Disclaimer
We have taken the trouble to make sure that this document is accurate and useful, but it is only a guide. Its content does not supplement nor remove any duty or responsibility others owe. In issuing this document, we do not guarantee that following any documents we publish is enough to make sure there are safe systems of work or operation. Nor do we agree to be responsible for monitoring our recommendations or people who choose to follow them, or for any duties or responsibilities others owe. If you plan to follow the recommendations, you should ask for independent legal advice on the possible consequences before doing so.

The Yellow Book now contains guidance on the application of the Yellow Book fundamentals to both projects and maintenance. A significant proportion of the guidance is written primarily for people working on projects. We have removed this guidance from this version, retaining the guidance which is written, at least in part, for people working in the maintenance phase. If you are applying the Yellow Book to maintenance you may find this a shorter and more convenient version to use from day to day. However, the text that we have removed will probably be of interest and value to you from time to time. Therefore, we hope that, if you use this abridged version, you will still keep the full book to hand for reference. We have clearly marked all the points where we have removed text.

Published by Rail Safety and Standards Board on behalf of the UK rail industry
This page has been left blank intentionally
Foreword

The Yellow Book is published by Rail Safety and Standards Board (RSSB) on behalf of the rail industry as a whole and updated under the direction of a steering group with representatives from across the industry. It is published in two volumes. Volume 1, which was originally published in 2005, sets out the fundamentals of Engineering Safety Management while volume 2 provides guidance on putting the fundamentals into practice.

Issue 3 of the Yellow Book covered railway projects, but in 2005 we published issue 4 of volume 1 in which we extended the fundamentals to cover railway maintenance as well. We also published an application note which provides guidance on putting these fundamentals into practice in a maintenance application.

Now we have reissued volume 2 so that it provides, in one integrated volume, guidance applicable to both projects and maintenance. We know that effective co-operation is essential to railway safety. We hope that this integrated guidance will allow railway professionals to co-operate even more effectively.

In updating volume 2, we have also tried to serve better those railway professionals whose work affects safety but who control risk through the disciplined and skilful application of standards, procedures and assessments. This reflects in part a shift from absolute reliance on risk assessment to an increasing reliance on developing and using improved standards and procedures, as embodied in the European railway interoperability directives and, in the UK, in the ‘The Railways and Other Guided Transport Systems (Safety) Regulations 2006’ (the ‘ROGS regulations’).

We did acknowledge in issue 3 that there were situations where risk was better controlled through standards and procedures, but readers of issue 3 in such situations would have found limited help with distinguishing the parts of the guidance which were relevant to them, such as the guidance on safety culture, from those parts which were not, such as the guidance on safety cases. In issue 4 we are much clearer on this. Where we know that the guidance in a chapter may need adaptation for a particular situation, then we say so.

Most of the chapters in issue 4 will be relevant to all readers but there are some chapters where the guidance remains primarily relevant to those readers who need to carry out risk assessment. In the next issue of the Yellow Book we intend to provide guidance on how to put all fundamentals into practice in applications where risk is controlled through standards and procedures, including those that fall under the interoperability directives and ROGS regulations.

We welcome feedback on this issue and our future plans, and will always try to respond to the needs of our readers. Please use the suggestion form in the full version of the Yellow Book if you want to send us comments.
Acknowledgements

There are now far too many contributors to the Yellow Book to acknowledge them all. In particular, the contents of this volume draw on a number of previous Yellow Book publications, each of which collectively includes the contribution of many people from across the railway industry and beyond.

This particular revision was prepared under the guidance of the following steering group, editorial committee and drafting team members:

Neil Barnatt  Richard Barrow
Paul Cheeseman  John Corrie
Dr Robert Davis  Bruce Elliott
Tony Fifield  Terry George
Eddie Goddard  David Jeffrey
Richard Lockett  Andy Mallender
Wendy Owen  Gab Parris
Martin Robinson  Mark Roome
Keith Rose  Jon Shaw
Louise Shaw  John Shepheard
Keith Watson  Ed Wells

This revision incorporates new guidance on Goal Structuring Notation which was prepared by a working group including the following additional contributors:

Dick Dumolo  Christopher Hall
Nick Holmes-Mackie  Dr Tim Kelly
Carolyn Salmon

We gratefully acknowledge the contribution of all of these people. We are also grateful to the following organisations that have allowed their personnel to contribute their time:

Association of Train Operating Companies  Atkins Rail
Bombardier Transportation  Channel Tunnel Rail Link (UK) Limited
ERA Technology  Hitachi Rail Group
Mott MacDonald Limited  London Underground Limited
Lloyd's Register Group  Network Rail
Porterbrook Leasing  Praxis High Integrity Systems
Rail Safety and Standards Board  Scott Wilson Railways Limited
Technical Programme Delivery Limited  Tube Lines
University of York  Westinghouse Rail Systems Limited

All of the contributors provided their time and expertise as professionals committed to improving railway safety. Their opinions do not necessarily reflect those of their employers.
Part 1

Introductory Material
Chapter 1

Introduction

1.1 Purpose and scope of this volume

Since issue 3, the Yellow Book has been in two volumes. Volume 1 presents the fundamentals of Engineering Safety Management (ESM) and volume 2 provides guidance on implementing the ESM fundamentals presented in volume 1.

Issue 3 of the Yellow Book only dealt with projects – activities that make significant, deliberate changes to the railway. In 2005, we reissued volume 1 at issue 4 to extend the fundamentals to cover maintenance as well. This issue of volume 2 now extends the guidance to cover maintenance as well, and benefits from some other improvements. It also incorporates some guidance on software, Human Factors and systems issues which was previously published in Yellow Book ‘application notes’ – pamphlets which are used to supplement the Yellow Book proper.

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

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 publication, 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 the Yellow Book may be useful for managing these other losses, 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 the health and safety of the people involved with the work itself. You will find that good practices in both fields are similar. We do discuss occupational health and safety issues in this volume and we do recommend that you co-ordinate the activities that you carry out to ensure railway safety and occupational health and safety. However, we only claim that the techniques described in the Yellow Book represent good practice for controlling railway safety risk. You should make sure that you are familiar with good practice and legislation in occupational health and safety, before adapting the guidance of this book for that field.

The Yellow Book 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, the Yellow Book 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 organisation’s values, and those of society at large, and for demonstrating that they do so.

1.2 How this volume is written

After this introduction we introduce a System Lifecycle and present high-level guidance on what ESM activities you should carry out in each phase of this lifecycle.
Then we provide more detailed guidance in a series of chapters, where each chapter deals with one or more of the fundamentals from volume 1. Each fundamental is reproduced in a box at the beginning and the summary guidance from volume 1 is reproduced afterwards. These chapters of volume 2 are in the same order as the fundamentals of volume 1. The fundamentals in volume 1 are arranged under four headings:

- **organisation**: the general features needed by any organisation whose work affects safety;
- **process**: methods of working that affect safety;
- **risk assessment**: identifying hazards and assessing risk; and
- **risk control**: controlling risk and showing that it is acceptable.

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

The chapters refer to each other and these cross-references are summarised in ‘Related guidance’ sections at the end of each chapter.

Supporting material is supplied in appendices which provide:

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

Specialist terms are printed in bold when introduced (but note that bold text is also used to highlight key words in lists). The most specialist terms, such as ‘Safety Case’ are written with initial capitals. All of these are defined in appendix A, the glossary. Appendix A also provides some more precise definitions of some terms which are used in a manner consistent with their ordinary English meanings. These are not written with initial capitals.

There is a list of referenced documents in appendix F and references are indicated in the text in the form '[F.1]'.

