, different assumptions may be made about similar systems and products in different places. Assumptions about track circuits for a line which is electrified may be different from those for one which is not.

Assumptions may be managed by using standards. Generally, these standards concern issues at the interface between parts of the railway, such as the running gauge – the distance between the rails.

Where an assumption is fully covered by a standard, then showing compliance with this standard will be enough to deal with the assumption. So, on a standard gauge railway, those responsible for the trains and the track show that they comply with the standard rather than placing assumptions on each other about the distances between the wheels and the rails. If a project wishes to depart from such a standard then it will normally need to make an application for permission to do so from some nominated authority who will need to take the assumptions underpinning the standard into account when deciding whether or not to authorize the departure.

In addition to any economic benefits, managing assumptions through standards will reduce the opportunities for mis-communication and the standards will generally describe tried and tested solutions. We therefore recommend managing assumptions through standards wherever practical.

Where an assumption is not dealt with by mandatory standards, it is worth considering whether there is a voluntary standard that would deal with it, and which both parties to the interface can agree to be bound by.

You should still look to see if the safety of your system or product relies on any assumptions that are not fully covered by standards. If there are any such assumptions, you should take steps to make sure that they are confirmed.

You should also look to see if anyone else is making assumptions about your system or product and either ensure that these assumptions are true or inform the people making the assumptions if they are not.

The rest of this sub-section provides guidance on how to do this.

F. If you are delivering a system or product, you should identify assumptions upon which the safety of the system or product relies.

Assumptions are identified at all stages of the system life cycle. In particular, assumptions may be identified while defining the boundaries of your system and form part of the specification of the boundary of the system. However, before you make an assumption, you should consider if it could be confirmed as a fact.

© Abbott Risk Consulting Ltd. 2022

All assumptions which are relevant to the safety of the system are likely to form part of the safety argument at some point, so when you identify then you should consider how you will confirm that they are true.

G. If you are delivering a system or product, you should find out whether the assumptions that you have made are true and take action if they are not.

You may need to do this by asking someone else to confirm that an assumption is true.

If an assumption turns out not to be true, you should adjust your estimation of the risk to align with the world as it is, evaluate whether the risk is now acceptable or not and, if it is not acceptable, take whatever action is necessary to make it acceptable.

H. If you are delivering a system or product, you should identify assumptions which other people make about your system or product.

You should consider all the other systems with which your system or product might interact (whether on purpose or not) and look for assumptions that their designers or operators may make about your system or product.

These assumptions will not always be written down, particularly when other systems have been in service for some time. Therefore, when looking for assumptions, it is important to involve people with sufficient domain knowledge of the system as a whole, and the operational environment, both physical and organizational, that the system must interact with. It is important to have not just those with specialist knowledge of small parts of the system, but also those with broader knowledge of the operation of the wider system.

If there are centrally co-ordinated registers of assumptions, you should consult them. However, you should not rely on a central register as your only source.

I. If you are delivering a system or product, you should either make sure that any assumptions that other people have made about it are true or inform them if they are not.

You should consider each assumption that is made about your system or product and decide whether you will ensure that it is true. If you do then it should become a requirement for your system or product and, if the assumption is safety-related, then it should become a safety requirement.

If you are not going to ensure that the assumption is true then you should inform whoever has made the assumption so that they can deal with the consequences of your decision.

© Abbott Risk Consulting Ltd. 2022

J. If you are delivering a system or product, you should track assumptions to closure.

You should use a consistent method of recording, naming and referencing assumptions in order to make communication and management simpler.

The management of assumptions should not require excessive additional bureaucracy, or paperwork. Therefore, you should attempt to integrate any method for the recording and management of assumptions with other parts of your process, and organization.

Assumptions may be conveniently stored in a register, which is part of, or kept with, the Hazard Log.

You should have some system for recording the assumptions that you make, for recording the assumptions that other people make about your system and for tracking the progress of both sorts of assumption to closure.

As each assumption is identified, someone who understands should be given responsibility for dealing with it.

If you are preparing evidence of safety in a safety report, then assumptions will also be discussed in it in order to provide context to the safety argument.

16.2.4 Managing application conditions

The developers of systems and products may need to specify conditions on how their systems and products may be applied, operated, maintained and disposed of'. We call these conditions, **application conditions**. For instance, a certain inspection regime may be required. EN 50126 [50126-1] also calls these contextual safety requirements.

Note. Similar terminology is used elsewhere. EN 50129 [50129] uses the term 'Safety-Related Application Condition' (SRAC).

The developers of systems and products may use other systems and products in which case they need to respect the application conditions associated with these systems and products.

People applying systems or products which are approved for use subject to certain application conditions will need to respect these application conditions.

Not all application conditions affect safety but many do. If they are not identified or are placed but not dealt with, a hazard may result.

K. If you are delivering a system or product, you should identify application conditions upon which the safety of the system or product relies.

Application conditions are identified at all stages of the system life cycle.

© Abbott Risk Consulting Ltd. 2022

L. If you are delivering a system or product, you should ensure that any application conditions that you define are passed to the people who have to respect them and that these people accept them.

Application conditions may be communicated in safety reports, Hazard Log, correspondence, formal handover documents, and operations and maintenance manuals. If you need operations or maintenance staff to respect an application condition, you will normally ensure that it is included in the operations or maintenance manuals and be traceable back to the relevant hazard. Typically, this will be safety-related information which you will need to highlight as such.

An application condition should not be considered closed until the recipient has confirmed that they understand and accept responsibility for it.

Application conditions may initially be passed to those responsible for the installation and integration of the system with the railway as a whole and transferred later to those who are responsible for the ongoing management of the system.

Before you define an application condition you should consider if you could design it out of your system. Reducing the dependency between systems and products is good systems engineering practice, and simplifies the integration of the system. You should weigh this against the effort involved and possible effects that such a redesign may have on the safety of the system. Designing out an application condition will not be appropriate in all circumstances.

You should make the transfer of responsibility part of your process for the handover of the project, working with clients and partner organizations to ensure that an appropriate person or group of people takes responsibility for each application condition. In some situations you may not be able to assign responsibility directly to the right person.

You may have to take a pragmatic approach. Most importantly, you must ensure that responsibility is never lost. If you cannot transfer responsibility to someone who can ensure that it is respected, then try to transfer it to someone who is in a position to assign it to someone else who can deal with it.

Transferring an application condition may have business implications; in which case, whoever is responsible for this application condition should be in a position to handle this aspect of it.

M. If you are making use of someone else's system or product then you should identify any application conditions associated with it.

This situation may occur if the system or product that you are delivering is composed of other systems or products. This situation may also occur if you are applying a product.

You will normally find the application conditions in the documentation provided with the system or product that you are using.

© Abbott Risk Consulting Ltd. 2022

N. If you are making use of someone else's system or product then you should ensure that any application conditions associated with it are respected.

You should treat any safety-related application conditions associated with systems and products that you use as safety requirements.

If you find that you cannot respect an application condition then you will need to find out what the consequences of this are for the risk associated with your system and, if the risk is unacceptable, take whatever action is necessary to reduce it to an acceptable level.

O. If you are delivering a system or product, you should track application conditions to closure.

Within your organization you should use a consistent method of recording, naming and referencing application conditions in order to make communication and management simpler.

The storage and management of application conditions should not require excessive administration or paperwork. Therefore, you should attempt to integrate any method for the recording and management of application conditions with other parts of your process, and organization.

Application conditions may be conveniently stored in a register, which is part of, or kept with, the system's Hazard Log. They should be managed in a similar way to hazards with a unique identifier, their source, who they are being placed on and the related hazard.

You should have some system for recording the application conditions that you identify and for tracking the progress of each application condition to closure.

If you are preparing evidence of safety in a safety report, then application conditions will also be discussed in it in order to provide context to the safety argument.

Safety certificates will contain application conditions.

16.3 Sources of further guidance

Section 8.2.2 provides guidance on risk estimation principles.

Chapter 9 provides guidance on managing safety requirements.

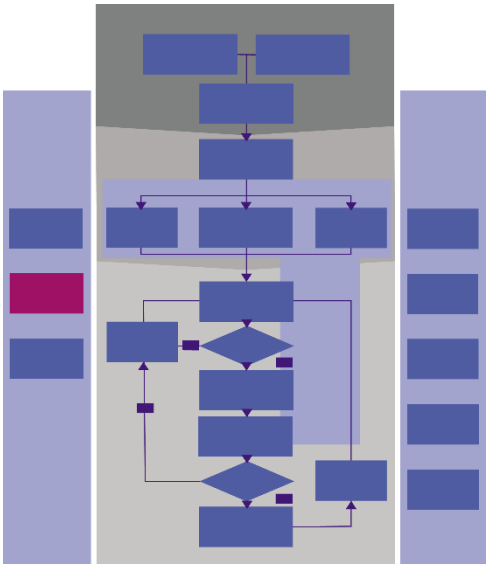
EN 50126 [50126-2] includes guidance on managing a Hazard Log.

© Abbott Risk Consulting Ltd. 2022

17 INDEPENDENT ASSESSMENT

17.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. An independent assessment provides a second opinion on the adequacy of ESM activities. It is a service both to the organization being assessed and to those considering whether to grant approval to bring the system into service or place the product on the market.



Your organization must ensure that engineering safety management activities are reviewed by competent people who are not involved with the activities concerned.

These reviews may be divided between process-focused reviews (often referred to as safety audits) to check how things are being done and product- focused reviews (often referred to as independent assessments) to check what is being produced. Audits provide evidence that you are following your plans for safety. Assessments provide evidence that you are meeting your safety requirements. How often and how thoroughly each type of review is carried out, and the degree of independence of the reviewer, will depend on the extent of the risk and novelty and on how complicated the work is.

If an ESM activity is done many times, it may be better to specify it precisely and review the specification rather than the activities themselves. You will still need to confirm that you comply with the specification each time you carry out the activity but this compliance will not be subject to independent assessment.

17.2 Guidance

17.2.1 Introduction to the guidance

This chapter describes independent assessments. It discusses how to go about commissioning an assessment, what an assessment should be checking for, and how the findings should be reported and used.

Independent assessment is the process of forming an independent, competent judgment as to whether or not the risk associated with a system or product is (or will be) reduced to an adequate level.

© Abbott Risk Consulting Ltd. 2022

It is normally a process that continues throughout the lifetime of a project. It may be performed in two different ways:

- Where a project is controlling risk through the application of standards (that is, it is employing the 'Applying standards' risk principle described in section 8.2.2 above), independent assessment will be mostly concerned with verifying that the standards cover the risk and have been applied correctly. Guidance on this situation is provided in the first sub-section below.
- In other circumstances, independent assessment will look more generally at the ESM performed on the project. Unless something goes wrong, this will result in the assessor supporting the project's claim that risk has been controlled to an acceptable level. Guidance on this situation is provided in the second sub-section below.

In either case, safety audits should be carried out to confirm that the plans for safety are being followed and are effective. In projects which are controlling risk through the application of standards, these audits will be separate from the technical checks; in other projects they will typically be part of the overall independent assessment process. Guidance on safety audits is provided in the third sub-section below.

This chapter is written for those who commission independent assessments and interpret the results, and those who perform them.

Guidance is structured under the following checklist items:

A. If you are relying on the application of standards to control risk, you should ensure that the correct application of these standards is independently and competently checked.
B. If you are delivering a system or product, you should arrange for a program of independent assessment to be carried out in order to confirm that risk associated with the system or product is being or has been reduced to an acceptable level.
C. If you intend to carry out a program of independent assessment, you should plan out the program and specify what you require from the program.
D. If you appoint independent assessors, you should ensure that they are sufficiently qualified for their role.
E. If you appoint independent assessors, you should ensure that they are independent of the project.
F. If you are performing an independent assessment, you should carry it out systematically.
G. If you are performing an independent assessment, you should provide your findings to the project quickly and in a way that supports effective action.
H. If you receive findings from an independent assessment, you should ensure that the action necessary to deal with them is taken.
I. If you are delivering a system or product, you should arrange for safety audits to be carried out in order to confirm that the project is conforming to plans and procedures that relate to safety.
J. Safety auditors should be sufficiently qualified for their role.
K. Safety auditors should be independent of the project.
L. If you are performing a safety audit, you should carry it out systematically.
M. If you are performing a safety audit, you should provide your findings to the project quickly and in a way that supports effective action.
N. If you receive findings from a safety audit, you should ensure that the action necessary to deal with them is taken.

17.2.2 Independent assessment of risk controlled by the application of standards

This guidance is applicable to projects which are controlling risk entirely through the application of standards. When a project is controlling some risk entirely through the application of standards and other risk through comparison with a reference system or explicit risk estimation then this guidance may be applied to the first class of risk.

© Abbott Risk Consulting Ltd. 2022

A. If you are relying on the application of standards to control risk, you should ensure that the correct application of these standards is independently and competently checked.

The independent checks required are typically an integral part of the processes of the discipline involved. The assessment may be limited to review of the work done but may also involve independent repetition of part of the work to check that the same results are obtained.

The people doing the checking should have sufficient competence that they could have carried out the work being checked but should have played no part in carrying out the work.

