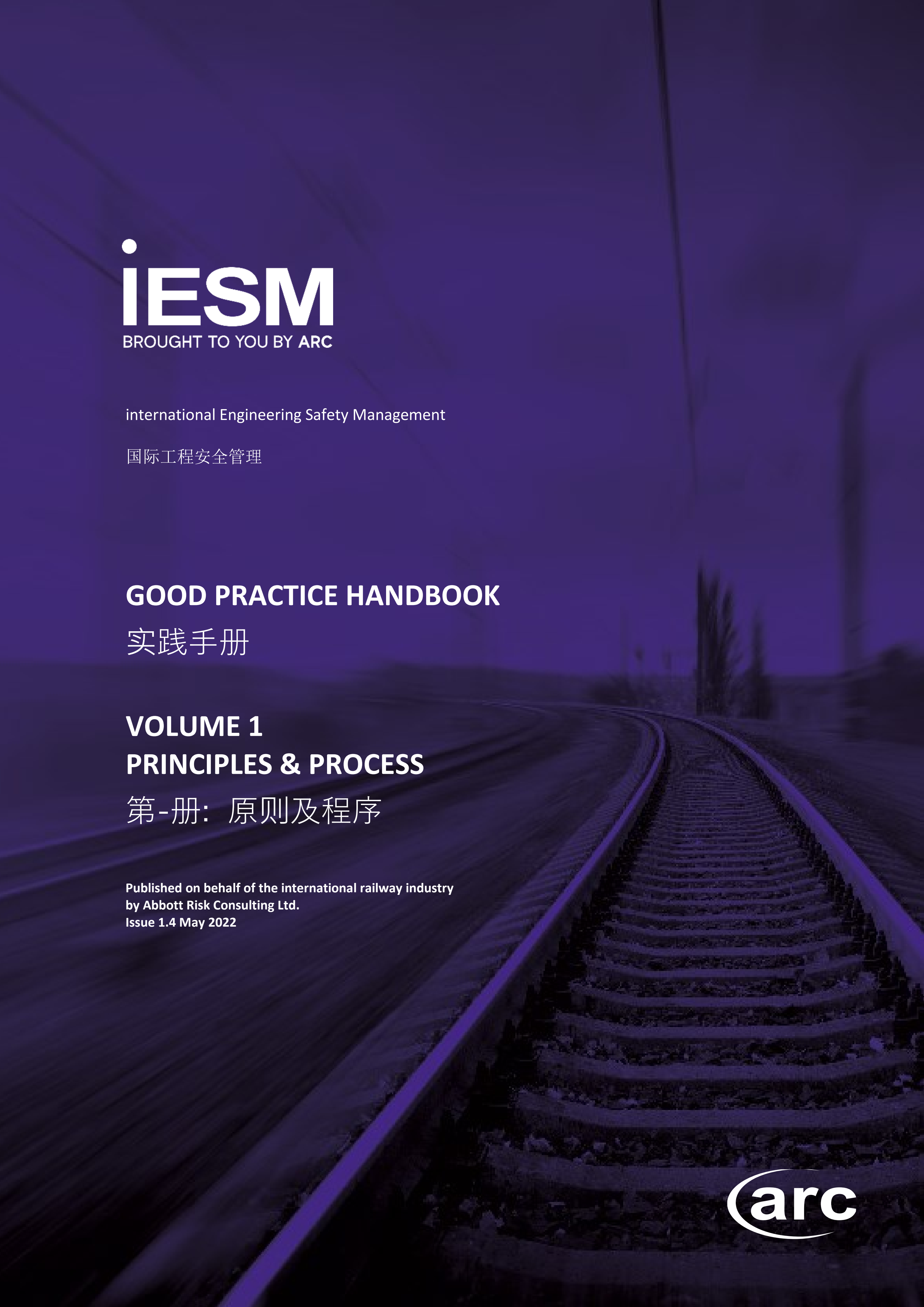


iESM

BROUGHT TO YOU BY ARC

international Engineering Safety Management

国际工程安全管理

GOOD PRACTICE HANDBOOK

实践手册

VOLUME 1
PRINCIPLES & PROCESS

第-册：原则及程序

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

arc

CONTENTS

Issue 1.4

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 has been written with help from the people listed below.

- D Beacham
- Dr G Bearfield
- S Bickley
- N Bowley
- M Castles
- P Cheeseman
- Dr Chen Roger Lei
- Dr R Davis
- B Elliott
- Dr KM Leung
- Dr I Lucic
- J McDonald
- Niu Yingming
- Ng Nelson Wai Hung
- G Parris
- J Shaw
- Shi Lisa
- G Topham
- Tse Shirley Lai
- Dr Fei Yan
- Dr Zhang Simon

These people worked for the organizations listed below.

- ARC - Abbott Risk Consulting Ltd.
- 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
- Crossrail
- Electrical and Mechanical Services Department Hong Kong Government
- Lloyd’s Register
- London Underground
- MTR Corporation, Hong Kong
- RSSB, UK
- Rio Tinto
- Sydney Trains
- Technical Programme Delivery Group
- EC Harris

We are grateful to the organizations listed who have supported iESM in various ways.

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

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 (1) and to guidance on European Common Safety Methods (2) among many others and we acknowledge our debt to them.

FOREWORD

It is good practice for railway organizations to establish systematic processes for managing safety and most railway organizations across the world are obliged by law to do so. The requirements for these processes are laid out in the law and in standards but there is a need for practical guidance, written by practitioners, for practitioners, on how to put these requirements into practice, both efficiently and effectively.