### 1.3 Relationship of Yellow Book with other publications

The Yellow Book has been designed to reflect good practice and the process used to write it has involved reviewing relevant UK, European and international standards. As a result, the Yellow Book is generally consistent with such standards.

We have also written the Yellow Book to be consistent with UK and European legislation, although our objective has been to give you guidance that complements this legislation rather than to write a book on how to comply with it.

We think that the Yellow Book will help you comply with standards and legislation, but following it will not generally be enough to comply and we cannot guarantee that there will be no conflicts. You will need to establish what standards and legislation apply to you. You may find the following contacts useful in doing so:
• RSSB (www.rssb.co.uk) maintain the Railway Group Standards that apply to some UK railways. They also publish information on the ‘Technical Specifications for Interoperability’, standards associated with European railway interoperability directives.

• Network Rail (www.networkrail.com) and London Underground Limited (www.tfl.gov.uk/tube) maintain standards catalogues for use on their networks.

• National, European and international standards can be obtained from the national standards organisation which is BSI (www.bsi-global.com) in the UK.

• Information on safety regulation in the UK is provided by the Office of Rail Regulation (www.rail-reg.gov.uk), of which Her Majesty’s Railway Inspectorate (HMRI) is a part.

• Information on the way that European legislation is embodied in UK law is provided by the Department for Transport (www.dft.gov.uk).

• Standards, guidance and codes of conduct are issued by the Engineering Council (www.engc.co.uk) and other professional bodies.

• There is a web-site for the Yellow Book itself (www.yellowbook-rail.org.uk) which may contain more up-to-date information.

1.3.1 How safe is safe enough?

In 2005, RSSB launched a new publication on behalf of the industry - ‘How safe is safe enough?’ [F.2] which tackles some of the long-standing challenges that railway companies face in making consistently safe decisions every day. It brings together a single overview of good practice in making decisions which affect safety.

The objective of ‘How safe is safe enough?’ is to ensure that the railway industry takes decisions with the proper balance of safety, performance and cost and that are consistent, legal, ethical and workable. It gives the rail industry and other stakeholders a common societal view of what is acceptable, helping companies to meet their legal duties without spending disproportionately on safety.

Yellow Book complements this by providing guidance on how to achieve and demonstrate safety in an effective and efficient manner.

---

1 RSSB’s work in this area is ongoing. You may wish to check the RSSB web-site for later guidance.
Chapter 2

General high-level guidance

2.1 Concepts and terminology

It is helpful to explain some concepts and terminology that we will use throughout this volume.

2.1.1 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.

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.

Hazards arise from events or sequences of events such as Failures, that is, when a system or component is unable to fulfil its operational requirements. An accident sequence may be represented as follows:

![Figure 2-1 Accident sequences](image)

However, not every failure results in a hazard and not every hazard results in an accident. 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.

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 Chapter 17.

*Note that even in complex systems, SILs are not the only means of controlling Systematic Failures; they may be controlled through architectural design features as well.*

**Risk** is defined to be the combination of the likelihood of occurrence of harm and the severity of that harm.

The **Individual Risk** experienced by a person is their probability of fatality per unit time, usually per year, as a result of a hazard in a specified system.

### 2.1.2 Systems

By a railway **system**, we mean a coherent part of the railway, such as a railway line or a train or an interlocking. Any railway project or maintenance activity can be associated with a system: introducing a new system or changing or maintaining an existing one.

Although the Yellow Book fundamentals make clear that you should understand the context within which your system exists and that you should work with others to reduce risk on the railway as a whole, your organisation will have a primary responsibility to make sure that the system that you are working on does not contribute to accidents, or at least that the risk associated with it has been controlled to an acceptable level.

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](image-url)
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 the system represents the extent of our responsibility, then the hazard is the point at which we cease to be able to affect the course of events.

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

We define a Causal Factor to be any state or event which might contribute to a hazard.
2.2 The System Lifecycle

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

<table>
<thead>
<tr>
<th>System lifecycle (group of phases)</th>
<th>System lifecycle phase</th>
<th>Definition of phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Service</td>
<td>Concept and Feasibility</td>
<td>All activities that precede the construction of a requirements specification for the system or equipment</td>
</tr>
<tr>
<td></td>
<td>Requirements Definition</td>
<td>The construction of a requirements specification</td>
</tr>
<tr>
<td></td>
<td>Design</td>
<td>All activities that result in a design baseline for the system and equipment</td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>All activities that are involved in realising the design before introducing any changes to the railway</td>
</tr>
<tr>
<td></td>
<td>Installation and Handover</td>
<td>All activities of introducing the change to the railway continuing up until normal operations start.</td>
</tr>
<tr>
<td>In Service</td>
<td>Operations and Maintenance</td>
<td>All activities involved in operating the system or equipment or keeping it fit for service</td>
</tr>
<tr>
<td>Post-Service</td>
<td>Decommissioning and Disposal</td>
<td>All activities involved in taking the system or equipment out of service, removing the system or equipment from the railway and then disposing of it</td>
</tr>
</tbody>
</table>

**Figure 2-3 The System Lifecycle**

*Note that 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 organisation during its life.*
Note also that each phase will generally involve two sorts of activities:

- activities which contribute directly to the output of the phase; and
- activities which check that these outputs are correct, that is consistent with the inputs to the phase and the overall requirements for the system.

Figure 2-3 collects the phases of the System Lifecycle into three groups. The In-Service and Post-Service groups only have one phase each, but later on we will find other ways of breaking down the activities that concern us within the groups.

Although the ESM fundamentals apply to all of the phases, they are sometimes applied in different ways in different phases. Each of the System Lifecycle phases within the Pre-service and Post-service groups can be considered as projects and we provide guidance on what to do in each of these phases in Chapter 3. We provide guidance on what to do in the Operations and Maintenance phase in Chapter 4.

2.3 Systems in context

While you may focus your energies on controlling the contribution of one system to overall risk on the railway, it does not follow that you can ignore the rest of the railway. On the contrary, you have to understand the context in which this system operates in order to understand the risk.

Most real accident sequences involve interactions between several systems. To understand how your system contributes to overall risk on the railway you have to understand how other systems may mitigate or exacerbate hazards in your system and how your system may mitigate or exacerbate hazards arising elsewhere. This requires a thorough understanding of the interfaces between all of the systems involved. These will include internal interfaces between sub-systems within your overall system and external interfaces between your system and other systems.

Note: we use the phrase 'sub-system' in a general sense to mean any small system which is part of a larger system. You should note that other publications, particularly those discussing European interoperability legislation, use the word in a more limited sense to refer to one of a fixed list of parts of the railway.

Also, if your system or its context involves people, which is almost always the case, you need to take account of the way that people interact with your system in order to manage people's contribution to the risk.

To err is human. Human error plays a part in most, if not all, accidents. If you have not considered human error when specifying your work, it will be difficult to show that you have controlled risk to an acceptable level. Similarly, you should consider the impact of human intervention on the management of hazards. Understanding how people react in the event of a failure is important in understanding the overall system risk.

Human error has causes. We understand some of these and know how to prevent them. When changing the railway you can and should follow the guidance in volume 1 to 'consider the people who your work will affect, and carry it out in a way which helps them avoid mistakes'. You should also look for opportunities to prevent human error from leading to an accident. People prevent accidents as well as contributing to them. Therefore you should try to help people prevent accidents.
In order to make decisions about whether risk is acceptable, it is not sufficient to look at the risk associated with each hazard of the system on its own. The overall risk must be considered, because a small risk associated with one hazard may be sufficient to make the overall risk unacceptable.