A record of the check should be made but that may be as simple as having the checker countersign a document or drawing.

If the checker finds any issues, these should be drawn promptly to the attention of the people doing the work who should revise the work as necessary to resolve the issues.

17.2.3 Independent assessment of risk not controlled by the application of standards

This guidance is applicable to projects which are not controlling risk entirely through the application of standards or where only basic integrity needs to be achieved and demonstrated.

An independent assessment should always be carried out for such projects. It is normal to refer to the assessor as an 'Independent Safety Assessor' or 'ISA'. The assessor may work for the organization delivering the project. Guidance on the level of independence is provided below.

EN 50128 [50128] and EN 50657 [50657] require the deployment of a software assessor for any project intending to show compliance with that standard (including functions identified as SIL0).

B. If you are delivering a system or product, you should arrange for a program of independent assessment to be carried out in order to confirm that risk associated with the system or product is being or has been reduced to an acceptable level.

The safety requirements for the system are central to an independent assessment. The assessor should review the safety requirements to assess whether they are sufficient to control risk, and review the system and its documentation to assess whether or not it meets or will meet the safety requirements.

The assessor should review the processes and organization employed on the project. This may be done by commissioning audits of the ESM activities (see below).

Any report arising from an independent assessment should include a judgment 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.

© Abbott Risk Consulting Ltd. 2022

C. If you intend to carry out a program of independent assessment, you should plan out the program and specify what you require from the program.

In general, the thoroughness of an independent assessment will depend on the complexity and level of risk presented by the project.

Assessment activities should be defined in the plans for the ESM program (see chapter 6). The project or organization may commission additional assessment activities.

Whoever commissions an independent assessment should write an assessment remit. This should record the requirements of the assessment and all the relevant details, including:

1. the project title and reference;
2. the name of the assessor, their qualifications and experience, and their level of independence; and
3. assessment requirements defining:
    - the scope of the 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);
    - the purpose of the assessment ;
    - the basis of the assessment, which should specify the legal framework and the ESM framework within which the project is being run; and
    - any previous assessments or audits whose results may be assumed in the performance of the current assessment.

The remit should be agreed and signed by the project manager and the assessor.

A program of work for the assessment should be agreed between the assessor and the client and used to estimate the effort required to perform the assessment.

D. If you appoint independent assessors, you should ensure that they are sufficiently qualified for their role.

The people performing an independent assessment should have the following technical knowledge and experience:

- demonstrable application domain experience;
- experience of process assurance (for instance quality or safety audits);
- familiarity with relevant standards;
- familiarity with the applicable legal and safety regulatory framework;
- knowledge of the engineering and operational activities being assessed;
- knowledge of ESM, including the techniques being assessed and the scope of their application;
- knowledge of relevant quality management techniques; and
- knowledge of conditions and application processes at the location where the system or product is being applied

The people performing an independent assessment should also have the following personal qualifications and attributes:

- professional status in an engineering or scientific discipline relevant to the system or equipment;

© Abbott Risk Consulting Ltd. 2022

- prior experience as an independent assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- a commitment to safety; and
- the flexibility to adapt to changing circumstances and the perform assessment. tasks efficiently and to minimize wastage of physical and virtual resources

Where an independent assessment is carried out by a team, the team as a whole should possess the technical knowledge and experience and the lead assessor as an individual should possess the personal qualifications and attributes.

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

- purpose of the project;
- technology and methods used; and
- integrity required of the system and accident potential.

The assessor should be appointed early in the project, before the end of the Concept and Feasibility stage in the system lifecycle. It is a good idea to retain the same assessor throughout the project.

If an independent assessor is required for a project then they should be regarded as an essential resource to the same extent as the principal delivery contractors. If no independent assessor can be found with the necessary qualifications and experience then it may be necessary to consider changing the scope of the project.

E. If you appoint independent assessors, you should ensure that they are independent of the project.

The assessors should be independent of the project and should not have contributed to the design, manufacture, construction, marketing, operation or maintenance of the system or product under assessment or to the ESM activities carried out for the system or product. They may work for another organization and this is recommended for systems which have been assigned a SIL of 3 or 4. In this case it is recommended that the assessor should work under contract to the organization procuring the system or product rather than the supplier of that system or product.

For other systems, the assessor may work for the organization delivering the system or product, provided that they do not report to the project manager or the project manager's immediate manager.

The independence of the assessors allows them to form different views from the project and so to reveal problems without pressure from their peers or supervisors. It is therefore essential that they should have the integrity to express their true views, even if this is inconvenient, and this should be taken into account when selecting assessors.

If the assessors work for another organization, that organization's remuneration should not depend upon whether its assessment is favorable or not. It is normal for the contract between the assessors and their client to bind the assessors to respect their client's secrecy.

Whoever commissions an assessment should decide upon the level of independence. The level of independence should be dependent primarily on the level of risk presented by the project.

© Abbott Risk Consulting Ltd. 2022

In specialist areas, it may be difficult to find assessors who are completely unconnected with the project but still have the qualifications and expertise (see below). It is better to accept a lower level of independence than desired in order to appoint someone with the right qualifications and expertise than to compromise on qualifications and expertise.

EN 50126 [50126-1] and iESM Application Note 4 provide guidance on the independent assessment process and the level of independence required.

The European regulation on the adoption of a common safety method on risk evaluation and assessment [CSM-RA] sets mandatory requirements on the selection of an independent organization to perform an independent assessment. These requirements are only applicable within the European Union within the scope of the regulation. However, the requirements are consistent with the approach described in this handbook and may be a useful source of guidance to readers who are not required to follow them.

F. If you are performing an independent assessment, you should carry it out systematically.

The assessor should become familiar with:

- the Hazard Log;
- the plans for the ESM program;
- the safety requirements; and
- the findings and recommendations of any previous independent assessments or safety audits.

This familiarization should be achieved through talking to project staff and preliminary inspection of project documents.

The 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 assessment reports; and
- assessment timescales, including the expected date of issue of assessment reports.

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; and
- demonstrations arranged at the assessor's request.

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

© Abbott Risk Consulting Ltd. 2022

The assessment should examine the development or application process, review the design decisions taken by the project staff which have safety implications and confirm that that risk has been controlled to an acceptable level in accordance with the safety requirements.

The assessor should derive an assessment checklist to guide the enquiries and to record results and evidence. The checklist should be drawn up to meet the assessment requirements, using the documents referenced in the remit. The assessor should note anything that they find that is objectively wrong, whether or not it relates to a checklist item. Note that these checklists are an aid for the 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 organization 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 analyze it for evidence of:

- hazards not previously identified;
- risks incorrectly classified;
- safety requirements not met; and
- changes in the pattern of operational use.

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 analyzing new and changed material.

If the assessment detects a flaw in the ESM program, then the assessor should establish the most likely root cause. The assessor should consider whether this throws doubt on any other aspects of the ESM program, 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 confirmed by checking the same information from other independent sources.

© Abbott Risk Consulting Ltd. 2022

G. If you are performing an independent assessment, you should provide your findings to the project quickly and in a way that supports effective action.

Findings should be communicated to the project manager and project team as soon as possible. You should not wait until the 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

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 system or product may become operational.
- **Category 2** - Issue is sufficiently important to require resolution within a short period after the system or product becomes operational, but the system or product may enter service in the interim, possibly with a protective control measure. The assessor should assess how urgent the resolution of the issue is and propose a period within which it should be resolved.
- **Category 3** – Anything of lesser importance.

Where there are a large number of lower category issues, the 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 rigor or quality in the document that has been reviewed.

A report should be produced at the end of the assessment. It should concentrate on the findings and recommendations of the independent assessment; the requirements and assessment details sections should be brief. It may include recommendations for action by the authorities approving the system or product, 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 authorities, who should then consider any such recommendations and implement promptly any necessary actions.

H. If you receive findings from an independent assessment, you should ensure that the action necessary to deal with them is taken.

You should formulate actions in response to the findings which are sufficient to put things completely right. This may require repetition of tasks that were not carried out completely satisfactorily the first time. It may be appropriate to record any faults discovered in the system itself in the project's Data Reporting, Analysis and Corrective Action System (see iESM Application Note 3). You should ensure that these actions are carried out.

© Abbott Risk Consulting Ltd. 2022

17.2.4 Safety audits

This guidance is applicable to all projects.

I. If you are delivering a system or product, you should arrange for safety audits to be carried out in order to confirm that the project is conforming to plans and procedures that relate to safety.

Safety audits are intended to check that the ESM on a project is adequate and has been carried out in conformance with the plans for the ESM program. If there is no plan for the ESM program, one should be written before an audit is carried out.

The report produced for an audit should include: a judgment on the extent of the project's compliance with the plans for the ESM program; a judgment on the adequacy of the plans for the ESM program; and recommendations for action to comply with these plans or to improve them.

An audit should consider:

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

An audit of ESM activities may be combined with an audit of other project activities.

J. Safety auditors should be sufficiently qualified for their role.

Auditors should have the following qualifications and experience:

- 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 applicable legal and safety regulatory framework; and
- training in ESM.

K. Safety auditors should be independent of the project.

Auditors should be independent of the project and should not have contributed to the design, manufacture, construction, marketing, operation or maintenance of the system or product under assessment. They may work for another organization but this does not have to be the case provided that they do not report to the project manager or the project manager's immediate manager.

L. If you are performing a safety audit, you should carry it out systematically.

The audit process consists of three activities:

© Abbott Risk Consulting Ltd. 2022

1. planning the audit and producing an audit schedule;
2. executing the audit schedule;
3. preparing a report.

The audit schedule should be produced by the auditor and approved by the project manager. Planned activities may be modified to reflect any required change of emphasis based on information gathered during the audit. 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; and
- report distribution and the expected date of issue.

During audit planning the auditor should become familiar with:

- the plans for the ESM program;
- 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; and
- details of project staffing.

This familiarization should be achieved through talking to project staff 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; and
- demonstrations arranged at the auditor's request.

The evidence for compliance or non-compliance with the plans for the ESM program that arises from these activities should be recorded for inclusion in the audit report.

The safety audit is a check for adequacy of the plans for the ESM program and compliance against the plans for the ESM program. 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 plans for the ESM program.

The auditor should derive an audit checklist for the investigation, to guide the enquiries and to record results and evidence. The format of the checklist should mirror that of the plans for the ESM program 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'.

© Abbott Risk Consulting Ltd. 2022

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

The audit should check that any standards or procedures called up by the plans for the ESM program have been correctly applied. It should also check that there is traceability from the plans for the ESM program 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.

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 confirmed by checking with other independent sources.

M. If you are performing a safety audit, you should provide your findings to the project quickly and in a way that supports effective action.

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 plans for the ESM program.

The guidance provided above on providing findings of an independent assessment is also applicable to a safety audit.

N. If you receive findings from a safety audit, you should ensure that the action necessary to deal with them is taken.

The guidance provided above on acting on findings of an independent assessment is also applicable to a safety audit.

17.3 Sources of further guidance

Chapter 6 provides guidance on safety planning.

Section 8.2.2 provides guidance on risk estimation principles.

iESM Application Note 3 provides guidance on Data Reporting, Analysis and Corrective Actions Systems.

RSSB have published various reports on Defect Reporting, Analysis and Corrective Actions Systems, see www.rssb.co.uk

iESM Application Note 4 provides more guidance on Independent Assessment

© Abbott Risk Consulting Ltd. 2022

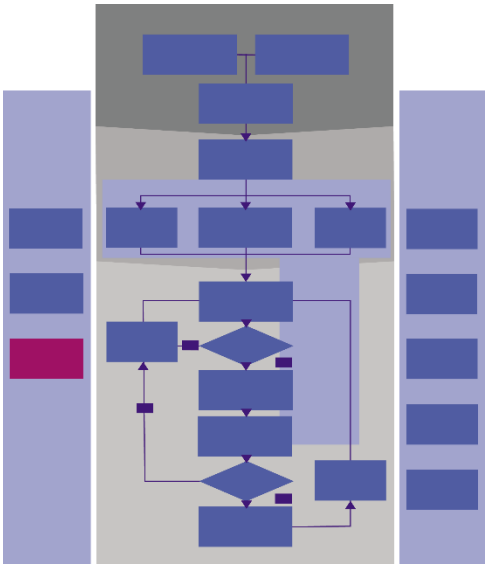
EN 50126 [50126-1] provides some guidance on the independent assessment process and the level of independence required. The European Commission Regulation on the adoption of a Common Safety Method on Risk Evaluation and Assessment [CSM-RA] sets mandatory requirements on the selection of an independent organization. These requirements are only applicable within the European Union. However, the requirements are consistent with the approach described in this handbook and may be a useful source of guidance to readers who are not required to follow them.

© Abbott Risk Consulting Ltd. 2022

18 MANAGING CONFIGURATIONS AND RECORDS

18.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. We use the word **configuration** to refer to the delivered system or product, its components and associated documents and data that need to be kept consistent with the system or product, such as manuals and hazard documentation. A disciplined approach to **configuration management** is required in order to keep the parts of the configuration consistent with each other as things change. This has to be underpinned by meticulous record-keeping.