Within the UK this need was met by the Engineering Safety Management handbook, often called “Yellow Book” (1), but, while the Yellow Book has been used in many places, it has always contained some guidance that is specific to the UK and European legal systems and remained silent on other approaches to managing safety. Moreover, in 2012, the publishers of the Yellow Book took a decision that it would no longer be maintained and that it should have the status of a withdrawn document.

This handbook has been written to provide up-to-date guidance that reflects emerging good practice yet is helpful to more people. The aim is that it is not specific to one country or railway and can be of use to readers across the world.

序言

对于铁路机构，建立系统化的安全管理过程是良好的做法, 而在世界各地大多数的铁路机构都须依从当地的法律建立系统化的安全管理。而这些过程的要求分别设立在法律和不同的标准内，故需要由从业者为铁路业界撰写实际的指导把这些要求有效地转化为实践。

在英国，「工程安全管理手册」, 或常被称为「黄皮书」（1）满足了这方面的需求。虽然黄皮书经已在许多地方使用，但它只包含特定于英国和欧洲法律制度的指导而没有包含其他管理安全的方法。此外，在 2012 年，黄皮书的出版商决定不再维持黄皮书，因此黄皮书现是一份已撤销文件。

本手册提供了最新的指导以反映最新的良好实践方法以协助更多的使用者。编写本手册的目的是让世界各地的读者都可以使用，而不只限于特定国家或铁路。

1 INTRODUCTION

1.1 Why read this handbook?

This handbook provides guidance on how to make sure that systems and products for railways, tramways and subway systems[1] are safe. This is an objective of great importance in its own right and the guidance in this handbook is designed to help you to deliver safe systems and products effectively and efficiently.

The guidance in this handbook is designed to be consistent with a large number of legal frameworks and has been derived from international good practice under the supervision of an international working group of experienced practitioners.

This handbook is intended to help you set up a process that controls risk and shows that this has been done. This process may also help you achieve other objectives, such as delivering reliability and performance, delivering on time and complying with the law and relevant standards.

This handbook is written for people who use their judgment to take or review decisions that affect railway safety. If you only take or review decisions within a framework of established procedures, you may not find it necessary to read this handbook. However, we would not discourage anyone from reading on: you may find this handbook useful if your work has any connection with railway safety.

1.2 Background and concepts

By efficiently moving people and goods from place to place, railways deliver great benefits to societies. However, they also create **hazards**[2] - situations that may lead to accidents. Some of these hazards can be eliminated but others are unavoidable consequences of the process of transportation. Railways have always suffered accidents and always will but, over time, human ingenuity has made these accidents less frequent and reduced the harm that people suffer when accidents do occur. By remaining diligent and ingenious, people can safeguard these achievements and build upon them.

A railway is a **system**, that is, a collection of assets, people and procedures that are intended to work together to accomplish some function. There are smaller systems within railways. These include signaling systems, track systems, stations, depots and trains.

The final output of a project that builds or changes a railway will be the system that contains all the new or changed parts. However some projects develop generic **products** that will be applied by later projects to create new systems.

[1] From now on, we will just write “railway”. What we say is equally applicable to tramways and metro systems.

[2] Words like “hazards”, which are shown in bold type, are specialist terms. We provide informal introductions to these terms in this volume. More precise definitions can be found in the other parts of this handbook.

Hazards are associated with systems and products.

We use the word '**risk**' to refer to the likelihood that an accident will happen and the amount of harm to people that could arise. We say that a system or product is **safe** when the risk associated with it has been controlled to an acceptable level. In most railways, delivering safety is at least as important as delivering performance, reliability or good customer service.

To deliver safety, we need to ensure that:

1. Safety is designed and built into the railway's systems and products;
2. Safety is preserved when these systems and products are maintained and changed; and
3. These systems and products are operated safely.

We refer to the business of ensuring that railway systems and products are safe, that is, of ensuring the first two items from the list above, and of demonstrating that this is the case, as **engineering safety management** or **ESM** for short. ESM is, or at least should be, an integral part of delivering and maintaining railway systems and products.

In this handbook, 'risk' is always associated with harm to people. Organizations also have to control other sorts of risk, including risk associated with economic and environmental losses. ESM may be seen as one part of more general risk management and may be integrated with processes to control other types of risk. This handbook does not provide guidance on managing other sorts of risk. For further guidance on more general risk management, please refer to ISO 31000 (3), which is an international standard on risk management.

1.3 Scope

This issue of the handbook is concerned with designing and building safety into the railway's systems and products. It is also important to ensure that both safety risks and related security risks are appropriately mitigated to minimize the danger of harm, disruption, and economic loss, although ESM is concerned mainly with the first of these. This guidance has been written to help those who are involved in railway projects to perform effective ESM. All but the simplest railway systems and products require input from multiple disciplines. This handbook is written for practitioners of all disciplines.

1.4 Structure

The iESM Guidance is structured in three layers:

1. Principles and process
2. Methods, tools and techniques
3. Specialized Guidance

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

The second layer comprises substantial detailed guidance structured around the principles and processes described here, known as Volume 2.

The third layer comprises a series of Application Notes where specific issues are tackled and in-depth guidance provided.

There are many effective ways of putting this generic process into practice. The other layers give guidance on ways that have proved effective.

We suggest that you read this volume first and refer to other parts of the guidance, if and when you find you need more help.

Further information is published on the web site www.intesm.org.