2.4 Taking decisions about safety

Engineering Safety Management 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.

If you are faced with a decision that involves risk, you will generally have to do four things:

1. Establish the facts on which you have to take a decision – what the hazards and risks are.
2. Establish and apply decision criteria to the facts and seek endorsement of your decisions from whoever will eventually approve the system or work.
3. Follow through on these decisions so that you can satisfy yourself and others that they have been fully carried out.
4. Seek approval before doing something that will affect risk on the railway such as starting work on the operating railway or bringing a new system into service.

Figure 2-4 illustrates this idea.

![Figure 2-4 Decision making](image-url)
Earlier versions of this book were aligned to:

- the UK legal framework for taking decisions about safety at the time: the duty to reduce risk 'so far as is reasonably practicable', recognising that this could sometimes be discharged by following good practice; and
- some aspects of the arrangements for approving work on UK railways.

During the lifetime of this book, the UK legal framework and the arrangements for approving work have both changed and they may change again. Moreover, this book is now being used by people outside the UK.

In order to provide the most useful and enduring guidance, we have now modified the volume so that it no longer assumes any particular legal framework or approvals regime. This means that, before you can use the guidance, you will have to establish:

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

When you have established these things, you will need to adapt the guidance to your specific situation. Our experience is that this guidance is applicable with limited and localised adaptation to a wide range of different legal frameworks and approvals regimes.

We discuss each of these topics a little further below.

### 2.4.1 The approvals regime

We consider that, before something is done that might affect railway safety, such as bringing a new system into service or starting work on the operational railway, someone should review the evidence that risk has been controlled and take an explicit decision as to whether it has been controlled to an acceptable level or not. Sometimes this evidence will include the results of a professional review by someone independent of the work (see Chapter 13). In this book we refer to this decision-making process as **Safety Approval** and to anyone who takes such a decision as a **Safety Approver**.

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

Note that, if you do not require Safety Approval from outside your organisation, it does not follow that other parties cannot hold you to account later if you do not properly control risk.

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

You should find out who will act as Safety Approvers for your work, what they must approve, the basis on which they will grant approval, and the evidence that they will require.
Note: you will also need to establish the terminology that your Safety Approvers use. The process that we refer to as ‘Safety Approval’ may be described as ‘acceptance’ or ‘endorsement’ or something else.

2.4.2 The legal framework for taking decisions about risk

As we said above, earlier versions of this book were aligned to the UK legal framework for taking decisions about safety at the time: the duty to reduce risk ‘so far as is reasonably practicable’. However, other states have adopted different criteria for taking safety decisions, including duties to:

- ensure that overall risk on the railway is not increased; and
- ensure that the risk experienced by a regular railway passenger is a small fraction of the risk that they experience in the rest of their life.

Moreover, to some degree or other, most legal frameworks rely on compliance with standards as a necessary, and in some cases sufficient, basis for controlling risk. We expand on this in the next section.

There are a few aspects of the guidance in this volume which are only relevant to people who have a legal obligation to reduce risk ‘so far as is reasonably practicable’. We have made this restriction clear in the sections concerned. We have retained this guidance because we believe that it will be of value to some of our readers. However, you should not take this to imply that this obligation applies to you, whether you are working in the UK or elsewhere. You will always need to establish the legal framework or frameworks which apply to you and then adapt the guidance in this book accordingly.

2.4.3 The role of 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. To understand this, it is convenient to refer to some definitions from the UK Offshore Operators Association’s ‘Industry Guidelines on a Framework for Risk Related Decision Support’ [F.1]. This document explains how risk related decisions can be placed in a spectrum running from:

- **technology-based** decisions for risks that are well understood, uncontroversial and with low severity consequences; to
- **values-based** decisions, where there is significant novelty, public concern or potential for catastrophic consequences.

If you are faced with decisions towards the technology-based end of the spectrum, you can replace some of the guidance in this volume about formal risk assessment (putting the **Identifying hazards** and **Assessing risk** fundamentals into practice) with reference to authoritative good practice (see section 15.2.2.6). Essentially the good practice embodies the results of analysis that has already been done which you do not need to repeat.
As we said in volume 1, ‘If the risk comes completely within accepted standards that define agreed ways of controlling it, evidence that you have met these standards may be enough to show that you have controlled the risk.’

We also repeat the warning of volume 1 that, ‘Before you decide that just referring to standards is enough, make sure that:

- the equipment or process is being used as intended;
- all of the risk is covered by the standards;
- the standards cover your situation; and
- there are no obvious and reasonably practicable ways of reducing risk further.’

If a standard does not completely cover the risk, its provisions may still provide a useful starting point for measures that do cover the risk.

Even if you use the full guidance of this book, you will still need to show that you have used good practice, unless you have moved so far from the technology-based end of the spectrum that there is no established good practice for what you are doing.

Hence, for several reasons, you will need to make sure that you are familiar with all of the standards that are relevant to your work.

Figure 2-5 illustrates the parts that good practice, formal risk assessment and stakeholder consultative processes might play in different sorts of decisions. Once the context for a risk-related decision has been located on the vertical dimension, the width of each band gives a rough indication of the relative significance of each type of activity to that decision.

Although we are primarily concerned with the role of ‘Good practice’ at the technology-based end, we should also remark on the role of ‘Consultative processes’ at the values-based end.

As you move towards the values-based end of the spectrum, you are likely to find that the process of establishing the facts becomes a progressively smaller part of the problem, and that establishing decision criteria becomes the larger part. For these decisions, you will need to supplement the guidance in this volume with significant additional activities to consult stakeholders in order to arrive at justifiable decisions.
2.5 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 organisation’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 organisation’s procedures in the normal course of business and only refer to this volume if these procedures do not fully cover the risk. You may find the guidance in this volume useful:

- as a starting point or benchmark for general ESM procedures; and
- as guidance on how to make sure that procedures which are designed to control specific risks do indeed control risk to an acceptable level.

**Figure 2-5 Approaches to different risk decisions**
Note: a comprehensive set of procedures for managing risk is often referred to as a Safety Management System.

We know that it is not possible to describe a single process that would represent an effective and efficient approach to performing Engineering Safety Management on all railway projects and maintenance activities, for two reasons:

- Railway projects and maintenance activities vary greatly and what would be effective and efficient in one area will require change to be effective and efficient in another area.

- There may be more than one effective way of doing Engineering Safety Management in any given situation. Railway organisations employ a variety of processes already and it would be inefficient for any organisation to abandon processes that work well and are well understood.

It is for these reasons that we have distilled some common fundamentals of Engineering Safety Management which we presented in volume 1. Volume 1 advised that, ‘If your organisation already has a systematic approach to managing safety, you should check that it puts all the fundamentals into practice. If you do not have a systematic approach yet, or if your approach does not yet put all the fundamentals into practice, you may find volume 2 useful’.

If you have not already checked your organisation’s processes against the fundamentals, you will almost certainly find it worthwhile to do that first – it will help you focus on the parts of this volume that are most useful to you.

It will also help if you establish what phases of the generic System Lifecycle your activities affect. You do not have to map your activities in detail to this lifecycle and in general such a mapping can be quite complex: it is perfectly normal for organisations to be working in more than one phase at the same time and for them to come back to the same phase more than once. At the very least, however, you need to decide whether you are involved in maintenance or projects or both, because some parts of the guidance offer different advice for maintenance and project activities.