Your organization must put in place configuration management arrangements that cover everything that is needed to achieve safety or to demonstrate it.

Your organization should keep track of changes to everything that is needed to achieve safety or to demonstrate it, and of the relationships between these things. This is known as **configuration management**. Your configuration management arrangements should help you to understand what you have got, how it got to be as it is and why it is that way.

To do this, your configuration management arrangements should let you:

- uniquely identify each version of each item;
- record the parts of each item (if it has any);
- record the relationships between the items;
- define precisely actual and proposed changes to items; and
- record the history and status of each version of each item.

You should decide the level of detail to which you will go: whether you will keep track of the most basic components individually or just assemblies of components. You should go to sufficient detail so that you can demonstrate safety.

If you are in doubt about any of the above, you cannot be sure that all risk has been controlled.

© Abbott Risk Consulting Ltd. 2022

Before a system or product is placed into service, you should ensure that there are arrangements in place to continue configuration management during service.

Full and auditable records of all activities that affect safety must be kept.

You should keep records securely until you are confident that nobody will need them (for example, to support further changes or to investigate an incident). Often, if you are changing the railway, you will have to keep records until the change has been removed from the railway. You may have to keep records even longer in order to fulfill your contract or comply with legislation or standards.

Your organization should keep records to support any conclusion that risk has been controlled to an acceptable level. You should also keep records that allow you to learn from experience and so contribute to better decision making in the future.

Your records should include evidence that you have carried out the planned ESM activities. These records may include (but are not limited to):

- the results of design activity;
- safety analyses;
- tests;
- review records;
- the Hazard Log;
- records of incidents, including near misses and accidents;
- maintenance and renewal records; and
- records of decisions that affect safety.

The number and type of records that you keep will depend on the extent of the risk.

18.2 Guidance

18.2.1 Introduction to the guidance

Configuration management and record keeping are linked. One of the functions of configuration management is to ensure that the 'information world' (of records) and the 'real world', which includes the delivered system, are in step. If you cannot be sure of this, then you cannot be sure that the evidence that you have collected for safety actually reflects the real world and you cannot build a convincing argument for safety.

This chapter is written for:

- 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.

Guidance is structured under the following checklist items:

A. If you are producing a system or product, you should put in place configuration management arrangements that cover everything that is needed to achieve safety or to demonstrate it.
B. If you are producing a system or product, you configuration management arrangements should reflect good practice in configuration identification.

© Abbott Risk Consulting Ltd. 2022

C. If you are producing a system or product, your configuration management arrangements should reflect good practice in configuration control.
D. If you are producing a system or product, your configuration management arrangements should reflect good practice in configuration status accounting.
E. If you are producing a system or product, you should audit your configuration management arrangements.
F. If you are producing safety-related software, your configuration management arrangements should cover the software and be suitable for this purpose.
G. If you are producing configurable safety-related software, you should place the configuration data under configuration management.
H. If you are producing configurable safety-related software, you should specify the structure of these data.
I. If you are producing configurable safety-related software, you should ensure that the preparation and transmission processes for configuration data are of sufficient integrity.
J. If you are carrying out activities that affect safety, you should keep full and auditable records of these activities.

18.2.2 Configuration Management

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.

ISO 10007 [10007] is an international standard for configuration management which divides configuration management into four activities and introduces some widely-understood names for these activities. According to ISO 10007, there are four main configuration management activities:

- **configuration identification** covers the selection of items to place under configuration management (referred to as **configuration items),** assigning unique identifiers to configuration items and establishing baselines;
- **configuration control** covers the control of changes to configuration items and the establishment of baselines;
- **configuration status accounting** covers the maintenance of data about configuration items and the preparation of reports from this data;
- **configuration auditing** covers checking whether configuration management arrangements are effective and being complied with.

A. If you are producing a system or product, you should put in place configuration management arrangements that cover everything that is needed to achieve safety or to demonstrate it.

Unless your organization has comprehensive procedures for configuration management which you are following, you should write a configuration management plan detailing how this will be achieved. You should ensure that you follow your procedures or your plan.

The project manager will normally be responsible for setting configuration management policy and defining processes for configuration control.

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 list of the types of configuration items;

© Abbott Risk Consulting Ltd. 2022

- responsibilities for configuration management within the project, including the person responsible for approving updates to configuration items;
- the baselines that will be produced;
- the version control arrangements;
- the change control process;
- software configuration management arrangements (if required); and
- any configuration management tools used.

EN 50129 [50129] provides requirements for configuration management of electrical, electronic and programmable electronic railway systems and products.

B. If you are producing a system or product, your configuration management arrangements should reflect good practice in configuration identification.

The identification of configuration items should be started during the early stages of project definition. There may be a hierarchy 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).

Configuration items for a system or product should include, as a minimum, requirements, design, software, significant tools, verification and validation information and key ESM deliverables.

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 should be established at major points in the System Lifecycle as a departure point for the control of future changes.

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.

Variants of an 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).

© Abbott Risk Consulting Ltd. 2022

C. If you are producing a system or product, your configuration management arrangements should reflect good practice in configuration control.

Any changes to an item placed in a baseline 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.

D. If you are producing a system or product, your configuration management arrangements should reflect good practice in configuration status accounting.

The following information should be maintained for each item:

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

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.

Configuration management requires a means of storing and controlling information about 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 as part of the evidence for the safety of the system.

E. If you are producing a system or product, you should audit your configuration management arrangements.

You may carry out audits of the configuration management process or audit specific baselines to check that they are complete and consistent. It is normally sensible to do both.

F. If you are producing safety-related software, your configuration management arrangements should cover the software and be suitable for this purpose.

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

- application programs;

© Abbott Risk Consulting Ltd. 2022

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

EN 50128 [50128] and EN 50657 [50657] provide requirements for configuration management of software in railway systems and products.

G. If you are producing configurable safety-related software, you should place the configuration data under configuration management.

Modern software is highly configurable. A significant number of failures result from errors in the configuration of a particular installation of software rather than from the development of the software in the first place. Moreover, an error in configuration data may lead to complex and subtle hazards of the system that are hard to identify and correct.

Therefore, it is important that as much attention is paid to the configuration of software as to its design and development.

There are two main classes of configuration data:

- that which describes how the software is to operate, the configuration of the actual software components; and
- that which describes the operational environment in which the software is to operate, for example the track layout, or the description of the timetable.

Configuration data may be largely static (for instance, track layout), or it may be dynamic, entered by people during the operation of the system (for instance, train delays).

You should treat the integrity of configuration data, with the same degree of importance as you treat that of the software itself. The approach taken to creating the data should be as rigorous as that taken during software development.

You should analyze the software to establish, for each item of data, any hazards which incorrect values might cause.

When doing this you should consider at least the following ways in which data may be incorrect (this list may not be complete):

- Omission of data;
- Corruption of data;
    - Duplicate or spurious entries,
    - Erroneous/corrupt data that is structurally correct,
    - Structural faults,
    - Type or range faults,
    - Value errors where the value is plausible but wrong,
    - Referential integrity failure between data,
    - Volume, too much/little data,
    - Incorrect ordering of data.

© Abbott Risk Consulting Ltd. 2022

Note: errors in some data items can cause unpredictable results. It may be simplest to regard these as potential causes of all hazards.

There is no precise agreement on how to treat data of different integrity but it may be useful to assign SILs to data items, in order to focus attention on the most critical. This may be done by identifying the highest SIL of any function which might deliver a hazardous output as the result of an incorrect value of this data item.
Further guidance on managing configuration data is available in EN 50128 [50128] and EN 50657 [50657].

H. If you are producing configurable safety-related software, you should specify the structure of these data.

When developing software that uses configuration data, you should specify both the grammar (that is the structure) and the lexicon (the permitted values) of the data. This specification should be complete and consistent. The specification of the data should form part of the overall specification of the system, and should be produced with the same degree of rigor as the rest of the specification.

This specification should also include a description of the manner in which the data is to be stored, including the data formats to be used (for example, the format for real numbers, the character set of text), and the manner in which the data are to be used (for example, which values represent the end of a record).

You should describe, as accurately as possible, the meaning of the data and the manner in which it is to be used. There are likely to be connections between different data items. One data item may refer to another data item or there may be a relationship between the values of the two items. You should document these connections.

You should consider how to detect errors in the data. You should consider the use of error detecting codes, sanity checks, and consistency checks. Checks should be considered both during the preparation of the data, and when the system is being used. Be careful however with automatic error correction in case it should create incorrect data. Corruption in storage and transmission may be more safely handled by requesting that data be sent again.

Your specification should describe error detection mechanisms and define what the system should do if it detects an error. Where practicable, software that is presented with erroneous configuration data should fail in a manner such that it maximizes safety, while indicating the failure and, when it is known, its cause. Failures should be recorded in order that the causes may be investigated. Changes in error rate may indicate a failure in a communication medium (for example, a loose connection), or a change in the operational environment (for example, increased interference from new equipment).

I. If you are producing configurable safety-related software, you should ensure that the preparation and transmission processes for configuration data are of sufficient integrity.

Guidance on ensuring that transmission processes for configuration data are of sufficient integrity is provided in iESM Application Note 3.

© Abbott Risk Consulting Ltd. 2022

18.2.3 Record keeping

Up-to-date and accurate records are essential if you are going to take decisions about your work safely and efficiently and review the way you do your work effectively. You might also need to keep records for legal purposes.

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

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

J. If you are carrying out activities that affect safety, you should keep full and auditable records of these activities.

You should keep adequate records of ESM activity (safety records), to provide evidence that these activities have been carried out.

The extent of the safety records maintained by a project will depend on the complexity and level of risk presented by the project. The activities carried out and the records kept should be sufficient to provide a basis for controlling the risk and evidence that the risk has been controlled. 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 back-up safeguards should be employed to ensure their integrity.

When setting up record-keeping arrangements for a project, you should consider taking the following steps to assist with keeping the records consistent:

- Create and maintain a project glossary to help people to use terms and abbreviations consistently;
- Create and maintain a project tree which shows the relationship between documents; and
- Provide facilities for maintaining cross-references (or some people say, 'traceability') from one document to other documents that it should be consistent with. This will make it easier to check that the documents are consistent.

18.3 Sources of further guidance

iESM Application Note 3 provides guidance on ensuring that transmission processes for configuration data are of sufficient integrity.

ISO 10007:2003 [10007] is a useful general reference for Configuration Management.

EN 50129 [50129] provides requirements for configuration management of electrical, electronic and programmable electronic railway systems and products.

EN 50128 [50128] and EN 50657 [50657] provide further guidance on managing configuration data.

© Abbott Risk Consulting Ltd. 2022

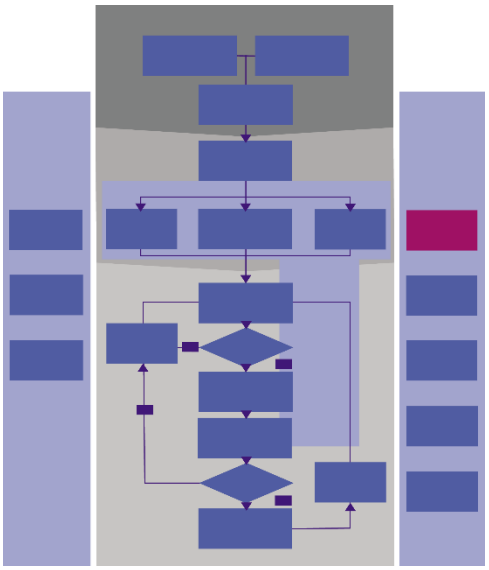
Part VI: Team Support

© Abbott Risk Consulting Ltd. 2022

19 MANAGING SAFETY RESPONSIBILITIES

19.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. In order to make sure that a safety-related activity is carried out, it is necessary to give one or more people responsibility for carrying it out.



Your organization must identify and write down safety responsibilities for its staff.

Everyone within the organization should have clear responsibilities and understand them. Your organization should identify who is accountable for the safety of work. This should normally be the person who is accountable for the work itself. They will stay accountable even if they ask someone else to do the work for them.

The organization should be set up so that its people work together effectively to meet this overall responsibility. Everyone should have clear responsibilities and understand them. People's responsibilities should be matched to their job. Anyone whose work creates a risk should have the knowledge they need to understand the implications of that risk and to put controls in place.

The organization that takes the lead in delivering a project should make sure that the other organizations are clear on their safety responsibilities and that these responsibilities cover everything that needs to be done to ensure safety.

Your organization must give people who have safety responsibilities sufficient resources and authority to carry out their responsibilities.

When people are given safety responsibilities, they should also be given the resources and authority that they need to carry out these responsibilities.

© Abbott Risk Consulting Ltd. 2022

Your organization must keep records of the transfer of safety responsibilities. Anyone who is taking on safety responsibilities must understand and accept these responsibilities. Anyone who is transferring responsibility for safety must pass on any known assumptions and conditions that safety depends on.

This principle will be relevant when a project delivers a system or product to another organization but there may be other occasions on which safety responsibilities are transferred as well.