1.5 Compliance with this volume

We offer this handbook purely as guidance. There is, however, consensus among railway engineers from several countries that the guidance in this handbook represents good practice.

This volume contains a number of principles, which are printed in section 3. We have written these principles so that you can, if you wish, require your staff or your suppliers to comply with them. We have phrased these principles using the word 'must' to indicate this possible use.

2 OBLIGATIONS

2.1 General remarks

If you are working on railway systems or products that affect safety then your organization will have obligations that constrain the ESM activities that you need to carry out. These obligations may come from some or all of the following:

- The laws and regulations of the country or countries in which you are working and in which the railway is situated;
- The policies and procedures of your organization;
- The standards applicable to the railway on which you work; and
- The requirements of any contracts that your organization has entered into.

You may also have personal obligations defined in law and in the codes of conduct of any professional societies and institutions to which you belong.

These obligations may include some or all of the following:

- Requirements on the ESM activities that you need to carry out, such as requirements to do risk analysis in a certain manner;
- Criteria that define when risk may or may not be accepted – **risk acceptance criteria**;
- Requirements that certain aspects of your work are reviewed by someone else;
- Requirements to obtain certain approvals from certain organizations before putting new or changed systems into service; and
- Requirements to behave professionally.

The guidance in this handbook is aligned with good practice and the requirements of legal frameworks and standards with which we are familiar. We hope and expect that you will find that it describes practical, proven methods that will help you discharge your obligations. However, we cannot guarantee that the guidance will be consistent with all of the obligations that you have and it is unlikely that following it will be enough to discharge all your obligations completely. Therefore you will need to make sure that you understand all your obligations before you apply the guidance in this handbook.

2.2 Risk acceptance criteria

The risk acceptance criteria mentioned in the previous section play a pivotal role in ESM. We discuss these criteria further in this section.

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 environment and, generally, 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 1 illustrates these activities, showing that, typically, a series of decisions will have to be taken at different times.

We provide guidance on the activities before and after the decision that will be applicable to most situations because these are matters of good engineering and management practice. However the risk acceptance criteria are matters of societal values and will vary from country to country and from railway to railway. You will need to make sure that you understand what risk acceptance criteria you should use and make sure you meet them when applying the guidance in the handbook.

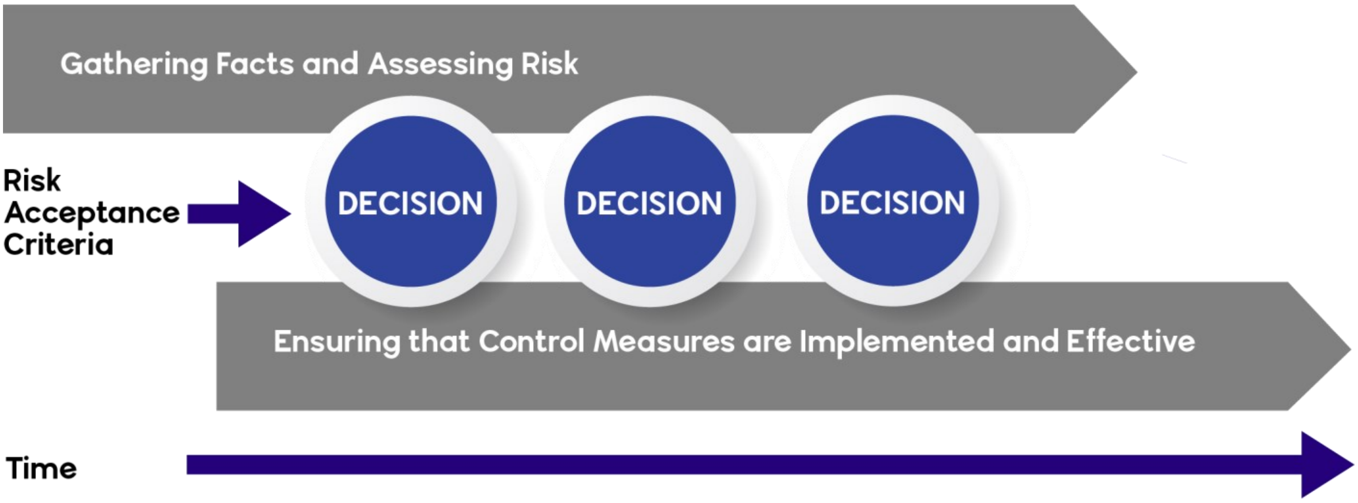

Gathering Facts and Assessing Risk
Risk Acceptance Criteria
DECISION
DECISION
DECISION
Ensuring that Control Measures are Implemented and Effective
Time

Figure 1: Risk Acceptance Criteria Play a Central Role in ESM

You may find that you are obliged to apply risk acceptance criteria of some or all of the following types:

- Absolute levels, such as, “the rate of occurrence of hazardous failure shall be no greater than once per billion hours on average”;
- A requirement to apply certain technical standards, sometimes with the understanding that no further risk reduction is required if the standards are fully applied; or
- A requirement to balance the costs of risk reduction against the amount by which the risk is reduced. In some countries there is a requirement to take all “reasonably practicable” steps to reduce risk, by which is meant all steps for which the costs are not disproportionate to the reduction in risk that is achieved.

If you are obliged to apply some risk acceptance criteria then you will have to put sufficient measures in place to meet them. There may be good reasons to do more than the risk acceptance criteria require. For example, you may choose to adopt some straightforward and inexpensive control measures because it would cost more to find out whether they were required in order to meet the risk acceptance criteria than it would cost to implement them. You may also decide to take measures that are designed to deliver non-safety benefits, such as improved performance, and that improve safety as a side effect.