Finally, it is a good idea to make an initial assessment of the risk, novelty and complexity associated with your work. We recommend that your Engineering Safety Management activities should be commensurate with these things. If the risk comes completely within accepted standards that define agreed ways of controlling it, evidence that you have met these standards may be enough to show that you have controlled the risk. Moreover, if you are working in an area which is low-risk, simple and conventional, then you may wish to simplify the activities suggested below and you may be able to use standards to control risk in some areas. But if you are working in an area which is unusually high-risk, novel or complex, then you may need to extend or supplement the activities described if you are going to control risk properly.
Having done this, it may be sufficient to go directly to parts 2, 3, 4, and 5. You will find that each of these parts corresponds to one of the groups of fundamentals in volume 1. Within these parts you will find that each chapter provides guidance on implementing one or more fundamentals. So, you can simply go to the chapters for the fundamental or fundamentals which you need guidance on, look up the guidance appropriate to your part of the System Lifecycle and interpret it in the context of the risk, novelty and complexity associated with your work.

However, if you do this, you will find little guidance on the order in which to do things – what to do first and what to do later. For the reasons we explained above, we cannot prescribe a single, universal process. But we can give you some advice on the ordering and timing of activities which you can use to construct a programme of work and we do this in the next two chapters – Chapter 3 provides guidance for projects; Chapter 4 provides guidance for maintenance. The activities listed in the guidance are appropriate to a fairly complex undertaking. You should take the novelty and complexity into account when deciding what you do; you may not need to carry out all of these activities in order to put the fundamentals into effect in your work.

Do bear in mind though that there are important aspects of Engineering Safety Management that do not fit easily into such a programme. Fostering 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 an organisation with a sound approach to Engineering Safety Management will want to give continuous attention to. So, if you just follow the guidance in Chapter 3 or Chapter 4 or both, you may miss something.

Broadly speaking Chapter 3 and Chapter 4 discuss the following ESM fundamentals:

- Safety planning;
- Systematic processes and good practice;
- Independent professional review;
- Defining your work;
- Identifying hazards;
- Assessing risk;
- Reducing risk;
- Safety requirements;
- Evidence of safety;
- Acceptance and approval.

You should take particular care to ensure that you have activities in place to implement the following fundamentals which cut across the lifecycle.

- Safety responsibility;
- Organisational goals;
- Safety culture;
- Competence and training;
- Working with suppliers;
• Communicating related information;
• Co-ordination;
• Continuing safety management;
• Configuration management;
• Records;
• Monitoring risk.

So we repeat our advice to check your organisation’s processes against all of the fundamentals and, to assist you, Table 2-1 provides a checklist which you may wish to photocopy and fill in.
<table>
<thead>
<tr>
<th>Fundamental</th>
<th>Do we already fully implement this fundamental?</th>
<th>Or do we need to consider using the guidance to strengthen our processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety responsibility</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Organisational goals</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Safety culture</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Competence and training</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Working with suppliers</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Communicating safety-related information</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Co-ordination</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Continuing safety management</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Safety planning</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Systematic processes and good practice</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Configuration management</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Records</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Independent professional review</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Defining your work</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Identifying hazards</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Assessing risk</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Monitoring risk</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Reducing risk</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Safety requirements</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Evidence of safety</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Acceptance and approval</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Table 2-1 Checklist for implementation of fundamentals
Chapter 3

High-level guidance for projects

This chapter has been removed from this version but is available in the full version of the Yellow Book.
Chapter 4

High-level guidance for maintenance

4.1 Introduction

This guidance is relevant to the Operations and Maintenance phase of the System Lifecycle. However, the scope of the Yellow Book does not include offering guidance for operations, so this chapter is restricted to maintenance.

We will introduce a maintenance cycle which breaks maintenance down into five stages, and then provide some guidance on what to do in each stage. First though, we offer some general guidance, starting with making clear what we mean by ‘maintenance’.

4.2 A definition of maintenance

Maintenance is a term used to describe all of the activities that need to be carried out to keep a system fit for service, so that assets (sub-systems, components and their parts) continue to be safe and reliable throughout the operational lifecycle phase. This means that when we talk about maintenance we are including activities such as:

- repetitive asset maintenance, inspection and testing;
- fault finding and repair;
- component replacement; and
- like-for-like renewal.

Maintenance is often concerned with keeping some parameter, such as the distance between the rails, within specified limits. It may be that these limits are specified to the maintenance organisation in standards and that someone else is relying on this parameter remaining within them. Alternatively, it may be that the limits have been specified by the maintenance organisation in order to meet targets for safety, performance, reliability and so on. Either way, allowing the parameter to go outside its limits may be hazardous.

We are also talking about planning and record keeping for maintenance, including:

- planning and recording the way maintenance will be done for new and changed assets; and
- planning and recording changes to existing maintenance activities.

The boundary between what is described as maintenance and what constitutes a project is not always clear. Maintenance sometimes also includes:

- refurbishment and overhaul;
- system modifications (temporary or permanent); and
- system upgrades.

The guidance in this chapter applies to these activities as well, but you may find it better to manage them as small projects.
4.3 **A summary of maintenance and risk**

If something could affect safety, then part of keeping it fit for service will involve keeping it safe. As nearly all railway equipment has the potential to affect safety, then controlling risk is an integral part of nearly all railway maintenance. Maintenance can contribute to risk through both action and inaction.

This volume provides guidance on controlling risk during maintenance. We do not provide guidance on achieving the other aspects of fitness for service but we recognise that they must be achieved together. In particular, we recognise that system reliability (performance) is closely linked to safety, particularly where degraded methods of working need to be introduced to operate trains when an asset fails.

When we talk about risk, we are considering the likelihood that an accident will happen and the harm that will arise to people who come into contact with the system, including staff and passengers. In many cases, risk cannot be eliminated entirely. We must accept this if we are to continually improve safety.

4.3.1 **New and changed assets**

Where projects affect operational railway assets (for example during stage-works), they may introduce new hazards. For example, the Safety Integrity of operational signalling circuits must be maintained when engineering work is taking place alongside lineside cable routes that contain working control circuits. Responsibilities for asset maintenance, including any changes to the way maintenance work will be done, will need to be agreed between the project and the maintenance organisations before the project work starts. The maintenance requirements should be fully understood and all of the resources should be put in place to implement them.

Before changes to the railway are placed into service, the project and maintenance organisations will have to agree and make sure that all of the resources that are needed for operational safety are put in place. Resources may include:

- new or upgraded maintenance facilities (such as depots and plant);
- additional maintenance tools and test equipment;
- spare parts;
- new and changed maintenance standards and procedures;
- staff competence changes;
- organisational changes; and
- system configuration records.

The maintenance organisation should find out whether the project has considered the risks in the context of the specific application or just the generic risks associated with the new or changed equipment.

Maintenance organisations might also need to change the maintenance for existing equipment as a result of the introduction of the new equipment and any changed railway operations that result from the project.

4.3.2 **Existing maintenance regimes**

If you are maintaining an existing application of a railway system, the maintenance work you are doing should be based on existing good practice, but you might not be able to fully justify the reasons why the work is being done in the way that it is.
In most cases, the way maintenance is done now is based on years of developing good practice and experience. Some decisions about maintenance work have resulted from enquiries into major incidents and some more recent practices may be fully supported by a risk assessment.

You can use this volume to help you to decide whether you are going to continue to work as you are or change something. In either case, you will need to decide whether the maintenance work that you are carrying out makes the best use of available resources and manages all of the risk to the required level. You should record and analyse information about how the railway is actually performing and compare it with the safety performance that you require.

It is not sufficient just to gather information whenever there is an incident or a deliberate change that could affect the part of the railway for which you are responsible. You should continually gather information, because change on the railway is continual and cannot always be detected easily. For example, there may be changes to:

- traffic patterns, train speeds and loadings;
- organisations and personnel;
- other parts of the railway;
- the local environment;
- society (for example increased vandalism, terrorism threat); and
- the level of risk that is considered to be tolerable.