19.2 Guidance

19.2.1 Introduction to the guidance

ESM is a team activity, involving people with different backgrounds from across the organization and outside it. Therefore, an important part of ESM is the allocation of safety roles with clearly defined safety responsibilities.

This chapter describes some common safety roles and the related responsibilities, and explains how they can be allocated and transferred, both within an organization and between organizations.

Responsibility is not necessarily the same as accountability. You are responsible for something if you are entrusted with making sure that it happens. To be accountable for something means that you can be called to account if it does not happen. Generally, managers remain accountable for ESM performance even though they may delegate responsibility for ESM activities.

This chapter is written for:

- managers responsible for the appointment of staff to safety-related tasks or for determining organizational structure; and
- anyone performing an assessment of personnel competence.

Guidance is structured under the following checklist items:

A. If you assign someone to a safety-related role or give them a safety-related task, you should define and write down that person's safety responsibilities and check that they accept them.
B. Senior management in your organization should allocate responsibilities for safety.
C. Managers who are accountable for delivering systems and products should also be accountable for the safety of these systems and products.
D. Your organization should find out and record the limits of its responsibilities and how its responsibilities relate to those of other organizations.
E. If you transfer safety responsibility to someone else in your organization, you should confirm that the other party accepts the responsibility and make sure that you pass on all relevant safety information.
F. If your organization transfers safety responsibility to another organization, your organization should confirm that the other organization accepts the responsibility and make sure that it passes on all relevant safety information.

19.2.2 Defining safety responsibilities

A. If you assign someone to a safety-related role or give them a safety-related task, you should define and write down that person's safety responsibilities and check that they accept them.

You should only give responsibility to someone who is prepared to accept it.

© Abbott Risk Consulting Ltd. 2022

The safety responsibilities related to the role or task may include reducing the risk of component failure, providing accurate technical manuals, ensuring that maintenance is performed in a timely and efficient manner, and so on.

Safety roles and responsibilities should be clearly defined and documented. The responsibilities assigned to individuals should be documented and made freely available within the organization.
The documentation should identify:

- the various organizational positions;
- the associated responsibilities and authorities for ESM; and
- the communication and reporting channels.

When someone is given a safety-related task, they should be given a task description, detailing their specific responsibilities, the authority that they will carry, and their lines of reporting.

Anyone assigned a safety-related role or task should confirm that they understand and accept the role or task description before their assignment is confirmed.

The definition of safety responsibilities for roles should be periodically reviewed.

In some cases, responsibility may be limited to working in accordance with a work plan and reporting defects and deviations to someone else. In other cases, safety responsibility will include deciding what actions you are going to take to improve safety or prevent a reduction in safety.

B. Senior management in your organization should allocate responsibilities for safety.

Responsibilities for safety should be allocated from the top of the organization downwards. Senior management should assign safety responsibilities to sub-ordinate line managers. In turn, the line managers may assign project managers to a project, or staff directly to tasks.

An organization performing safety-related work will commonly make one or more senior managers responsible for setting safety policy and safety goals, defining other safety responsibilities, granting safety approval, and establishing communication channels for safety-related information. They will typically have a high level of authority within the organization and considerable operational experience and technical knowledge. Their responsibilities may include:

- setting, maintaining and monitoring safety policy;
- ensuring that ESM arrangements are effectively implemented and maintained;
- agreeing the safety classification of projects;
- endorsing key safety documentation;
- monitoring the ESM performed; and
- appointing independent assessors.

There should be some form of organizational structure chart available to all employees, containing details of the organization's safety roles.

Safety roles and their responsibilities should be regularly reviewed to ensure that they are still relevant.

© Abbott Risk Consulting Ltd. 2022

C. Managers who are accountable for delivering systems and products should also be accountable for the safety of these systems and products.

A basic principle of ESM is that those whose activities create a risk should be accountable for controlling that risk. This implies that safety responsibility should be an integral part of the responsibilities of management and not divorced from responsibilities in other areas.

The staff performing ESM on a project may have a second, independent reporting line to a senior manager responsible for ESM across the organization. However, this does not mean that they are not part of the project.

The managers responsible for a project should ensure that the ESM activities on the project are performed efficiently and effectively. They may appoint a specialist to lead the ESM activities on the project but they should be familiar with what is being done and with any significant safety issues. They should:

- assign sufficient people and other resources to carry out the program of ESM activities:
- ensure that staff performing ESM are competent for their jobs, providing training if needed; and
- monitor the ESM performed.

D. Your organization should find out and record the limits of its responsibilities and how its responsibilities relate to those of other organizations.

You should record the railway system boundaries that describe the limits of your responsibility. These boundaries may be based on particular railway components or by defined geographical boundaries along a line of route.

You need to understand this to react effectively to safety issues. If you become aware of an issue that falls within your area of responsibility then you should resolve it. If you become aware of an issue that falls within someone else's area of responsibility then you should bring it to their attention so that they can resolve it.

You should also record the limits of your work activities, so that you can understand where your responsibilities begin and end.

Where the part of the railway or the work you do has a boundary with another part of the railway or organization then you may find that the boundary and the protocols for managing it are clearly defined in interface standards and procedures for the railway. Where an interface standard is mandatory and the other party has told you that there are no areas where they do not comply, then you are entitled to assume that it will indeed be complied with.

However, if there could be any doubt about where safety responsibilities begin and end, the organizations on both sides of the boundary should agree in writing where the boundary is. This agreement is to prevent additional safety risks from arising and to make sure that everything that needs to be maintained is covered. This might include sharing information about the type of work that you are both going to do so that you can understand what effect it will have on safety at the boundary.

© Abbott Risk Consulting Ltd. 2022

19.2.3 Transferring safety responsibilities

E. If you transfer safety responsibility to someone else in your organization, you should confirm that the other party accepts the responsibility and make sure that you pass on all relevant safety information.

Transfer of safety responsibilities may occur within an organization in a number of circumstances including the following:

- one project manager replaces another;
- (within a product organization) a project manager hands over a completed development to a manager with a product support role; and
- (within an operating organization) a project manager hands over a completed project to the operating function.

Typically, the manager accepting responsibility will take on all the safety responsibilities that the relinquishing manager had, although the relinquishing manager will remain accountable for his or her past actions.
Many different situations may occur, but two fundamental points should be observed:

- No responsibility should be transferred until the accepting manager confirms in writing that they are prepared to accept it.
- The relinquishing manager should make sure that all relevant safety information is recorded and that the records are up-to-date.

When a system is handed over, all information relevant to the safe operation of the system should be passed on to whoever is accepting the system.

Table 19-1 provides a checklist of types of information. You should consider each item in this checklist and include the item in the information to be passed over if it is relevant.

Typically, the relinquishing manager passes on a good deal of this information by handing over an up-to-date and comprehensive Hazard Log for the project and by passing on a comprehensive list of assumptions and application conditions (see chapter 16).

A.	System description, including details of interfaces and operational environmental requirements;
B.	hazards, precautions and safety features of the system;
C.	safety information for operators of the equipment or system;
D.	detailed instructions for the operation, servicing and maintenance of the equipment, including operating and technical handbooks, parts and spares identification lists, drawings, and so on;
E.	installation details, including calibration, verification testing, training requirements, inspection schedule, and decommissioning requirements;
F.	details of responsibilities to be transferred, including maintenance of the Hazard Log, training, system maintenance, and so on;
G.	details of items to be transferred, including hardware, software, and documentation;
H.	procedures for fault reporting and change control, including approval; and
I.	details of training requirements, including routine operation, emergency procedures, maintenance, and so on.

Table 19-1 Checklist of Information to be Passed on When Handing Over a System or Product

© Abbott Risk Consulting Ltd. 2022

F. If your organization transfers safety responsibility to another organization, your organization should confirm that the other organization accepts the responsibility and make sure that it passes on all relevant safety information.

When responsibility for the system's operation is handed over to another party, risk may then be created by the organization accepting the system, and therefore some safety responsibilities are also transferred. However, the organization transferring responsibility will retain accountability for the work it did in the past.

Typically this occurs when a supplier completes a contract for the supply of a safety-related system.
Exactly which areas of safety responsibility are transferred to the customer and which remain with the supplier will be determined by the law and the contract. The contract may leave the supplier with responsibility for maintenance, for instance, in which case associated safety responsibilities will also remain with the supplier.

In any case, the supplier will remain accountable for their past actions.

Many different situations may occur, but two fundamental points should be observed:

- No responsibility should be transferred until the accepting organization confirms in writing that it accepts the responsibility.
- The supplier should make sure that all relevant safety information is recorded and transferred.

Table 19-1 provides a checklist of types of information. You should consider each item in this checklist and include the item in the information to be passed over if it is relevant.

Typically, the relinquishing manager passes on a good deal of this information by handing over an up-to-date and comprehensive Hazard Log for the project and by passing on a comprehensive list of assumptions and application conditions (see chapter 16). Your organization may also hand over a safety report, if it is preparing one. The system or product supplier will usually retain a copy of the documents handed over, and agreement is needed on who will hold the master document.

19.3 Sources of further guidance

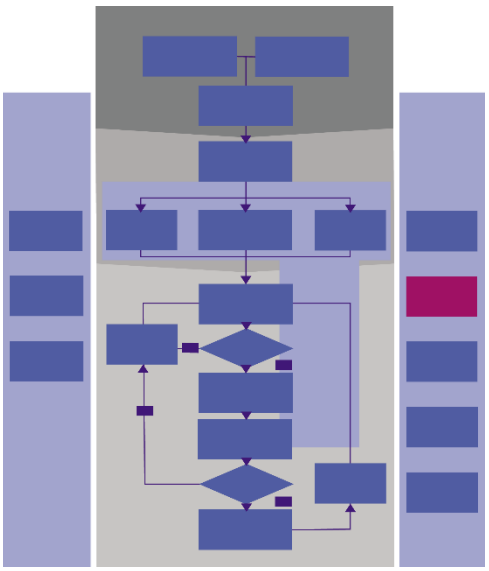
Chapter 16 provides guidance on maintaining a Hazard Log and on managing assumptions and application conditions.

© Abbott Risk Consulting Ltd. 2022

20 PROMOTING A SAFETY CULTURE

20.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. If staff are to work together effectively to deliver safety, they need to share positive values and attitudes towards safety.



Your organization must make sure that all staff understand and respect the risk related to their activities and their responsibilities, and work effectively with each other and with others to control it.

The people leading your organization should make sure that:

- staff understand the risks and keep up to date with the factors that affect safety;
- the organization is adaptable enough to deal effectively with abnormal circumstances;
- staff are prepared to report safety incidents (even when it is inconvenient or exposes their own errors) and management respond effectively;
- staff understand what is acceptable behavior;
- staff are reprimanded for reckless or malicious acts and are encouraged to learn from errors[4];
- the organization learns from past experiences and uses the lessons to improve safety; and
- they set a personal example.

20.2 Guidance

20.2.1 Introduction to the guidance

An organization's safety culture is its general approach to and attitude towards safety.

[4] James Reason [Reason] refers to an organizational culture that meets this criterion as a 'just culture'.

© Abbott Risk Consulting Ltd. 2022

In a good safety culture, safety always comes first, and this will be apparent in the work that the organization carries out. Safety is built into the organization's products, and its safety procedures support what is already being achieved.

In an organization with a good safety culture, everyone:

- is aware of the importance of safety;
- makes safety the highest priority in all that they do;
- continually strives to improve safety; and
- understands the parts of the law and other regulations that are relevant to them.

The benefits of nurturing a good safety culture are that:

- safety is built into the organization's products and systems;
- potential hazards and failures are detected and eliminated or controlled early;
- the organization's products are safe and visibly so;
- the organization realizes efficiencies and cost savings; and
- the risk of not conforming to legal obligations is reduced.

A good safety culture will enhance an organization's reputation, whereas a single major incident can ruin it. Indeed a major incident can mar the reputation of the industry as a whole, and cause harm to many of the interdependent organizations that contribute to and rely on the industry's success.

This chapter provides guidance on promoting a good safety culture and explains the key role of an explicit safety policy in doing this. It describes the content of safety policy statements and how an organization may implement them.

This chapter is written for directors and managers of organizations performing safety-related work.

Guidance is structured under the following checklist items:

A. The senior management of your organization should promote a healthy safety culture and exhibit leadership in this area.
B. Your organization should have safety as an explicit primary goal.
C. The senior management of your organization should make sure that staff are aware of the organizations' goals for safety.
D. The senior management of your organization should set specific targets for safety at an organizational level and work towards them.
E. The senior management of your organization should take action to achieve its targets, monitor progress towards its goals and targets and revise its plans where necessary.

20.2.2 Safety culture and leadership

A. The senior management of your organization should promote a healthy safety culture and exhibit leadership in this area.

A healthy safety culture has the following elements:

- Staff understand and share the organization's commitment to safety;
- There is compliance with applicable standards and procedures;
- There is a commitment to getting things right first time;
- There is intolerance of poor standards of work;

© Abbott Risk Consulting Ltd. 2022

- Staff understand that risk is not constant and that new hazards need to be identified and managed as they arise;
- The organization learns from incidents and uses this learning to improve safety;
- Information about risk is widely shared; and
- When something is found to be wrong it is corrected promptly.