3 A GENERIC ENGINEERING SAFETY MANAGEMENT PROCESS

3.1 Overview

In this section we present a generic ESM process that contains the most important ESM activities and the most important flows of information between them. ESM should be an integral part of all engineering activities. The generic ESM process contains activities, such as configuration management, which are essential to deliver safety but are also required for other reasons. You may find activities in the generic process that your organization chooses to regard as parts of other processes. You may also find that your organization draws the boundaries between activities in different places or gives them different names. The manner in which you structure and name these activities makes no difference to their effectiveness. All that matters is that they should be done and done well.

The generic process is shown in Figure 2.

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 that are not shown. An arrow from activity A to activity B does not imply that A needs to 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.

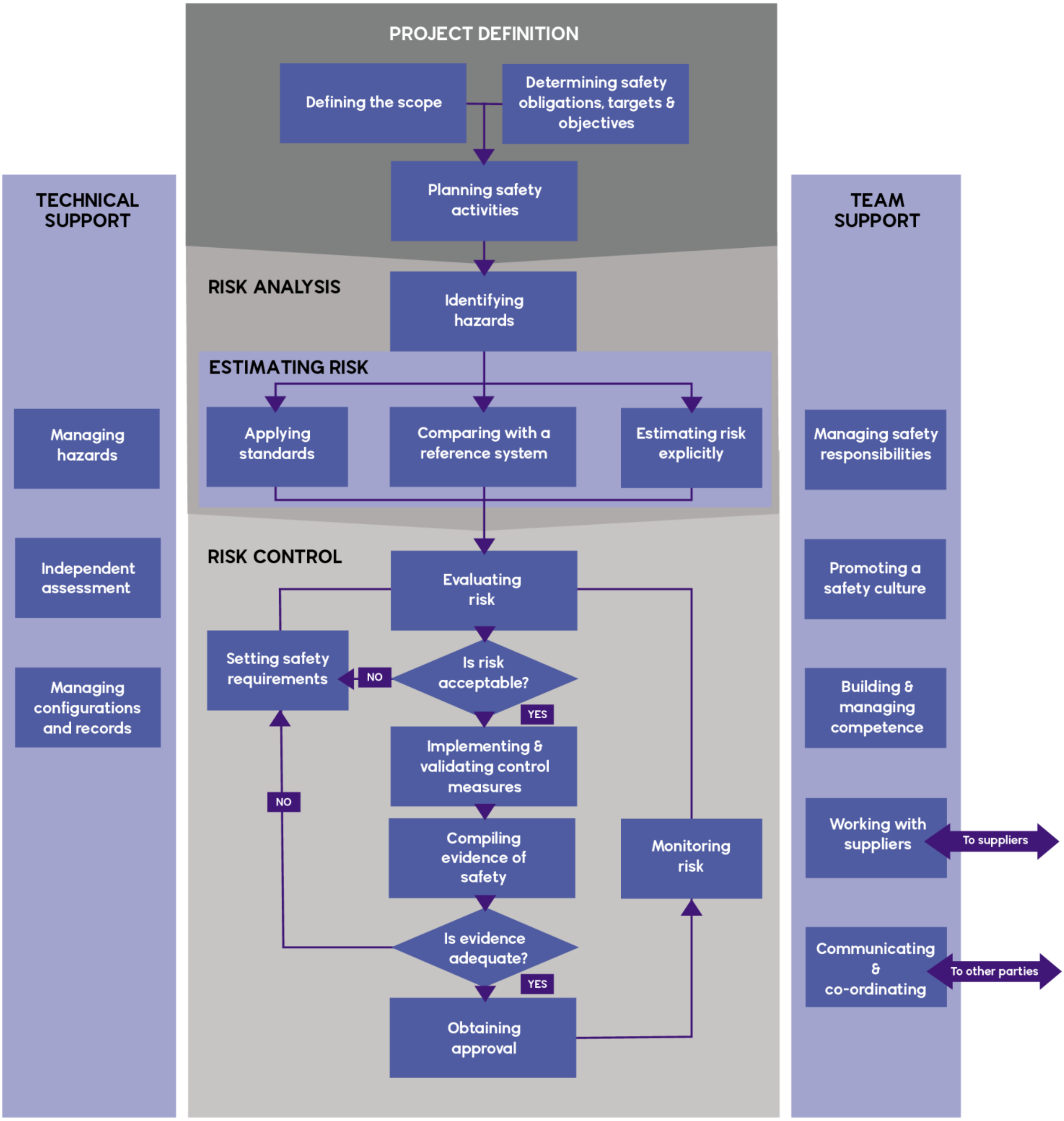

PROJECT DEFINITION
Defining the scope
Determining safety obligations, targets & objectives
Planning safety activities
RISK ANALYSIS
Identifying hazards
ESTIMATING RISK
Applying standards
Comparing with a reference system
Estimating risk explicitly
RISK CONTROL
Evaluating risk
Setting safety requirements
NO
Is risk acceptable?
YES
Implementing & validating control measures
NO
Compiling evidence of safety
Monitoring risk
Is evidence adequate?
YES
Obtaining approval
TECHNICAL SUPPORT
Managing hazards
Independent assessment
Managing configurations and records
TEAM SUPPORT
Managing safety responsibilities
Promoting a safety culture
Building & managing competence
Working with suppliers
To suppliers
Communicating & co-ordinating
To other parties

Figure 2: A Generic Process for ESM

3.2 Cross acceptance

When a product is put to use in a particular environment, we refer to that as an ‘application’ of the product.