If you only maintain a part of the railway system, it is important to understand that changes that occur elsewhere can affect the part of the railway for which you are responsible. It is therefore good practice for your maintenance organisation to work with other organisations in areas where work could result in increased risk. For example, deterioration of a track-bed can result in a greater rate of deterioration of rolling stock suspension, and vice-versa.

You should understand how the part of the railway that you are maintaining degrades during the lifecycle. To do this, you will need to understand what critical failures modes exist, particularly those where a single item failure could lead to a significant incident. Two examples are:

- failure of a component (such as a station escalator brake) as a result of the expected cyclic loading; and
- abnormal loading of a component because of a failure in some other part of the railway (such as rail failure as a result of excessive wheel flats).

The maintenance work that you do should take these things into account.

You will also have to monitor periodically the actual performance of the railway and compare it with the performance that you predicted when you decided what maintenance work you were going to do. If there is a difference, it could be because:

- the assumptions, dependencies and caveats used as a basis for your maintenance decisions were inappropriate;
- the design of the equipment is not sufficiently robust; or
- not all of the risks were properly identified or controlled.
Figure 4-1 illustrates some of the concepts described above. It shows how, without intervention, risk may rise above an acceptable level (dotted line), but intervention can prevent this from happening (solid line).

**Example of risk during the operational life cycle**

**Example of risk arising from project work**

**Figure 4-1 Relationship between maintenance and risk**
4.3.3 Focussing maintenance on risk

There are well-established systematic processes which may be used to ensure that maintenance activities are focussed on the risk. Normally they consider risks beyond safety risk (such as performance risk) but they can be used to control safety risk as well. They generate maintenance strategies from details of the characteristics of the failure under review, the risks that might be involved and the costs that are incurred.

The basic information about the selected asset in its operating context that needs to be taken into account is:

- the functions and the associated performance standards of the asset;
- the ways it can fail to fulfil its functions;
- the causes of each functional failure;
- what happens when each failure occurs;
- the consequences of each functional failure;
- what can be done to prevent each failure; and
- what should be done if a suitable preventive task cannot be found.

This approach is consistent with the Yellow Book fundamentals because it takes into account the risks associated with failures that might result from not conducting maintenance activities. Highly structured inter-disciplinary review groups (at least one person from maintenance and one from user function) need to be established to apply the process and hence determine the maintenance requirements of each asset.

A great strength of this approach is the way in which it provides simple, precise and easily understood criteria for deciding which (if any) preventive tasks are technically feasible and worth doing in any given operating context. It also provides a means for deciding how often each task should be done and who should do them.

4.4 Maintenance cycles

Maintenance is often modelled as following a Plan-Do-Review cycle. We find that it is normal to be able to discern two interlocking cycles. A single ‘Do’ stage is subject to planning and review at two levels:

- a day-to-day level, where the planning and reviewing is concerned with the immediate day-to-day maintenance tasks and is probably performed by the organisation doing these tasks; and
- a strategic level, where the planning and reviewing is concerned with long-term issues, such as when to replace assets, and may be performed by a separate group, perhaps called an ‘asset management’ group.
This cycle is illustrated in Figure 4-2.

**Figure 4-2 The maintenance cycles**

We provide guidance on activities which are appropriate to each stage in a series of diagrams. Each of which takes one stage, suggests a series of activities that are appropriate at this stage and relates these to the underlying fundamental and to the possible techniques and tools for implementing it.

You should also ensure that you have such activities in place to implement the fundamentals which cut across the lifecycle, as stated in section 2.5.

The extent to which this guidance is applicable to your work depends on the risk, novelty and complexity associated with your work.

Figures 4-3 to 4-7, inclusive, illustrate a typical programme of activities.

*Note: although only shown in figure 4-7 a Data Reporting Analysis and Corrective Action System (DRACAS²) is likely to inform the activities of all stages.*

---

² The acronym FRACAS is sometimes used instead
4.5 Planning maintenance (strategic)

Figure 4-3 Planning maintenance (strategic)
4.6 Planning maintenance (day-to-day)

Figure 4-4 Planning maintenance (day-to-day)

4.7 Doing maintenance

Figure 4-5 Doing maintenance
4.8 Reviewing maintenance (day-to-day)

**Guidance**
- Review safety record.
- Collect information on incidents, asset condition data, surveillance results and failures.
- Keep and review records to monitor risk.

**Fundamental**
- Monitoring risk (ch 16)

**Techniques & Tools**
- FMEA/FMECA - used to determine root causes of failures/safety incidents/investigate alleged irregularities of signalling equipment operation.
- DRACAS/FRACAS – used to identify trends (App E).

**Records (ch 12)**

*Figure 4-6 Reviewing maintenance (day-to-day)*

4.9 Reviewing maintenance (strategic)

**Guidance**
- Review safety record.
- Review surveillance results.
- Review information on incidents, failures etc.
- Assess risk and look for control measures.

**Fundamental**
- Monitoring risk (ch 16)
- Assessing risk (ch 15)

**Techniques & Tools**
- DRACAS (App E)
- Fault Tree Analysis (App E)

*Figure 4-7 Reviewing maintenance (strategic)*
Part 2

Organisation Fundamentals
Chapter 5

Safety responsibility

Fundamental from volume 1: Safety responsibility

Your organisation must identify safety responsibilities and put them in writing. It must keep records of the transfer of safety responsibilities and must make sure that anyone taking on safety responsibilities understands and accepts these responsibilities. It must make sure that anyone who is transferring responsibility for safety passes on any known assumptions and conditions that safety depends on.

5.1 Guidance from volume 1

Everyone within your organisation should have clear responsibilities and understand them. Your organisation 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.

Any organisation whose work might contribute to an accident will have a corporate responsibility for safety. This will cover the safety of everyone who might be affected by its activities, which may include workers and members of the public. Your organisation 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 organisation that takes the lead in changing, maintaining or operating some aspect of the railway should make sure that the other organisations are clear on their safety responsibilities and that these responsibilities cover everything that needs to be done to ensure safety.

For each part of the railway, someone should be responsible for keeping up-to-date information about how it is built, how it is maintained, how safely and reliably it is performing, how it was designed and why it was designed that way, and for using that information to evaluate changes.

5.2 General guidance

5.2.1 Introduction

ESM is a team activity, involving people with different backgrounds from across the organisation 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 organisation and between organisations.

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 fundamental applies to people whose action or inaction might contribute to risk. This will include most, if not all, maintenance personnel.

As the fundamental implies, you can only give responsibility to someone who is prepared to accept it.

There are certain legal obligations placed on employers and employees with regard to defining responsibilities. See volume 1 for further details.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for:
- managers responsible for the appointment of staff to safety-related tasks or for determining organisational structure; and
- anyone performing an assessment of personnel competence.

### 5.2.2 Different types of safety responsibility

A basic principle of ESM is that those whose activities create a risk should be responsible for managing and reducing that risk. This implies that safety responsibility should be an integral part of the responsibilities of general management and not divorced from responsibilities in other areas.

These activities may be related to a particular system or piece of equipment (such as development, operation, maintenance, or modification), or to the provision of resources or information. The safety responsibilities related to these activities 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.

Whatever the activity may be, it is important to:
- clearly define the safety roles and responsibilities;
- gain agreement from all parties on their allocation; and
- pass on any relevant safety-related information.

When responsibility for the system’s operation is handed over to another party, risk may then be created by the organisation accepting the system, and therefore some safety responsibilities are also transferred. However, the organisation transferring responsibility will retain accountability for the work it did in the past.