Safety culture can deteriorate, particularly where repetitive tasks can result in perceived familiarity and a false sense of security. Your organization should put measures in place that minimize the potential for complacency, such as varying people's tasks and encouraging ownership.

Management should nurture and encourage good safety practices, monitor safety, and provide the necessary resources.

Management should show an example by making safety a priority in their day-to-day activities and by behaving as they wish their staff to behave.

20.2.3 Safety goals and targets

B. Your organization should have safety as an explicit primary goal.

Your organization should demonstrate a top-level commitment to safety. This commitment should cover the safety of all people affected by your work.

If you set a goal for reducing risk to a certain target level, you should keep this level under review and reduce it further if this become possible.

You should communicate this commitment throughout your organization and ask your staff to share it.

C. The senior management of your organization should make sure that staff are aware of the organizations' goals for safety.

The senior management of your organization should publish a safety policy which covers the following issues:

- confirmation that safety is a primary goal for the organization;
- definition of management's responsibility and accountability for safety performance;
- the responsibility of everyone in the organization for ensuring safety;
- the provision of assurance that products meet safety requirements;
- the continual improvement in safety within the organization;
- compliance with regulations and standards; and
- taking all reasonable steps to reduce risk.

Absolute safety cannot be guaranteed and attempting to achieve it can distort the allocation of resources, so safety should be balanced against other factors.

This means that:

- although safety should be a primary goal, it is not the only goal;

© Abbott Risk Consulting Ltd. 2022

- pursuit of safety at all costs is not advisable; and
- judgment is required to know when to stop trying to reduce risk.

Everyone in the organization should be made aware of the importance of safety and of the organization's safety policy. The methods for achieving this will vary according to the size and type of the organization. It may be possible with smaller organizations to provide direct briefing of the safety policy. With larger organizations, cascade briefing may be more practical.

D. The senior management of your organization should set specific targets for safety at an organizational level and work towards them.

Chapter 5 provides guidance on setting targets that are specific to systems or products that you deliver. In addition to this, your organization should set targets for safety at an organizational level. To do this, your organization should:

- understand current levels of safety performance;
- identify relevant legislation;
- establish safety targets that are consistent with relevant legislation and your organization's goals for safety;
- initiate action to meet the targets; and
- initiate action to collect data about progress towards the targets (see chapter 15).

E. The senior management of your organization should take action to achieve its targets, monitor progress towards its goals and targets and revise its plans where necessary.

The senior management of an organization should ensure that:

- there is management commitment to following the safety policy;
- everyone in the organization is aware of the importance of following the safety policy;
- the necessary training and resources are provided;
- the way that the organization performs ESM is monitored and improved;
- the safety of the organization's products is monitored and improved; and
- the organization is regularly audited to assess its performance with regard to safety.

Management should assign responsibilities for implementing the actions required and provide the necessary resources to carry out these actions. This will include personnel with suitable background and training, as well as equipment.

Management should encourage all staff to improve the safety of their work. Management should provide an environment in which staff feel able to bring safety shortcomings to management attention without fear of recriminations.

Management should check that the safety policy is being implemented. Typically, this will be done with a rolling program, which ensures that every aspect of the policy is monitored over a period of a few years.

© Abbott Risk Consulting Ltd. 2022

Typically, an aspect of the safety policy is monitored on a random selection from all the relevant activities of the organization. In some cases it may be sufficient to carry out a simple inspection of these activities. In other cases it may be appropriate to commission a formal audit. The guidance on safety auditing in section 17.2.4 may be used as a basis for such an audit.

The way in which the safety policy is implemented should be regularly reviewed to check that it is consistent with good practice, which evolves over time.

If any of these monitoring tasks reveals the need for action, management should act as required.

20.3 Sources of further guidance

Chapter 5 provides guidance on setting targets that are specific to systems or products.

Chapter 15 provides guidance on monitoring levels of safety.

Section 17.2.4 provides guidance on safety auditing.

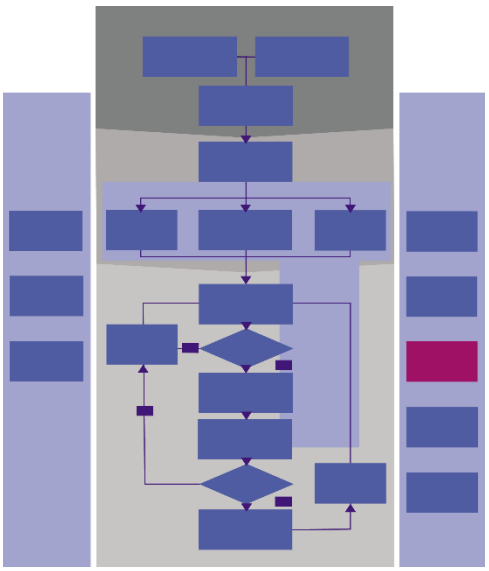
'*Managing the Risks of Organizational Accidents*' [Reason] describes how safety culture contributes to risk and the elements of a good safety culture.

© Abbott Risk Consulting Ltd. 2022

21 BUILDING AND MANAGING COMPETENCE

21.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. The staff who carry out ESM activities should be competent to do their jobs.



Your organization must make sure that all staff who are responsible for activities that affect safety must be competent to carry them out.

The people leading your organization should be competent to set and deliver safety responsibilities and objectives for the organization.

Your organization should set requirements for the competence of staff who are responsible for activities that affect safety. That is to say, it should work out what training, technical knowledge, skills, experience and qualifications they need in order to perform their work satisfactorily. This may depend on the help they are given – people can learn on the job if adequately supervised. You should then select and train staff to make sure that they meet these requirements.

Your organization must monitor the performance of all staff who are responsible for activities that affect safety in order to ensure that they carry out their responsibilities competently.

You should regularly monitor the performance of staff who are responsible for activities that affect safety and verify that they meet these requirements.

© Abbott Risk Consulting Ltd. 2022

21.2 Guidance

21.2.1 Introduction to the guidance

To be competent, you must have the necessary training, technical knowledge, skills, experience and qualifications to do *a specific task* satisfactorily. Competence is not a general reflection on someone's overall abilities. Just because you are not yet competent for a specific task does not mean that you are an incompetent person. And conversely, being competent at one task will imply little about your competence for another, unless the two tasks are very similar.

This chapter is concerned with the competence of individuals. See chapter 22 for guidance on managing the competence of suppliers. This chapter does, however, apply to individual contract personnel who work under your organization's supervision.

Competent people still make mistakes. Assuring competence is not a substitute for having processes in place which can catch these mistakes before an accident occurs. Other chapters in this handbook describe such processes.

This chapter is written for:

- those responsible for assigning safety-related tasks to staff; and
- anyone otherwise assessing the competence of staff.

Guidance is structured under the following checklist items:

A. If you assign staff to roles which affect safety, you should specify criteria for the competence that is required for each role.
B. If you assign staff to roles which affect safety, you should ensure that the staff that you assign to the roles are competent to carry them out.
C. If you assign staff to roles which affect safety, you should keep records of competence management.
D. If you assign staff to roles which affect safety, you should ensure that they have the necessary resources and authority to perform their roles.
E. If you supervise staff in roles which affect safety, you should monitor their performance.
F. If you supervise staff in roles which affect safety, you should take steps to develop their competence further.
G. If you are introducing a formal approach to assessing competence within your organization, you may need to make transitional arrangements.
H. Your organization should monitor its competence criteria and arrangements for managing competence and initiate improvement action where required.
I. You should not personally accept a safety-related role for which you are not competent unless you are provided with adequate support.

21.2.2 Specifying competence criteria

A. If you assign staff to roles which affect safety, you should specify criteria for the competence that is required for each role.

Chapter 19 describes how to allocate and document responsibilities for safety-related work.

From these responsibilities, you should derive the activities that someone performing the role must undertake and then derive criteria for the competence that is necessary to perform these activities in a satisfactory manner.

© Abbott Risk Consulting Ltd. 2022

The UK Health and Safety Executive publishes a guide called "*Managing competence for safety-related systems*" [HSE] which describes this process in further detail.

Consider setting competence criteria on:

- knowledge of methods, practices and hazards;
- skills, including the ability to communicate effectively;
- education and training;
- professional status;
- experience; and
- personal attributes such as knowledge of one's limitations and the discipline to remain within these limitations.

Do not just choose competence criteria because they are easily assessed; try to define what is really required to perform the role.

Many tasks require more skills and knowledge than any one person possesses. In that case they will have to be tackled by a team and you should specify the required collective competence of the team as a whole.

In addition to project-specific and non-safety criteria, project managers on safety-related projects and those leading ESM should generally:

- have received training in ESM; and
- be a full member of a professional organization.

Anyone taking a leading role in the design or operation of a safety-related system should be familiar with:

- the applicable law and standards; and
- current good practice.

Annex G of EN 50126 [50126-2] suggests some key competencies for some safety-related project roles.

21.2.3 Assessing staff competence

B. If you assign staff to roles which affect safety, you should ensure that the staff that you assign to the roles are competent to carry them out.

Before someone is assigned a safety-related role, they should be assessed to decide whether or not they meet the competence criteria for the role.

A manager of people performing safety-related roles is also performing a safety-related role and, therefore, competence criteria should be set for this role.

When considering whether a person meets the competence criteria, you should consider:

- technical skills, knowledge and experience;
- leadership and managerial skills; and
- personal attributes such as integrity, confidence and the resolve to resist any pressure to compromise safety.

© Abbott Risk Consulting Ltd. 2022

The assessment is usually done by the individual's manager or a third person. It is usually most effective if the assessor works with the person being assessed when carrying out the assessment.

A proven track record in a job is the most direct evidence of competence. However, it is necessary to show not just that the individuals have held a post for a period of time, but also that their performance has been satisfactory during that period.

Assessment of education, experience and professional status can be checked by direct reference to curricula vitae, which should be kept on file. Examinations or other tests may be used to assess general skills and knowledge, but it is generally more useful to refer to evaluated performance on similar tasks.

It is sometimes useful, or even necessary, to assign a safety-related task to someone who does not yet fulfill the requirements to perform it, but who is likely to gain the necessary qualifications (perhaps through performing the task). This is acceptable, provided that they work under the supervision of an experienced mentor who does fulfill the requirements. The mentor should be accessible to the person being supervised and should take overall responsibility for the work.

When you assess people who have to take safety decisions, you should look for evidence that they have the breadth and depth of competence necessary to take correct decisions. One good way of addressing this is to set scenarios that explore the person's ability to understand and manage the overall safety risk. They should be able to identify the information they need, the communications required with other people and the applicable standards. They should then be able to use their judgment to take the correct decision.

You should look for good practice assessment techniques that are used elsewhere in the industry. Sometimes, assessment standards are dictated by railway industry standards. In other cases, assessment standards are published by professional organizations.

C. If you assign staff to roles which affect safety, you should keep records of competence management.

Your organization should keep up-to-date competence records for all personnel who do safety work, or take safety-related decisions, and make them available to people who allocate the work.

21.2.4 Providing sufficient resources and authority

D. If you assign staff to roles which affect safety, you should ensure that they have the necessary resources and authority to perform their roles.

People who are authorized to do work should also be given responsibilities for putting problems right.

People should not be asked to take responsibility for controlling a risk if they do not have the authority to take the necessary action to control it.

People should be given sufficient resources to carry out their responsibilities. This includes having the information that they need to take sound decisions.

© Abbott Risk Consulting Ltd. 2022

21.2.5 Monitoring performance

E. If you supervise staff in roles which affect safety, you should monitor their performance.

It is not sufficient just to specify and check competence once. Your organization should periodically and routinely check that staff who are responsible for activities which affect safety have the competence and resources that they need.

Most organizations have periodic evaluations of staff performance for business reasons. These evaluations are particularly important for staff performing safety-related work, to re-assess their level of competence for this work. This re-assessment provides information on any additional training that they may need, or whether the person is not suited to this role and should be transferred. Feedback on performance may also come from audits and assessments and from incident evaluations.

It is good practice to assess people by observing them doing the required work, either at the workplace or by setting simulated exercises.

Your organization should regularly review competence records and work allocation to make sure that an authority to work does not lapse through certification expiry or lack of application. It should continue to monitor the integrity of work that is done and look for any lapses in competence. Where competence lapses are identified, you should restore the competence and implement remedial work where lapses may have introduced a safety risk. If you find a competence gap, you should look for alternative ways of managing the work safely. Solutions include mentoring staff or reallocating work to other competent staff until additional training and assessment has been completed.

If review of the occurrence of an incident reveals a lack of competence for someone performing a safety-related role, you should take corrective action straight away.

In the case where a person performing a safety-related task needs to be replaced or retrained, it is necessary to act quickly but with sensitivity.

21.2.6 Developing competence

F. If you supervise staff in roles which affect safety, you should take steps to develop their competence further.

You should keep records and regularly review competencies, work requirements and standards and decide whether any additional training is required. Where you identify training needs, you should make sure that the training is provided to all those who need it.