Sometimes, the evidence for the safety or one application of a product may rely upon the approval of a similar product in a similar environment. This reliance is referred to as ‘cross acceptance’.

Preparing a cross acceptance argument introduces some new activities and provides an alternative approach to performing some of them, as indicated in Figure 3 below. Cross acceptance is unlikely to completely replace any of the activities with which it overlaps in the figure because the differences between the two products and their applications will normally require analysis and action.

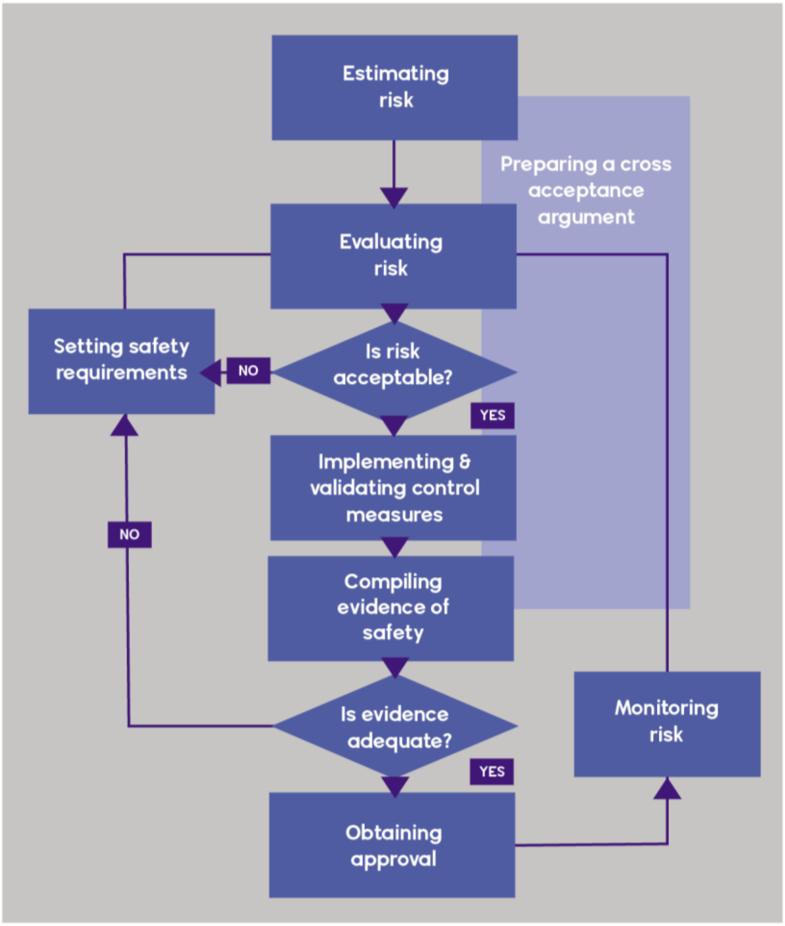

Estimating risk
Preparing a cross acceptance argument
Evaluating risk
Setting safety requirements
NO
Is risk acceptable?
YES
Implementing & validating control measures
NO
Compiling evidence of safety
Is evidence adequate?
YES
Monitoring risk
Obtaining approval

Figure 3: Cross Acceptance

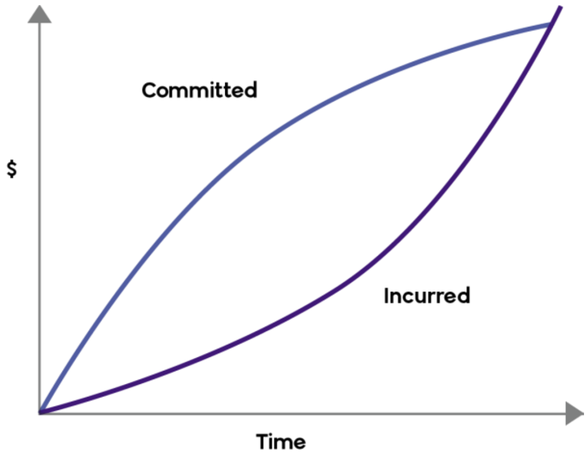
3.3 Guidance

Each of the following five sections contains guidance on one group of activities. After an introduction, the guidance for each activity is presented in two columns with the guiding principle on the left and more detailed guidance on the right.

The guidance draws upon good practice as described in various sources, including IEC 61508 (4), EN 50126 (5), the European Common Safety Method on Risk Evaluation and Estimation (2) and the Yellow Book (1).

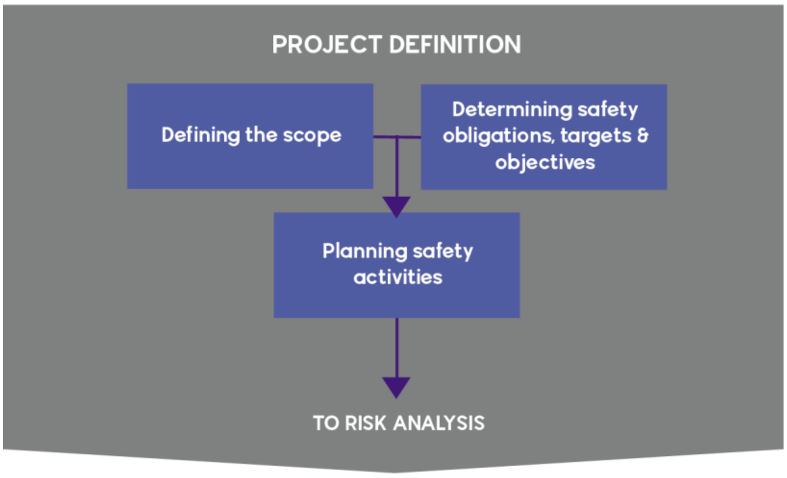
When carrying out all ESM activities, you should consider all the people whom your work will affect, including customers, the general public, installers, operators and maintainers. You should do what you can to help them avoid errors and prevent accidents.