An organisation also needs certain ESM roles that are independent of any particular project. Their responsibilities will include setting safety policy and safety goals, defining other safety responsibilities, granting authority and approval, providing resources, and establishing communication channels.

Safety roles and their responsibilities should be regularly reviewed to ensure that they are still relevant.
5.2.2.1 Head of Safety

An organisation performing safety-related work will commonly appoint a senior person as Head of Safety, responsible for dealing with general safety issues throughout the organisation. They will typically have a high level of authority within the organisation and considerable operational experience and technical knowledge. Transport Operators, organisations which manage infrastructure or operate trains, will usually appoint an officer with such responsibilities in order to meet their legal obligations.

Their role is to promote ESM within the organisation, and to ensure that the work produced by the organisation meets the required safety standards. They will also report on any shortcomings in safety, and provide independent advice on safety issues.

The Head of Safety’s responsibilities may include:

- setting, maintaining and monitoring safety policy;
- ensuring that a Safety Management System is effectively implemented and maintained;
- agreeing the safety classification of projects;
- endorsing key safety documentation;
- monitoring the ESM performed; and
- appointing Independent Safety Auditors and Assessors.

For larger organisations, there may need to be multiple Heads of Safety, with knowledge and experience in different areas.

The people carrying out this role will not necessarily have ‘Head of Safety’ in their job title. The role may be carried out by people with other titles such as ‘Chief Engineer’ or ‘Safety and Standards Director’.

5.2.3 Line Manager

An organisation may assign a Line Manager to a group of staff and/or a group of projects, to ensure that their activities are run effectively and safely. The Line Manager should assure himself or herself that ESM is performed correctly by the staff and on the projects that they manage. The Line Manager should be familiar with the safety issues relating to these projects.

The Line Manager’s safety responsibilities may include:

- assigning sufficient ESM resources (both personnel and other);
- ensuring that staff have the skills necessary for the tasks to which they are assigned (providing training if needed); and
- ensuring that the ESM performed is monitored.

5.2.4 Allocating safety responsibilities

Responsibilities for ESM should be allocated from the top of the organisation downwards. The senior manager in an organisation or department appoints the Heads of Safety and assigns responsibilities to them. The senior manager should also assign safety responsibilities to the Line Managers. In turn, the Line Managers may assign Project Managers to a project, or staff directly to tasks.
It is essential that safety roles and responsibilities are clearly defined and documented. The responsibilities assigned to individuals should be explicit and understood by everyone in the organisation. In this respect, they should be documented and made freely available within the organisation.

The documentation should identify:

- the various organisational positions;
- the associated responsibilities and authorities for ESM; and
- the communication and reporting channels.

Safety roles and responsibilities should be put in writing. When someone is proposed for safety-related work, they should be given a task description, detailing their specific responsibilities, the authority that they will carry, and their lines of reporting. They should confirm that they understand and accept the task description before their assignment is confirmed.

There should be some form of organisational structure chart available to all employees, containing details of the organisation’s safety roles.

The definition of safety responsibilities should be periodically reviewed. You will need to make sure that everyone within your organisation who is given safety responsibility clearly understands the extent of that safety responsibility. This understanding should start at staff induction and be developed throughout their career, for every person.

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.

5.2.5 Recording safety responsibility

Your organisation should write down the safety responsibilities that each person has, so that safety decisions are taken at, and escalated to, the correct person in your organisation. You should make sure that personnel are formally advised of their responsibilities and understand what they must do, particularly whenever there is a change in safety responsibility.

One way of doing this is by issuing job descriptions to your staff. You should make sure they are briefed on the contents and confirm that they clearly understand their responsibilities.

5.2.6 Safety responsibilities at boundaries

Your organisation should find out and record how the part of the railway that you are responsible for interfaces with passengers, neighbours, the rest of the railway and the work done by other organisations.

It is good practice to 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 properly 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 to that they can resolve it.
For example, responsibility for the track system may be divided between a number of maintenance organisations using defined geographical boundaries, whereas the corresponding signalling equipment boundaries may overlap in a more complex component boundary arrangement. Similarly, for rolling stock, the responsibility for maintenance of the traction system on a vehicle may be separate from the responsibility for maintenance of internal fittings on the same vehicle.

It is also good practice to 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 organisation, 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 organisations 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.

5.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

5.4 Additional guidance for maintenance

5.4.1 Scope of safety responsibility

Your maintenance organisation will need to set out and communicate (see Chapter 9), what responsibilities it has for safety, including:

- the parts of the railway it has to maintain;
- the maintenance work it will do;
- the people whose actions it is responsible for; and
- the people whose safety it is responsible for.

You will have to agree responsibilities with any other organisation that the work will involve and be clear how the work that you do interfaces with work done by other organisations. For example, your maintenance organisation could be responsible for infrastructure maintenance on a metro system; another organisation is responsible for rolling stock maintenance and a third organisation for incident investigation covering both infrastructure and rolling stock events.

You should understand the relationship between the safety of the parts of the railway that you maintain and the overall safety of the railway. For example, a signalling maintenance organisation should understand how the maintenance work that it does could affect the safe operation of train movements and its own staff. It should also know how the maintenance is directly related to the safety of the travelling public.
5.4.2 Allocating safety responsibility

Someone should be given and accept responsibility for managing the safety of each part of the railway. Your organisation should match resources and authorities to the safety responsibilities that each person has. For example, the authority to take a safety-related decision should be matched by the resources the person has available to implement the decision.

You should have contingency plans that make sure that safety continues to be managed when safety-critical staff and support staff are not available.

When you consider the safety of the part of the railway, you should make sure that someone is responsible for collecting up-to-date information about how it is built, how it is maintained, how safe and reliable it is, how it was designed and why it was designed that way, and for analysing this information for trends. This is to help those who are responsible for taking decisions about changing things to do it safely.

5.5 Related guidance

Competency and training requirements for the roles outlined in this chapter are dealt with in Chapter 7.

Communicating safety-related information is discussed in Chapter 9.

Safety Cases and Safety Approval are discussed in Chapter 18.

Hazard Logs and assumptions are discussed in Chapter 12.

The roles of the Independent Safety Auditors and Assessors and their responsibilities are described fully in Chapter 13.
Chapter 6

Organisational goals; Safety culture

**Fundamental from volume 1: Organisational goals**

Your organisation must have safety as a primary goal.

**Fundamental from volume 1: Safety culture**

Your organisation 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.

6.1 Guidance from volume 1

6.1.1 Organisational goals

The people leading your organisation should make it clear that safety is a primary goal, set targets for safety together with other goals and allocate the resources needed to meet them.

Your organisation will have other primary goals. The Yellow Book gives guidance only on managing safety. It does not give guidance on achieving other goals, but it recognises that it will be most efficient to consider all goals together.

6.1.2 Safety culture

The people leading your organisation should make sure that:

- staff understand the risks and keep up-to-date with the factors that affect safety;
- staff are prepared to report safety incidents and near misses (even when it is inconvenient or exposes their own mistakes) and management respond effectively;
- staff understand what is acceptable behaviour, are reprimanded for reckless or malicious acts and are encouraged to learn from mistakes;
- the organisation is adaptable enough to deal effectively with abnormal circumstances; and
- the organisation learns from past experiences and uses the lessons to improve safety.
6.2 General guidance

An organisation’s safety culture is its general approach and attitude towards safety.

In a good safety culture, safety always comes first, and this will be apparent in the work that the organisation produces. Safety is built into the organisation’s products, and its safety procedures support what is already being achieved.