Those responsible for staff training should make sure that staff skills and knowledge are kept up-to-date. It may be necessary to arrange specific training for the work that they need to do.

Training does not just include formal courses but also distance learning packages, computer-based training and on-the-job coaching from senior staff.

© Abbott Risk Consulting Ltd. 2022

Several professional organizations provide continuing professional development schemes which can help in selecting appropriate training. The members of these organizations are expected to maintain their professional competence through self-managed continuing professional development but the concept is of value to other professionals as well. The schemes generally provide individuals with mentors who periodically assist the individual to set plans for their learning needs and to monitor progress against previous plans. Each individual maintains a log book in which they record planned and actual professional development. Some schemes also provide guidance on the sort of training and experience which should be acquired for different types of work and levels of seniority.

If your organization is arranging its own training, then providing certificates of attendance or of passing a final test can make it easier to assess people later. Certificates should have a limited life.

21.2.7 Introducing and monitoring competence management arrangements

G. If you are introducing a formal approach to assessing competence within your organization, you may need to make transitional arrangements.

When introducing a formal approach to assessing competence, you should check whether the staff currently assigned to safety-related roles meet the competence criteria set for them.

It may be found that the most experienced and capable personnel have not been through the training program that would be required for someone new taking on their job. This does not mean that they should not continue in their roles, and in fact they may be required to coach more junior staff.

It is normal when introducing a formal approach to assessing competence to write some transitional arrangements into the training criteria, which exempt some existing staff from the formal criteria for their current roles, however these arrangements should only apply to staff who have been performing their roles satisfactorily for some time.

H. Your organization should monitor its competence criteria and arrangements for managing competence and initiate improvement action where required.

Your organization should monitor changes in the work that it does and the way in which responsibilities are divided and, if necessary, revise the competency criteria for roles and initiate any necessary training.

Your organization should arrange to periodically review and/or audit the competency arrangements to check that they are being put into action as planned and that they are effective.

If necessary, improvement actions should be defined and implemented.

© Abbott Risk Consulting Ltd. 2022

21.2.8 Obligations on individuals

I. You should not personally accept a safety-related role for which you are not competent unless you are provided with adequate support.

This is a requirement of the codes of practice of several professional institutions.

21.3 Sources of further guidance

Chapter 19 provides guidance on allocating and documenting responsibilities for safety-related work.

Chapter 22 provides guidance on managing the competence of suppliers.

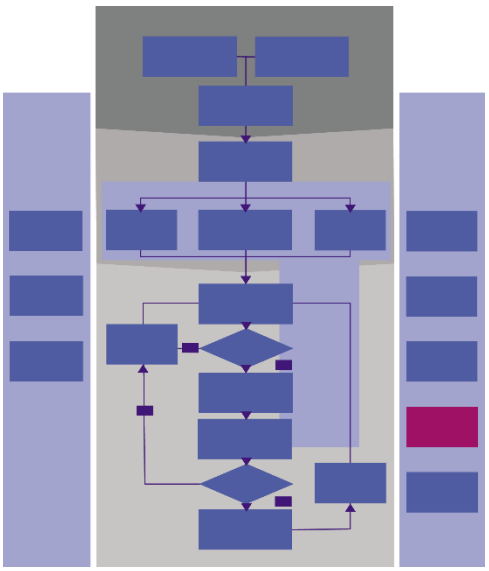
Annex G of part 4 of EN 50129 [50129] suggests some key competencies for some safety-related project roles.

© Abbott Risk Consulting Ltd. 2022

22 WORKING WITH SUPPLIERS

22.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. This activity is needed to make sure that the other activities do not get lost in contractual relationships.



Whenever your organization contracts out the performance of activities that affect safety, it must verify that the supplier is capable of doing the work, including any necessary aspects of engineering safety management.

Your organization should set specific requirements, that are relevant to the work being done, before passing the requirements on to the supplier. You also need to verify that your suppliers are capable of passing requirements on to their suppliers.

A supplier is anyone who supplies your organization with goods or services. You can share safety responsibilities with your suppliers but you can never transfer them completely. If you carry out the **safety responsibilities** activity fully, you will be clear about what safety responsibilities you are sharing.

The capability of a supplier will depend upon its culture, the competence of its staff and its procedures and equipment, among other things.

Whenever your organization contracts out the performance of activities that affect safety, it must verify that the supplier does what they are required to do.

This may be done by auditing the supplier, reviewing assurance material which the supplier provides or inspecting the supplier's deliverables.

© Abbott Risk Consulting Ltd. 2022

22.2 Guidance

22.2.1 Introduction to the guidance

Most organizations rely on suppliers for some element of delivering work. Suppliers generally provide one or more of the following resources:

- products, such as materials, tools, equipment and spare parts;
- individual staff, typically contract laborers; and
- services, for example outsourced repairs and specialist investigation.

This chapter is concerned with the situation where your organizations contract another organization to carry out a task or deliver a product which might affect the safety of your system or product. It is not concerned with contract personnel who work under your organization's supervision. It is good practice to include such personnel within your own competence management arrangements. See chapter 21 for guidance on managing the competence of individuals.

The guidance in this chapter is not concerned with the situation where a sub-contracted task or a procured product is not relevant to the safety of your system or product.

This chapter is written for anyone who is considering contracting other organizations to perform safety-related work.

Guidance is structured under the following checklist items:

A. If you contract out a safety-related task, you should make sure that the supplier is competent to do the work.
B. If you contract out a safety-related task, you should specify what the supplier must do in order to control risk.
C. If you contract out a safety-related task, you should check that the supplier is doing what is required of it.
D. If you procure a safety-related product you should define safety requirements for it and check that these requirements are met.
E. If you contract out a safety-related task or procure a safety-related product, you should inform the supplier about hazard, risks and safety requirements which are relevant to their work.
F. If you contract out a safety-related task or procure a safety-related product, you should co-operate with your suppliers to improve safety.

22.2.2 Assessing the competence of suppliers

A. If you contract out a safety-related task, you should make sure that the supplier is competent to do the work.

A supplier assessment should be proportionate to the risks involved in the work. It need not be extensive where the requirements are straightforward but it should be written down and put on file.

Criteria should be set for the capabilities that a supplier should have to perform the tasks satisfactorily. Typically, these will include requirements that the supplier has:

- a suitable organization with competent personnel;
- the necessary equipment which is adequately maintained;
- a suitable health and safety policy appropriate to the work;
- an ability and commitment to undertake suitable and sufficient risk estimations;
- effective arrangements to control the risks identified;

© Abbott Risk Consulting Ltd. 2022

- effective quality controls; and
- the competence to deliver the contract.

Evidence should then be collected that the supplier meets these criteria. The following documents may provide such evidence:

- a pre-tender Safety Plan;
- responses to a questionnaire;
- a copy of their safety policy and procedures;
- incident records;
- training records;
- curricula vitae for the staff who will be performing the work;
- quality assurance procedures;
- project review and monitoring documents;
- details of previous experience; and
- references from other customers.

You do not need to obtain all of these documents. You need only obtain those documents necessary to provide sufficient evidence.

For complex tenders, a pre-selection procedure might be appropriate, with a detailed assessment of those who are short-listed.

Where your business involves contracting out the same sort of work repeatedly, it may save time to use a list of pre-assessed approved suppliers. You do not necessarily have to set up your own approved supplier scheme; there are a number of industry-wide schemes already in operation. If you use a list of approved suppliers, it should detail the type of work that each supplier has been approved for.

The performance of suppliers on current contracts should be recorded and taken into account if the supplier bids for further contracts.

You should deal with any situations where you are using a supplier who does not have all the competences required. You may do this using your own resources or bringing in additional outsourced resources.

22.2.3 Specifying what suppliers should do

B. If you contract out a safety-related task, you should specify what the supplier must do in order to control risk.

You should produce written specifications of all safety-related work to be done by suppliers and check that the suppliers meet these specifications.

© Abbott Risk Consulting Ltd. 2022

You should make sure that each supplier is fully aware of the risks that it is responsible for controlling, and fully accepts its safety responsibilities. You cannot pass all of your safety responsibilities onto a supplier but you can share responsibilities with them. If you do decide to use a supplier, you should make it clear which safety responsibilities you are sharing and agree with them how you are going to work together to manage safety.

Ways of doing this include:

- insisting that suppliers provide method statements that explain how the risk will be controlled; and
- requiring suppliers to provide certificates of conformity.

You should make sure that your suppliers have processes in place that fulfill the safety, quality and performance standards that you require and deliver the things that you need from them. This includes ensuring that supplied staff are fit and competent to deliver the work that you require from them. For example, you should make sure that the materials and test equipment you use for railway safety applications have been accepted for use and have been correctly handled, maintained and calibrated to meet your safety requirements. Similarly, you should make sure that supplied personnel fulfill your competence and fitness requirements and comply with working time limits.

You should make sure that your suppliers know which records they have to keep and when they must be made available to you.

Where responsibility for work is to be shared with a supplier, you should agree relevant aspects of your plans with the supplier.

You should make sure that your suppliers understand the division of responsibilities, in particular (where appropriate):

- what specification of work they have to follow;
- what work and level of checking they have to do;
- who is responsible for checking that the work has been done correctly;
- who is responsible for site safety;
- what records are required and how they will be recorded;
- the competencies and authorities required for each part of the work;
- who is responsible for making safety decisions about the work; and
- the methods they should use to communicate information about the work.

You should do this for work of a one-off nature, as well as repetitive and regular tasks.

© Abbott Risk Consulting Ltd. 2022

22.2.4 Monitoring suppliers

C. If you contract out a safety-related task, you should check that the supplier is doing what is required of it.

You should monitor work done by suppliers.

For simple requirements it may be sufficient to directly inspect the work being done.

Another way of doing this is by auditing the supplier.

Additional deliverables may also be specified, such as audit and assessment reports, which may be used to check compliance. In other cases a direct audit or assessment of the work may be needed, either by your organization, or by contracting a third party to do this. If a direct audit or assessment is required, then the necessary access to the supplier's information, people and premises should be specified in the contract.

If you find something wrong then you and your supplier should act to put it right.

If you find a problem, you should consider removing a supplier from a preferred supplier list or changing the scope of responsibility granted to that supplier, until they can demonstrate that they have put things right.

You may also have to notify others where a supplier causes a safety incident.

22.2.5 Procuring safety-related products

D. If you procure a safety-related product you should define safety requirements for it and check that these requirements are met.

The safety requirements will normally be integrated with other contractual requirements and the arrangements for obtaining assurance that the safety requirements have been met will normally be integrated with other assurance arrangements.

The degree to which you check that safety requirements are met yourself as opposed to requiring evidence from the supplier will depend upon your confidence in the supplier's processes.

22.2.6 Passing information to suppliers

E. If you contract out a safety-related task or procure a safety-related product, you should inform the supplier about hazard, risks and safety requirements which are relevant to their work.

For guidance on doing this, see section 23.2.2.

© Abbott Risk Consulting Ltd. 2022

22.2.7 Working with suppliers to improve safety

F. If you contract out a safety-related task or procure a safety-related product, you should co-operate with your suppliers to improve safety.

You should work with your suppliers to improve safety.

You should agree with your suppliers how the human factors work will be shared between themselves, and ensure that they all understand their responsibilities.

22.3 Sources of further guidance

Chapter 21 provides guidance on assessing the competence of personnel.

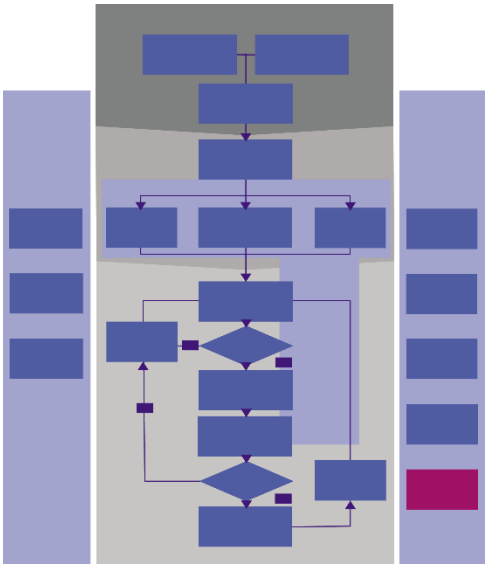
Section 23.2.2 provides guidance on communicating safety-related information to suppliers.

© Abbott Risk Consulting Ltd. 2022

23 COMMUNICATING AND CO-ORDINATING

23.1 Principles from Volume 1

The position of this activity in the generic ESM process is indicated below. There may be more than one organization involved in performing the work and there will certainly be other organizations with whom your organization must deal. These other organizations will all play a part in delivering safety, and communications and co-ordination are required to support that.



If your organization information that someone else needs to control risk, your organization must pass it on to them and take reasonable steps to make sure that they understand it.

Your organization should pass on any relevant information about hazards and safety requirements to its suppliers and customers.

This information may include:

- information about the current state of the railway;
- information about how systems are used in practice;
- information about the actual performance of the railway and its systems;
- information about the current state of work in progress – especially where responsibility is transferred between shifts or teams;
- information about changes to standards and procedures;
- information about an incident;
- problems you find in someone else's work; and
- assumptions about someone else's work that are important to safety.