You should start the ESM process as soon as you can. As the graph on the right shows, the decisions made early in the project will result in committing a large proportion of the expenditure on the project when only a small proportion of the expenditure has actually been incurred. By starting ESM early, it is possible to ensure that safety is designed into the system or product and to avoid expensive rework later on.



3.4 Definition

The definition activities are concerned with establishing clear objectives and a clear scope for the project and planning out a program of activities to deliver these.


PROJECT DEFINITION

Defining the scope

Determining safety obligations, targets & objectives

Planning safety activities

TO RISK ANALYSIS

Figure 4: Project Definition Activities

3.4.1 Defining the scope

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 environment in which it will operate.

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

3.4.2 Determining safety obligations, targets and objectives

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.

Section 2 above lists sources of safety obligations that you should consult as well as some of the types of obligations that you may have. 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.

3.4.3 Planning safety activities

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 confirm that they remain 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.

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.

3.5 Risk analysis

The risk analysis activities are concerned with establishing and analyzing the facts to provide a sound basis for decisions about risk control. The **Estimating risk** activity has three sub-ordinate activities.

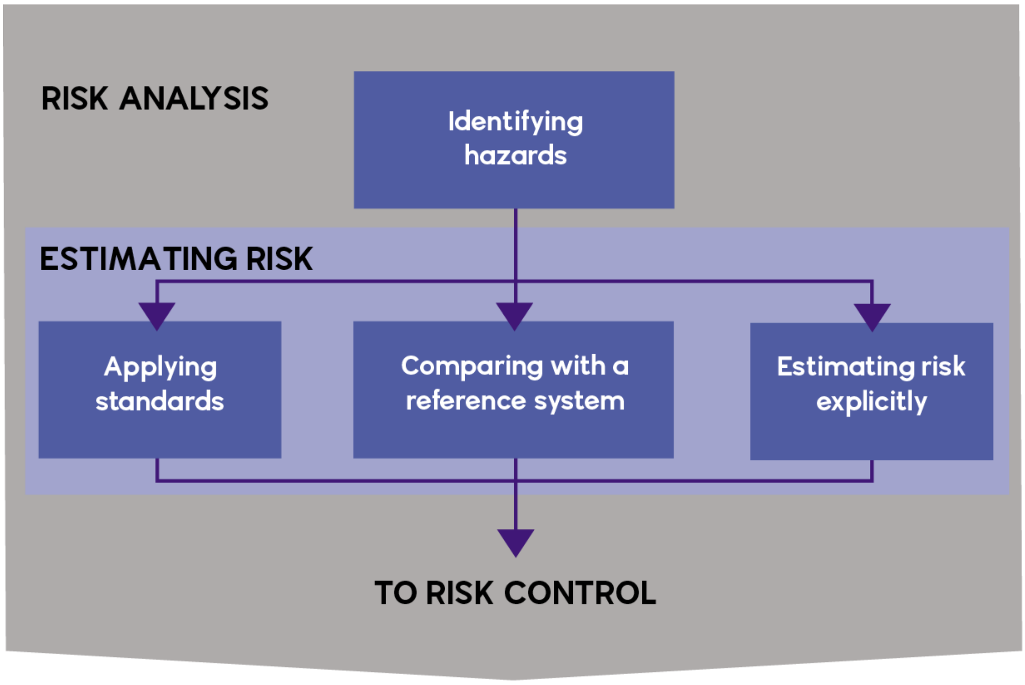


Figure 5: Risk Analysis Activities

3.5.1 Identifying hazards

Hazards are initially identified from the definition of scope. The hazard log is reviewed throughout the life of the system and product. 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.

You should look for hazards associated with 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.

3.5.2 Estimating risk

The risk associated with each hazard is estimated and aggregated to estimate the risk associated with the system or product. This estimate 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 confirm 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 estimating risk, or at least of showing that it is below an acceptable threshold, that may support sound decisions with considerably less effort.

Firstly, if a hazard is fully addressed by accepted standards[3] 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 achieved by meeting electrical standards.

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 a particular hazard of your system is no more than that associated with the reference system, then you may be able to conclude that this risk from this particular hazard is acceptable.

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 undue 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 the risk associated with the railway as a whole, for example installing automatic train protection. You should still assess them in case they introduce other risks that need to be controlled or fail to achieve the intended level of risk reduction.

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

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.

3.6 Risk control

The risk control activities are concerned with taking the results of risk analysis, deciding what control measures to take and then ensuring that these are fully and effectively implemented.

Where a product being developed is an adaptation of one that has previously been shown to be safe then some of the activities may be omitted, at least in part, because they have been done before. The process of re-using work that has been done before in this fashion is often referred to as **cross-acceptance** and the potential for such re-use is indicated on the diagram by an activity, **Preparing a cross acceptance argument**.