A good safety culture may be achieved through a combination of sound safety policy set by management, awareness on everyone’s part of the importance of safety in all activities, and motivation to put safety policy into practice.

This chapter provides guidance on fostering 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 organisation may implement them.

There are certain legal obligations on employers, relating to their safety policy. See volume 1 for further details.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for directors and managers wishing to establish or improve the safety culture within their organisation.

6.2.1 Organisational goals

All organisations that do work that could affect safety should have safety as a primary goal. Your organisation should demonstrate a top-level commitment to deliver safety. It is good practice to provide organisational leadership by communicating your safety policy throughout your organisation and motivate your personnel to follow it in full.

You will have to identify what legislation applies to your organisation and set your goals to make sure you will comply. In the UK, to comply with the law, railway organisations need to address three areas when considering how they are to manage safety.

1. safety of passengers;
2. safety of personnel; and
3. safety of others affected by the work.

Your organisation should set targets to manage safety for all three and provide the necessary resources to meet those targets. To meet those targets, you will need to:

- understand how safe you are now;
- decide what your safety targets will be; and
- decide what work you need to do to meet your targets.

To achieve this, you will need to consider:

- how you are going to collect data about safety (see Chapter 16); and
- how you will plan and co-ordinate your work to ensure safety (see Chapter 11 and Chapter 9).

You should also have goals for reducing staff safety incidents and near misses (or near hits). The long-term aim should be a zero accident level and you should focus your safety policy on this.
When you have decided what your organisational goals are, you should consider whether you have the correct attributes (such as structure, management systems, tools, facilities, equipment, staff motivation and competence) to achieve them. If you do not, you should work out what goals you can achieve and decide whether that is enough to manage safety.

6.2.2 Safety culture

Your safety culture should be promoted throughout your organisation and led from the top, so that it is felt and observed throughout your organisation.

You should try to promote a culture with the following elements:

- ‘compliance’ with applicable standards and procedures;
- ‘right first time’;
- ‘not accepting poor standards of work’;
- ‘understanding’:
  - the overall risks that are being managed,
  - that risk is not constant and that new hazards need to be captured and managed as they arise,
  - what the organisation is supposed to achieve,
- ‘learning’ from incidents and near misses to improve the safety of work and overall safety of the railway;
- ‘sharing information’ so that your maintenance staff become the eyes and ears necessary to detect things that are wrong; and
- ‘action’ where something is found to be wrong.

You should recognise that there can be a tendency for safety culture to deteriorate, particularly where repetitive tasks can result in perceived familiarity and a false sense of security. It is essential to put measures in place that minimise the potential for complacency, such as varying people’s tasks and encouraging ownership.

6.2.3 The benefits of a safety culture

In an organisation 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 organisation’s products and services;
- potential hazards and failures are detected and eliminated or controlled early;
- the organisation’s products are safe and visibly so;
- the organisation realises efficiencies and cost savings; and
- the risk of not conforming to legal obligations is reduced.
A good safety culture will enhance an organisation'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 organisations that contribute to and rely on the industry's success.

James Reason, in his book ‘Managing the Risks of Organizational Accidents’ [F.7] provides a clear account of how safety culture contributes to risk and the elements of a good safety culture. This book is recommended for further reading on ESM.

### 6.2.4 Safety policy

The starting point for a good safety culture is a commitment on the part of management. This is best expressed by the setting of a safety policy, endorsed by the board of directors. A safety policy should state the organisation's aims for achieving safety.

The safety policy statements should define the fundamental approach to managing safety within the organisation. They should encompass both process and product safety issues. It is up to each individual organisation to define their own set of safety policy statements, according to the nature of their business. However, the safety policy statements should cover the following issues:

- confirmation that safety is a primary goal for the organisation;
- definition of management’s responsibility and accountability for safety performance;
- the responsibility of everyone in the organisation for ensuring safety;
- the provision of assurance that products meet safety requirements;
- the continual improvement in safety within the organisation;
- 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;
- pursuit of safety at all costs is not advisable; and
- judgement is required to know when to stop trying to reduce risk.

By defining the safety policy statements, ensuring that they are effectively implemented, and monitoring their effect on safety and on the organisation, it is possible to encourage and develop a good safety culture. Setting safety policy statements alone is not enough. Management should nurture and encourage good safety practices, monitor safety, and provide the necessary resources.

### 6.2.5 People's responsibilities within a safety culture

A Head of Safety is commonly appointed to take on the role of initiating, implementing, and maintaining an organisation's safety culture and its safety policy.
Everyone within an organisation, from the board of directors down, is responsible for understanding the importance of safety, following the safety policy, and incorporating it into their everyday activities.

Generally, managers remain accountable for ESM performance even though they may delegate responsibility for ESM activities.

Roles and responsibilities for specific activities within ESM are described in Chapter 5.

6.2.6 Putting safety policy into practice

The board of directors of an organisation should ensure that:

- there is management commitment to following the safety policy;
- everyone in the organisation is aware of the importance of following the safety policy;
- the necessary training and resources are provided;
- the way that the organisation performs ESM is monitored and improved;
- the safety of the organisation’s products is monitored and improved; and
- the organisation is regularly audited to assess its performance with regard to safety.

Awareness is a key factor in the successful implementation of safety policy. Everyone in the organisation should be aware of the importance of safety and of the organisation’s safety policy. The methods for achieving this will vary according to the size and type of the organisation. It may be possible with smaller organisations to provide direct briefing of the safety policy. With larger organisations, cascade briefing may be more practical.

Management should put in place procedures to implement the key components of safety policy. Resources for ensuring successful implementation of safety policy should be made available. This will include personnel with suitable background and training, as well as equipment.

Management should provide the opportunity and motivation to all staff to improve the safety of their work.

6.2.7 How to monitor safety policy

Management should check that the safety policy is being implemented. Typically, this will be done with a rolling programme, which ensures that every aspect of the policy is monitored over a period of a few years.

Typically, an aspect of the safety policy is monitored on a random selection from all the relevant activities of the organisation. 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 Chapter 13 may be used as a basis for such an audit.

Management should check that the findings of inspections and audits are acted upon.

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.
Management should provide an environment in which staff feel able to bring safety shortcomings to management attention without fear of recriminations.

6.2.8 Managing Human Factors

You should treat Human Factors with the same importance as any other part of Safety Engineering.

The railways rely on people to ensure that they operate safely. People make mistakes. Therefore human error is likely to contribute to risk; it may even be the major source of risk. Any organisation that professes to have a safety culture should treat human behaviour as an important issue.

Your organisation should treat human error with as much seriousness as any other aspect of safety, such as component reliability. You should put checks in place to ensure that this is the case.

6.3 Additional guidance for projects

There is no specific guidance for projects.

6.4 Additional guidance for maintenance

On the basis that the part of the railway that you are responsible for has been designed to be safe when there are no failures, a good maintenance organisation will have a goal to minimise the number of failures and the effect of failures that occur. It is good practice to set targets to reduce the number of failures that occur. It is also good practice to identify critical failures and set additional targets for these. You should set targets for responding to failures (such as time to repair) and make sure that you meet them.

6.5 Related guidance

Roles and responsibilities for specific activities within ESM are described in Chapter 5.

Guidance on co-ordination is provided in Chapter 9.

Guidance on safety auditing is provided in Chapter 13.

Guidance on safety planning is provided in Chapter 11.

Guidance on monitoring risk is provided in Chapter 16.
Chapter 7

Competence and training

Fundamental from volume 1: Competence and training

Your organisation must make sure that all staff who are responsible for activities which affect safety are competent to carry them out. It must give them enough resources and authority to carry out their responsibilities. It must monitor their performance.