Communications should be two-way. The people leading your organization will need to make sure that they get the information that they need to take good decisions about safety and then make sure that these decisions are communicated to the people who need to know about them. Similarly, your organization should consult with stakeholders affected by its work to obtain the information that it needs to control risk.

© Abbott Risk Consulting Ltd. 2022

If someone tells you or your organization something that suggests that risk is too high, it must take prompt and effective action.

This action will generally require performing some of the activities described above.

Whenever your organization is working with others on activities that affect the railway they must co-ordinate their engineering safety management activities.

Activities that have potential to affect safety that are split between organizations should be co-ordinated to ensure that the railway is and remains safe. Where changes are being planned, activities between organizations should be co-ordinated to ensure each operational state of the railway is safe to operate. Co-ordination may lead to making complex changes in a particular order or way.

23.2 Guidance

23.2.1 Introduction to the guidance

Safety issues do not respect organizational boundaries. Effective communications and co-ordination are often needed to resolve them.

The sources of information needed to take safety decisions may exist anywhere within your organization, such as a report from a maintenance technician at the front line. Alternatively information may come in to your organization at any point from somewhere else, such as a railway operator or from the general public.

This chapter is written for managers and engineers who have safety-related information that is required by someone else or who need to work or liaise with others in the interest of safety.

Guidance is structured under the following checklist items:

A. Your organization should make arrangements to communicate information that is needed to control risk within the organization.
B. If you have information that someone else needs to control risk, you should pass it on to the other party and take reasonable steps to make sure that it understands it.
C. If someone tells you something that suggests that risk is too high, you should take prompt and effective action.
D. If you communicate information that is needed to control risk, you should consider the needs of the recipient and you should choose a method and a time that reflects the urgency and value of the information relative to any other information that needs to be communicated.
E. If your organization is working with others on activities that affect the railway, all these organizations should co-ordinate their ESM activities under normal conditions.
F. If your organization is working with others on activities that affect the railway and there is a possibility that they may have to deal with an incident, all these organizations should have joint plans for dealing with an incident.

© Abbott Risk Consulting Ltd. 2022

23.2.2 Passing on safety-related information

A. Your organization should make arrangements to communicate information that is needed to control risk within the organization.

Your organization should have arrangements to communicate up-to-date information that is needed to control risk to all those who need to know, at the time and place that they need it. This will help the correct people to take the correct safety decisions.

Decisions taken by management need to be communicated to those at the front line who have to implement the decision. You should communicate requirements to apply standards and procedures throughout your organization, particularly when these requirements change.

Decisions taken at the front line need to be communicated to management.

You should make sure that everyone in your organization knows who to tell if they find information that there is an unacceptable safety risk.

There will probably need to be several different processes for communicating different sorts of information. Do not feel restricted to using formal documents (such as memoranda, user manuals, safety reports and Hazard Log). You may find it effective to communicate information by:

- face-to-face briefings;
- informal documents (such as newsletters, bulletins, electronic mail);
- audio-visual packages; and
- training.

Whatever method you choose, you should make sure that it is auditable.

You should establish communication systems that are capable of use in normal, degraded and emergency situations. In all cases, your organization should have a system to record the safety information that you need to communicate.

For example, someone at the front line should have a way to quickly communicate information about a safety failure or incident to the person who will decide what action to take. Further communications may then be required to quickly gather the necessary information. The decision should then be clearly communicated to the person who has to take the corrective action and, finally, completion of the work should be communicated and recorded.

© Abbott Risk Consulting Ltd. 2022

B. If you have information that someone else needs to control risk, you should pass it on to the other party and take reasonable steps to make sure that it understands it.

Where information about safety risk could have wider implications, your organization should have arrangements to pass the information to someone who has the authority to act on it. This may require communication with other organizations that look after parts of the railway. For example, an axle defect that you find in a railway vehicle may have implications on other vehicles owned by other organizations.

Your organization should make arrangements to pass on the following sorts of safety-related information to people who need it to reduce risk:

- hazards, risk and arrangements to control them;
- limitations on the products and systems that your organization makes and any implications for users and maintainers;
- defects in standards;
- lessons learned, relating to safety; and
- safety-related information about your products, principally to your customers.

In particular, you should make sure that any of your suppliers who are doing safety-related work have all relevant information regarding:

- hazard identification and risk estimations that you have carried out;
- strategies that you have defined to control risk; and
- safety requirements that you have established.

If any of this information changes, then you should make sure that you inform your suppliers of the change promptly.

If one of your suppliers tells you about a safety issue that other suppliers should be aware of, then you should pass the information on.

Considerations of commercial confidence and the expense of providing certain classes of information can make passing necessary information around slow and expensive. To avoid this happening, it is often a good idea to enter into non-disclosure agreements and to agree who will pay for what at the outset of any partnership.

It is common for a single individual on the railways to use a number of systems. When designing a system, the user's interaction with other systems should be taken into account. A failure to adequately communicate information between projects may result in decisions being taken that are detrimental to the safety of the system as a whole, for instance by introducing unnecessary and unwanted inconsistencies between systems used by one person.

Key information includes:

- Characteristics of end users, their capabilities and limitations. In order to understand how safely a system will be used, you need to understand those who will use it.
- How the system is intended to be used. The manner of use and context of the system will have a significant impact on the safety of a system.
- Details of existing and/or similar systems and products. In order to identify human factors safety requirements, you need to understand how existing or similar systems and products are used.

© Abbott Risk Consulting Ltd. 2022

If you employ people who will be affected by a change, you should provide those performing the human factors work with access to them. It is difficult to perform assessment of the human factors issues in a project without access to these people.

C. If you communicate information that is needed to control risk, you should consider the needs of the recipient and you should choose a method and a time that reflects the urgency and value of the information relative to any other information that needs to be communicated.

When you communicate information, you should make sure that the information has been correctly received and is understood by the recipient.

It is good practice for organizations to co-ordinate the flow of safety-related and time-critical information using a dedicated reporting facility (examples range from a maintenance control center to a single telephone hotline). You should make sure that people have the contact details and that the resources you provide are sufficient to manage and prioritize all of the information types that you need to deal with.

Methods of communication include:

- written communication;
- verbal communication; and
- information technology and data systems.

Initially it is often a good idea to pass information on verbally, so that misunderstandings can be quickly resolved. However, communication of safety-related information should be done auditably, so it should be confirmed in writing afterwards.

When you choose a method of communication, you should consider the need to maintain a record of the communication.

Good written communications use clear language and graphics to communicate information in a consistent way. Written communication is particularly effective when you need to communicate the same information to a lot of people, for example:

- communicating requirements using method statements, written specifications or checklists;
- communicating system configuration information using design drawings; and
- communicating system status information using written reports.

If you are using written documents to communicate your requirements, you should make sure that all of your personnel have access to the correct, up-to-date version. You should make sure that the document hierarchy is clearly understood and that documents are consistent with each other.

Good verbal communication requires clear language. Use agreed technical vocabulary and standard English; avoid informal jargon or colloquialisms. It is good practice to use a structured message notation for communicating safety information. This includes the phonetic alphabet and a structured message format that uses positive acknowledgements.

It is good practice for message recipients to repeat verbal messages back to the sender to confirm their understanding. This is particularly important where face-to-face communication is not possible.

© Abbott Risk Consulting Ltd. 2022

It is also good practice to record and store safety-related spoken messages using backed-up information technology systems so that they can be replayed, typically to support incident investigations and support learning to prevent incidents leading to people being hurt.

The internet and mobile telecommunication can be used to quickly make a large amount of information available to a large number of people. You should make sure that processes are in place to maintain communication integrity (including coverage and back-up systems). You should avoid sending out too much information, because the information you want people to use could be overwhelmed by other, less important or less accurate material.

Because this method of communication is largely one way at a time, you should have procedures that require recipients to acknowledge receipt.

Your organization should have a fall-back method to maintain communication in the event of a failure in its telecommunications facilities.

23.2.3 Acting on safety-related information

D. If someone tells you something that suggests that risk is too high, you should take prompt and effective action.

Your organization should have arrangements to:

- capture and record this sort of information;
- decide what action, if any, to take; and
- respond to whoever has provided the information.

If action is necessary, your organization should have arrangements to define the action, assign it to someone and track it to completion.

23.2.4 Co-ordination

E. If your organization is working with others on activities that affect the railway, all these organizations should co-ordinate their ESM activities under normal conditions.

Cross-organization working groups with a focus on safety may be used to co-ordinate activities. If several organizations set up such a working group, they should involve all other interested parties, including users, maintainers and suppliers.

The working group should be given clear terms of reference. It should have the authority to resolve straightforward issues directly, but will need to escalate issues which have a complexity outside its scope, or which are outside its authority (often where significant, unplanned resources need to be expended).

It can be useful to maintain a database of safety issues and to track their resolution.

© Abbott Risk Consulting Ltd. 2022

Your organization should co-operate with the other organizations involved in a project to develop shared procedures and a co-ordinated work plan.

Your organization should co-ordinate human factors work with the other organizations working the project.

Where different organizations are developing multiple systems and products that will be used by the same people, it is important that work is co-ordinated to avoid inconsistency. For example: where two systems or products use the same noise to alert the driver to a problem, confusion is likely to result.

Where multiple projects are part of a wider program you should have a program-wide human factors co-ordinator. This will improve communication and visibility of human factors within a program consisting of many projects. The program-wide human factors co-ordinator will be responsible for making sure that projects co-ordinate their activities, and also aid the discovery of conflicts.

All co-ordination arrangements should be put in writing so that they can be audited.

F. If your organization is working with others on activities that affect the railway and there is a possibility that they may have to deal with an incident, all these organizations should have joint plans for dealing with an incident.

If your organization potentially has to deal with an accident or emergency, then it should have contingency plans in place to co-ordinate responses with others. In order to do this:

- Your organization will need to have arranged, in advance, lines of communication and control and have set up dedicated communications facilities, such as land lines or radio communications.
- Your organization should have agreed arrangements in place for dealing with emergency services and for communicating with the general public and the media.

It is good practice that emergency plans are established. These arrangements should be sufficient to control additional risk introduced as a result of an emergency, and should be briefed to all persons who may be affected by such incidents, so that everyone is aware of the actions to take in event that an emergency arises.

These arrangements should be reviewed regularly and updated as necessary.

Typical risks, not exhaustive, considered as part of emergency plans are:

- derailment or collision of trains
- fire and arson
- terrorism
- trespass and vandalism
- flood and other extremes of weather
- oil / chemical spills; and
- high-risk activities such as work in confined spaces, high temperature work and other ‘Permit to Work’ activities; and
- loss of critical equipment and systems.

© Abbott Risk Consulting Ltd. 2022

Emergency plans should include arrangements for key personnel to communicate with each other and with other external agencies. Details of local hospitals, emergency services, utility services and fire evacuation plans are all examples of information that should be made available in emergency arrangements. Isolation of power, gas and water supplies may be necessary to provide a safe working environment at the site of an emergency.

Depending on the scale of the emergency a command structure may be required to manage the incident, which will involve your organization and the emergency services and other relevant agencies. Interfaces with these agencies and mobilizing arrangements should be described and understood by those involved. Control centers may be required from which to operate and to act as a focus for information in and out.

Availability of key personnel will have to be ensured, with the right skills in the right locations able to respond within appropriate timescales. Alternative facilities and arrangements for staff when buildings/depots/offices are unavailable due to the emergency will have to be considered.

Arrangements to ensure key systems are maintained, and the continued supplies of critical materials, tools and equipment, will also be considered as part of the arrangements. Back-ups of essential computer-based information will be planned as part of the routine day-to-day management, so that your business can be operational as soon as possible after the emergency.

Your organization will need to ensure that the access to the assets that you might need to deal with an emergency is not impeded.

It is good practice to test that your emergency arrangements will work using simulated exercises such as fire drills, desktop exercises and practical simulations.

23.3 Sources of further guidance

No sources of further guidance have been identified for this chapter.

© Abbott Risk Consulting Ltd. 2022

Part VII: Supplementary Material

© Abbott Risk Consulting Ltd. 2022

24 GLOSSARY

This glossary defines the specialized terms and abbreviations used in this volume. Volume 1 uses simpler and more restricted terminology, which is introduced in the volume itself.

We have tried to minimize inconsistencies between the terminology used in this volume and that used in other principal sources of information for railway ESM. However, it is not possible to eliminate inconsistency entirely, because there is variation in usage between these other sources.