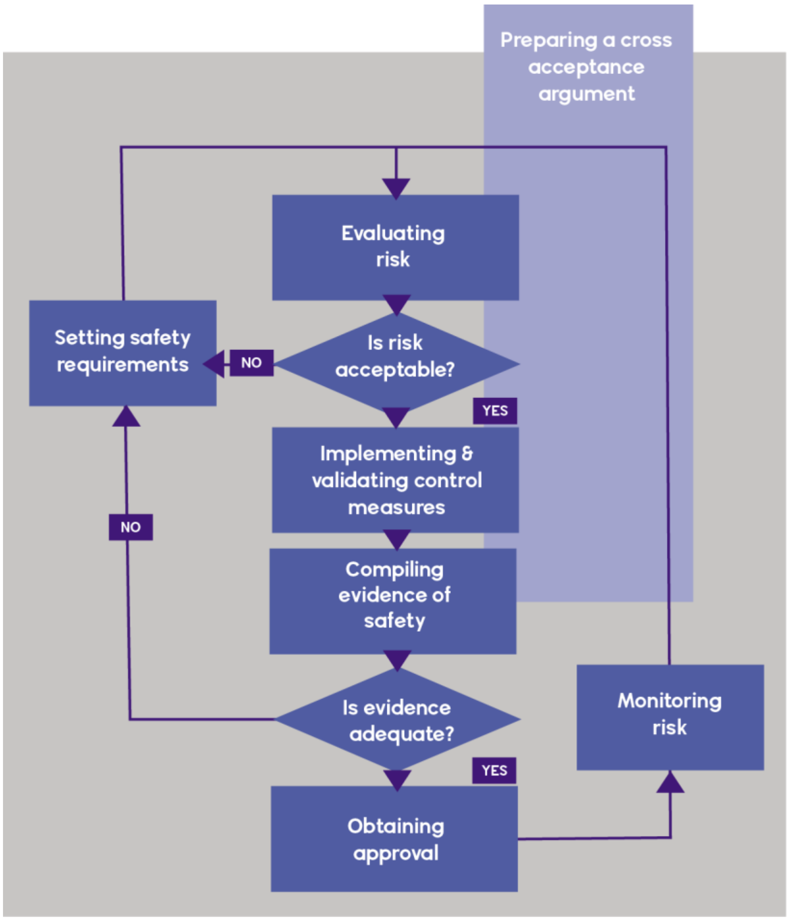

Preparing a cross acceptance argument
Evaluating risk
Setting safety requirements
NO
Is risk acceptable?
YES
Implementing & validating control measures
NO
Compiling evidence of safety
Is evidence adequate?
YES
Monitoring risk
Obtaining approval

Figure 6: Risk Control Activities

3.6.1 Setting safety requirements

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 needs to be maintained.

A safety requirements specification may also include details about the environment in which the system or product will operate.

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 validate that they have been met.

Some of the ways people behave and some of the reasons for their errors are understood. Writers such as James Reason (6), 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.

3.6.2 Evaluating risk

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 'Yes' arrow on the diagram): or
2. The risk cannot be accepted as it is but could be accepted if the safety requirements were strengthened (the 'No' arrow on the diagram); or
3. The risk cannot be accepted and cannot be reduced to an acceptable level and, therefore, the system or product needs to 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 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.

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.

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.

3.6.3 Implementing and validating control measures

This activity involves implementing the control measures defined in the previous activity and validating 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.

3.6.4 Preparing a cross-acceptance argument

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 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 evidence for the safety of the target application without referring to the detailed evidence behind the original approval. It is also possible, and often sensible, when performing ESM on one project to re-use and adapt the detailed evidence accumulated on another project. However, that sort of re-use is not cross-acceptance and 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 environment and approved for use in that 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 environments.

If the native and target applications 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 application as part of the evidence for the target application. However you should identify all material differences between the native and target applications, because each of these differences may mean that the risk associated with the two applications is different. Having done this you should establish that none of these differences results in unacceptable risk, using the activities described above.

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 assumptions should be identified and confirmed.

There is a guide on cross-acceptance that is numbered PD CLC/TR 50506-1: 2007 (7) and that provides further useful advice.

3.6.5 Compiling evidence of safety

This activity involves compiling evidence of the satisfactory performance of ESM 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 control 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 estimate 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 robust. You should record and confirm 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.

3.6.6 Obtaining approval

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 use these processes to approve the placing of some systems into service without seeking external approval.

If you are building or changing a railway, you may need approvals before you starting construction or bring the new railway into service, or both. Some projects carry out their work in stages, in which case each stage may need approval.

3.6.7 Monitoring risk

As soon as a system first enters service (or enters trial operation in an environment that closely resembles 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
- aspects of the circumstances within which the railway operates that affect risk – traffic levels, for instance.

You should consider collecting and analyzing data about:

- incidents, 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.

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, accidents and near misses, 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 you to perform some of the activities described above.

3.7 Technical support

This section contains three activities that provide technical support to the activities listed above.