24.1 Abbreviations

COTS	Commercial Off The Shelf
DRACAS	Data Reporting Analysis and Corrective Action System
ESM	Engineering Safety Management
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
GSN	Goal Structuring Notation
HAZOPS	Hazard and Operability Study
ISA	Independent Safety Assessor
OSHA	Operating & Support Hazard Analysis
PHA	Preliminary Hazard Analysis
SHA	System Hazard Analysis
SIL	Safety Integrity Level
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
UML	Unified Modeling Language
VPF	Value of Preventing a Fatality

© Abbott Risk Consulting Ltd. 2022

24.2 Specialized terms

Specialized terms are written in upper-case in this appendix and in the body of the document, unless the definition simply makes the ordinary English meaning a little more precise, in which case they are written in lower case.

accident	Unintended event or series of events that results in harm to people.
accident likelihood	Likelihood of an accident occurring. May be expressed as numeric probability or frequency or as a category.
accident sequence	Potential progression of events that results in an accident.
accident severity	Measure of amount of harm. May be expressed as a financial value or as a category.
accident trigger	Condition or event which is required for a hazard to give rise to an accident.
application condition	Condition which needs to be met in order for a system to be safely integrated and safely operated.
approval	Process by which someone reviews the evidence that risk has been controlled and takes an explicit decision as to whether a system may be placed into operation, including trial operation and operation for testing, or whether a product may be applied. Note. Some people distinguish different sorts of approval and give some sorts different names, such as 'acceptance' or 'endorsement'.
barrier	(In the context of risk estimation) anything which may act to prevent a hazard giving rise to an accident. Barriers may be physical, procedural or circumstantial,
baseline	Consistent and complete set of configuration item versions used as a departure point for the control of change.
basic integrity	Integrity attribute for safety related function with a TFFR better (less demanding) than 10^{-5} per hour or non-safety-related function.
broadly acceptable	Description for risk which is low and routinely accepted in ordinary life.
broadly accepted	Synonym of 'broadly acceptable'.
causal analysis	Analysis of events that are likely to happen before a hazard has occurred
causal factor	Event, state or other factor which might contribute to the occurrence of a hazard.
Commercial Off The Shelf (COTS)	Product manufactured for a wide market and whose fitness for purpose has been deemed acceptable by general usage.
configuration audit	Examination to determine whether a configuration item conforms to its configuration documents.
configuration control	Activities comprising the control of changes to a configuration item after formal establishment of its configuration documents.
configuration identification	Activities comprising determination of the product structure, selection of configuration items, documenting the configuration item's physical and functional characteristics including interfaces and subsequent changes, and allocating identification characters or numbers to the configuration items and their documents.
configuration status accounting	Formalized recording and reporting of the established configuration documents, the status of proposed changes and the status of the implementation of approved changes.
configuration item	Aggregation of hardware, software, documentation, processed materials, services, or any of its discrete portions, that is designated for configuration management and treated as a single entity in the configuration management process.

© Abbott Risk Consulting Ltd. 2022

configuration management	Process of identifying and documenting the functional and physical characteristics of a configuration item, to control changes to those characteristics, to record and report change processing and implementation status and to verify compliance with specified requirements.
consequence analysis	Analysis of events that are likely to happen after a hazard has occurred
control measure	Measure taken to reduce risk.
Cross Acceptance	Process by which a product that has been accepted by one authority to the relevant standards and is acceptable to other authorities without the necessity for further assessment
Design Analysis	Analysis of constraints, internal or external interactions, and the logic flow within a design to identify and remove hazardous design flaws.
Data Reporting Analysis and Corrective Action System (DRACAS)	Administrative system used to collect and analyze data concerning the performance of a system or product and to support the management of corrective actions, where necessary.
Engineering Safety Management (ESM)	Activities involved in making a system or product safe and showing that it is safe. Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering.
error	Mistake made by a person that produces an unintended result.
Event Tree Analysis	Method of illustrating the intermediate and final outcomes which may arise after the occurrence of a selected initial event.
failure	Deviation from the specified performance of a system, product or other change. A failure is the consequence of a fault or error.
Failure Mode and Effects Analysis (FMEA)	Process for reliability, availability and safety analysis, where all known failure modes of components or features of a system or product are considered in turn and the outcomes are identified.
Failure Mode, Effects and Criticality Analysis (FMECA)	Extension to FMEA in which the criticality of the effects is also assessed.
fault	Fault is a defect in a system, product or other change which may cause a failure.
Field Programmable Gate Array (FPGA)	Electronic device in which the connections between components may be changed after installation.
Fault Tree Analysis (FTA)	Method for representing the logical combinations of various states which lead to a particular outcome (top event).
generic application	Product or system considered in the context of a class of similar applications.
generic product	Product considered without any particular application in mind.
Goal Structuring Notation (GSN)	Notation for representing a logical argument as a diagram,
hazard	Condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product definition.
Hazard and Operability Study (HAZOPS)	Structured study carried out by application of guide words to identify all deviations from the design intent with undesired effects for safety or operability.
human factors	Field of study and practice concerned with the human element of any system, the manner in which human performance is affected, and the way that humans affect the performance of systems.
Hazard Log	Register that records details of hazards identified, including or referencing their status, relevant decisions made, solutions adopted and mitigation status..

© Abbott Risk Consulting Ltd. 2022

Incident	Unintended event or series of events that results in harm to people or could, in other circumstances have resulted in harm to people. Note. All accidents are incidents. Some incidents are not accidents.
independent assessment	Process of peer review to form an independent judgment whether a system, product or other change to the railway has met its specified safety requirements and that the safety requirements are adequate for its intended application.
independent assessor	Person or organization who carries out an independent assessment.
Independent Safety Assessor (ISA)	Organization, independent of the project organization, acting as independent assessor.
Risk	Combination of the likelihood of harm to people and the severity of that harm associated with some cause or type of accident.
likelihood-severity matrix	Matrix defining broad categories of likelihood and severity for the purposes of risk estimation.
maintenance	Activities that need to be carried out to keep a system or product fit for service and in conformance with its specification.
minimal cut set	Set of basic events in the fault tree which are sufficient to cause the top event to occur, such that removing any event from the set would mean that the top event would not occur.
occupational health and safety	Health and safety of people at work, including those making a change to the railway.
Preliminary Hazard Analysis	Exercise to identify hazards and estimate risks early in the life of a project.
railway safety	Freedom from unacceptable risk of harm to people during railway operations.
random failure	Failure resulting from random causes such as variations in materials, manufacturing processes or environmental stresses.
reliability	Probability that an item can perform a required function under given conditions for a given time interval.
risk	Combination of the likelihood of occurrence of harm and the severity of that harm.
risk estimation	Process of producing a measure of the level of risk associated with a hazard or demonstrating that it is below an acceptable threshold.
Safety	Freedom from unacceptable risk of harm to people.
safety analysis	General term encompassing identifying hazards, analyzing hazards and assessing risk.
safety audit	Activity to check and ensure that a project is being run according to its Safety Plan. It should also address the adequacy of the safety plan.
Safety Case	Formal presentation of evidence, arguments and assumptions aimed at providing assurance within a defined scope, that a system or product has met its safety requirements and that the risk associated with it has been reduced to an acceptable level.
safety integrity	Ability of a safety-related function being performed satisfactorily under stated conditions within a stated operational environment and a stated period of time.
Safety Integrity Level (SIL)	One of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems.
safety lifecycle	Series of ESM activities carried out in conjunction with the System Lifecycle for safety-related systems.
Safety Plan	Document detailing the ESM activities to be carried out on a project, and responsibilities of people to perform these tasks.

© Abbott Risk Consulting Ltd. 2022

Safety Requirements Specification	Specification of the requirements that a product, system or change to the railway must satisfy in order to be judged safe.
safety-related	Item is safety-related if any of its features or capabilities has the potential to contribute to or prevent an accident.
specific application	The application of a product or system at a specified site in a specified operational environment.
Sneak Circuit Analysis	Analysis of a design, which is used to look for interactions between parts of the system or between the system and other things which might lead to unexpected and hazardous behavior.
standard	Authorized document, including specification, procedure, instruction, directive, rule or regulation, which sets requirements.
System	Collection of elements which interact according to a design, where an element of a system can be another system, called a “subsystem” and may include hardware, software, procedures and human interaction. An entire railway is a system, and so is a tunnel, a station, a train and a signaling system..
system lifecycle	A sequence of phases through which a system can be considered to pass. A product may also pass through some of these phases.
systematic failure	Failure due to errors, which causes the product, system or process to fail deterministically under a particular combination of inputs or under particular environmental or application conditions.
triggering event	Event, outside the system or product of interest, which is required in order for a Hazard to result in an Accident.
Unified Modeling Language (UML)	Notation for expressing the structure, behavior and operational environment of a system.
validation	Activity of confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
Value of Preventing a Fatality (VPF)	Indication of the level of expenditure which is considered to be justified in order to reduce the statistical expectation of harm by one fatality.
verification	Activity of confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

© Abbott Risk Consulting Ltd. 2022

25 REFERENCED DOCUMENTS

This section provides full references to the documents referred to in the body of this volume.

[00-56] UK Ministry of Defence, DEF-STAN 00-56, *Safety Management Requirements for Defence Systems*, Issue 4, June 2007

[0492] NUREG 0492, The Fault Tree Handbook, 1981

[10007] ISO 10007:2003, *Quality management systems. Guidelines for configuration management*

[50126-1] EN 50126-1 2017, *Railway applications – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) Part 1 Generic RAMS Process*
Also published as IEC62278-1

[50126-2] EN 50126-2 2017, *Railway applications – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) Part 2 Systems Approach to Safety*
Also published as IEC62278-2

[50128] EN 50128:2011, *Railway applications. Communication, signalling and processing systems*
Software for railway control and protection systems. Also published as IEC 62279.

[50129] prEN 50129:2016, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling.*
Also published as IEC 62425

[50159] EN 50159:2010, *Railway Applications – Communications, signalling and processing systems – safety-related communication transmission systems*

[50506] PD CLC/TR 50506-1: 2007, *Railway applications. Communication, signalling and processing systems. Application guide for EN 50129. Cross-acceptance*

[50567] EN 50657:2017, Railways Applications - Rolling stock applications - Software on Board Rolling Stock

[5760] BS 5760: Part 5 1991, *Reliability of systems, equipment and components: Part 5 Guide to failure modes, effects and criticality analysis*

[61508] IEC 61508:2003, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[730] *IEEE Std 730-2002 - IEEE Standard for Software Quality Assurance Plans,* 2002

[760] Civil Aviation Authority Safety regulation Group, CAP 760, *Guidance on the Conduct of Hazard Identification, Risk estimation and the Production of Safety Cases for Aerodrome Operators and Air Traffic Service Providers,* 13 January 2006

[8004] German Federal Railways Standard Mü 8004

[CIA] Chemical Industries Association, *A Guide to Hazard and Operability Studies*, Kings Buildings, Smith Square, London SW1P 3JJ, 1992

[CSM-M] Commission Regulation (EC) No 1078/2012 on the Common Safety Method (CSM) for Monitoring

[CSM-RA] Commission Regulation (EC) No 402/2013 on the adoption of a Common Safety Method on Risk Evaluation and Assessment

[DoT] U.S. Department of Transportation, Federal Aviation Administration (ed.): *System Safety Handbook*, December 30, 2000: Chapter 9, Table 9-1

[Ericson] Ericson, C. F.: *Hazard Analysis Techniques for System Safety*, Wiley, 2005.

[Hessami] Hessami A., *Risk – A Missed Opportunity?,* Risk and Continuity, volume 2, issue 2, pp. 17-26, June 1999

[Hollywell] Hollywell, P.D., *Incorporating Human Dependent Failures in Risk estimations to Improve Estimates of Actual Risk*. Safety Science, Vol. 22, No. 1-3, pp.177-194, 1996

[HSE] Health and Safety Executive, *Managing competence for safety-related systems,* 2007, *available from* www.hse.gov.uk

[Kelly] *The Goal Structuring Notation – A Safety Argument Notation*, Tim Kelly and Rob Weaver, University of York, UK

© Abbott Risk Consulting Ltd. 2022

[Kirwan] Kirwan, B., *A Guide to Practical Human Reliability Assessment*, Taylor and Francis, London, 1994, ISBN 0748401113

[Kletz] Kletz Trevor A., *Hazop and Hazan*, (The Institution of Chemical Engineers, 2006), ISBN 0852955065

[Leveson1] Leveson N., *Safeware: System Safety and Computers*, Addison-Wesley 1995, ISBN 0-201-11972-2

[Leveson2] Leveson N., *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, 2012, ISBN 978-0262016629

[Preece] Preece J., Rogers Y., Sharp H., Benyon D., Holland S. and Carey T., Human-Computer Interaction, Addison Wesley, 1994, ISBN
0-521-36570-8

[Reason] Reason J., *Managing the Risks of Organizational Accidents,* Ashgate Publishing Limited, 1997, ISBN 978-1840141054

[RSSB1] Rail Safety and Standards Board, *"Taking Safe Decisions",* 2014, available from www.rssb.co.uk

[RSSB2] Investigation Guidance, RSSB, 2014

[YB4] *Engineering Safety Management, issue 4, "Yellow Book 4",* ISBN 978-0-9551435-2-6 Yellow Book 4 now has the status of a withdrawn document.

Note: This revision (Issue 1.4) of Volume 2 has not modified any of the technical content present in the previous revision. Some of the standards referenced may have been revised. A full technical review is planned to be undertaken of this document prior to its next revision.

© Abbott Risk Consulting Ltd. 2022

iESM

BROUGHT TO YOU BY ARC

international Engineering Safety Management

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.4 May 2022

arc