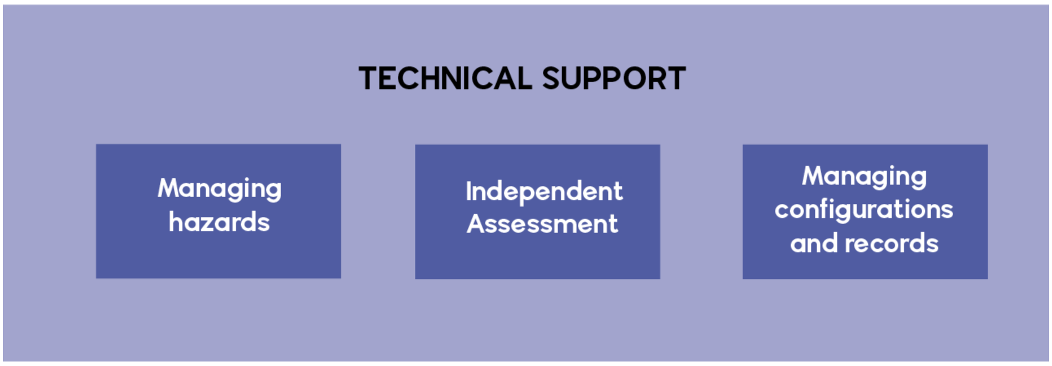


Figure 7: Technical Support Activities

3.7.1 Managing hazards

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 keep a record of all hazards identified, the analysis of these hazards, the implementation of measures to put in place to control these 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 which is a register of hazards 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.

3.7.2 Independent assessment

An independent assessment provides a second opinion on the status 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.

3.7.3 Managing configurations and records

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.

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 or building a railway, you will have to keep records until what you have delivered has been taken out of service. 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 near misses, incidents 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.

3.8 Team support activities

This section contains a number of activities that support the activities above indirectly by ensuring that the people involved in these activities are competent and well-organized.

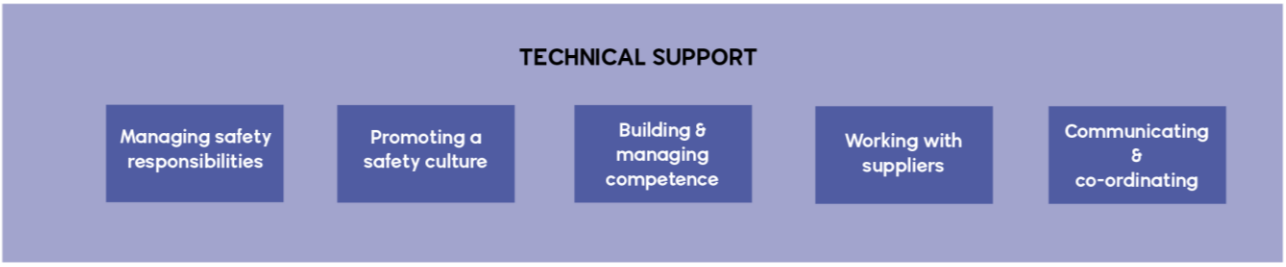

TECHNICAL SUPPORT
Managing safety responsibilities
Promoting a safety culture
Building & managing competence
Working with suppliers
Communicating & co-ordinating

Figure 8: Team Support Activities

3.8.1 Managing safety responsibilities

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.

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.

3.8.2 Promoting a safety culture

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 and near misses (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.

[4] James Reason (6) refers to an organizational culture that meets this criterion as a 'just culture'.

3.8.3 Building and managing competence

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 are 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 to decide what to do and to do it properly. This may depend on the help they are given – people can learn on the job if properly 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 confirm that they meet these requirements.

3.8.4 Working with suppliers

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 confirm 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 confirm 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 **Managing 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 confirm 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.

3.8.5 Communicating and co-ordinating

There may be more than one organization involved in performing the work and there will certainly be other organizations with whom your organization works. These other organizations will all play a part in delivering safety, and communications and co-ordination are required to support that.

If your organization has 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

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. Co-ordination may lead to carrying out the project in a particular order or way.

4 USING THE GENERIC PROCESS

If you already have an ESM process in place, we hope that you will use the generic process in this volume as a benchmark for assessing your process. If you do not already have an ESM process, we hope that you will find the generic process useful for creating one. For every activity above, you will be able to find guidance in the other parts of this handbook on performing that activity. You do not have to use the approach described there and it is not the only effective approach, but it has been proven in practice. More detailed guidance is available in Volume 2 of the iESM Guidance and in supporting Application Notes, available from www.intesm.org.

You might also find the following further reading helpful:

- *Crash: Learning from the World's Worst Computer Disasters*, T Collins and D L Bicknell, Simon & Schuster Ltd, 1999, ISBN 0684868356
- *Software Failure: Management Failure*, S Flowers, Wiley, 1996, ISBN 0471951137
- Mission Improbable: Using Fantasy Documents to Tame Disaster, L Clarke, University of Chicago Press, 2001, 0226109429
- *Reducing risks, protecting people: HSE's decision-making* process, UK Health and Safety Executive, 2001, ISBN 0 7176 2151 0
- *Safeware: System Safety and Computers*, Nancy G Leveson, 1995, ISBN 0201119722
- PAS 55-1:2008 / ISO 55000-1, Asset management. Specification for the optimized management of physical assets

5 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.

6. REFERENCES

This section provides full descriptions of documents that we have referred to in the text.

1. 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.*
2. Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment
3. ISO 31000, Risk management – Principles and Guidance
4. ISO / IEC 61508-2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
5. EN 50126-1:2017, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety, Part 1 Generic RAMS Process EN50126-2:2017, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety, Part 2 Systems Approach to Safety
6. Managing the Risks of Organizational Accidents, James Reason, 1997, ISBN 1840141050
7. PD CLC/TR 50506-1: 2007, Railway applications. Communication, signalling and processing systems. Application guide for EN 50129. Cross-acceptance

Note: This revision (Issue 1.4) of Volume 1 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.

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