7.1 Guidance from volume 1

The people leading your organisation should be competent to set and deliver safety responsibilities and objectives for the organisation.

Your organisation should set requirements for the competence of staff who are responsible for activities which 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. You should monitor the performance of staff who are responsible for activities which affect safety and check that they are in fact meeting these requirements.

7.2 General guidance

It is a requirement of good practice, and sometimes of the law, that all people who do safety-related work are competent and fit.

To be competent, you must have the necessary training, technical knowledge, skills, experience and qualifications to do a specific task properly. 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.

There are two primary obligations on you if you are assigning or accepting a safety-related task:

1. You should know your limitations and not go beyond them.
2. If you are assigning people to safety-related work, then you should ensure that they are competent for that work.

The first obligation is a requirement of the codes of practice of several professional institutions. For instance the British Computer Society Code of Conduct requires that members ‘shall only offer to do work or provide service which is within [their] professional competence’.
The second obligation is a legal duty in certain circumstances. See volume 1 for further details.

This chapter is concerned with the competence of individuals (Chapter 8 talks about suppliers). It provides some general guidance on the following aspects of assuring the competence of staff:

1. specifying requirements for staff competence;
2. assessing personnel;
3. training; and
4. monitoring.

Team competence should be considered, as well as individual competence. Your organisation should make sure that all personnel are competent to fulfil their safety responsibility and that all of the people can work effectively together to deliver safety. Remember that competent people still make mistakes. Assuring competence is not a substitute for having systems in place which can catch these mistakes before an accident occurs.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for:

- those responsible for assigning safety-related tasks to staff; and
- anyone otherwise assessing the competence of staff.

### 7.2.1 Specifying competence requirements

Chapter 5 described how to allocate and document the responsibilities for safety-related work. From these responsibilities, you should derive and document criteria for knowledge, skills, experience and qualifications that are necessary to carry out the work.

Consider setting requirements on:

- education (for instance, relevant degrees or attendance at specific courses);
- professional status (for instance, Chartered Engineer); and
- experience (for instance, three years involvement in safety or quality auditing).

However, do not restrict yourselves to requirements, like those above, which are easily assessed, but try and set criteria for the minimum fundamental skills and knowledge that are required to perform the task.

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.

### 7.2.2 Assessing competence

Competence management should start by selecting people who have the basic abilities to do the job. These people should continue to be developed through their careers using training, mentoring and workplace experience. When considering whether a person is competent, you should consider:

- technical skills, knowledge and experience;
• leadership and managerial skills;
• attitude and integrity;
• fitness; and
• confidence.

Before someone is assigned a safety-related task, they should be assessed to decide whether or not they meet the criteria set for that task. This initial assessment should be documented and kept, along with any supporting evidence. This evidence may be required for the following reasons:

• as part of a Safety Case;
• for an independent Safety Assessment; or
• in investigating an incident.

The assessment is usually done by the individual’s manager or a third person, but it is usually most effective to work with the individual.

Assessment of education, experience and professional status can be checked by direct reference to CVs, 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 fulfil 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 fulfil the requirements. The mentor should be accessible to the person being supervised and should take overall responsibility for the work.

All of this guidance applies as much to individual contract personnel as to employees (although the selection of suppliers to take on specified tasks is covered in Chapter 8).

Pre-employment screening is a good way of filtering potential candidates for a safety position. You will need to fully understand the job profile and health requirements and then screen people for pre-existing conditions as part of the selection process.

It is good practice to assess people by observing them doing the required work, either at the workplace or by setting simulated exercises. Newly-qualified staff may require extra supervision and coaching.

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, the applicable standards and finally be able to use their judgement 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 organisations such as the Institution of Railway Signal Engineers (IRSE).
Your organisation 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. You should make sure that their competence continues to match the requirements of their job.

Your organisation 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.

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.

### 7.2.3 Developing competence

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 (such as those provided by the Open University), computer-based training and on-the-job coaching from senior staff.

Several professional organisations (including the Institution of Engineering and Technology (IET), the Institution of Mechanical Engineers (IMechE) and the British Computer Society (BCS)) provide continuing professional development schemes which can help in selecting appropriate training. Professional engineers 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 logbook 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 organisation 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.

### 7.2.4 Monitoring

It is not sufficient just to specify and check competence once. Your organisation should continue to check that staff who are responsible for activities which affect safety have the competence and resources that they need periodically, as a matter of routine.
Most organisations 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.

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.

**7.2.5 Transitional arrangements**

When introducing a more formal approach to assessing competence, it may be found that the most experienced and capable personnel have not been through the training programme 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.

A proven track record in a job is the most direct evidence of competence. It is normal under these circumstances to write some transitional arrangements into the training criteria, which exempt some existing staff from the formal criteria for their current job. However, it is necessary to show not just that the individuals have held the post for a period of time, but also that their performance has been satisfactory during that period.

**7.2.6 Review and audit**

Management 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.

**7.2.7 Resources and authority**

People who are authorised to do work should also be given responsibilities for putting things 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.

**7.2.8 Managing Human Factors**

Staff carrying out Human Factors work should be competent to do so. Without competent staff, the results of Human Factors work may be unreliable. The competence required will depend upon the project. It is not necessary that all work that involves Human Factors should be carried out by trained ergonomists; for example signal sighting is all about Human Factors but is correctly performed by teams comprising signal engineers, drivers and specialists in signal sighting. The skills and competency level should be relevant to the work to be carried out.

You may find it useful to refer to some of the societies and organisations that are involved in Human Factors work, such as the Ergonomics Society of Great Britain, the British Psychological Society and the Human Factors and Ergonomics Society, for assistance on assessing the competence of staff involved in Human Factors work through professional accreditation schemes.
7.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

7.4 Additional guidance for maintenance

Competence in a maintenance organisation can be categorised in two areas:

- competence and fitness to do the required maintenance work; and
- competence to change the way maintenance is done.

7.4.1 People who do maintenance work

Your maintenance personnel should be competent and fit to do maintenance work, in accordance with the required standard and in the environment that the work is to be done. When deciding who will be responsible for doing maintenance work (such as a team leader), it is good practice to take into account a person’s ability to work under pressure, particularly where they will be expected to respond to incidents or failures that affect train running.

For personnel who do maintenance work, the scope and methods of assessment should consider:

- the maintenance processes that need to be followed;
- the systems, components and equipment that they need to work with;
- the underpinning knowledge needed to take decisions;
- the attitude and experience of the person being assessed;
- the required working environment (including situations that they may face); and
- the activities that they are required to do, including use of tools, materials and test equipment.

It is good practice to make sure that the overall capability of your maintenance teams includes the right balance of technical abilities and leadership qualities, and that team members understand and can use the information and resources they need.

The number and location of your personnel should take into account the need to respond to unforeseen events and the location of the assets that they are responsible for.

7.4.2 Competence of people who take decisions about what maintenance to do

In order to effectively manage safety, your organisation will require certain people to use their judgement to take safety decisions. These people should be competent and be located within your organisational structure so that the safety decisions can be effectively implemented.

7.5 Related guidance

Chapter 5 provides guidance on defining responsibilities.

Chapter 8 provides guidance on selecting contract organisations to carry out safety-related work.
Chapter 8

Working with suppliers

Fundamental from volume 1: Working with suppliers

Whenever your organisation contracts out the performance of activities that affect safety, it must make sure that the supplier is competent to do the work and can put these fundamentals (including this one) into practice. It must check that they do put them into practice effectively.

8.1 Guidance from volume 1

A supplier is anyone who supplies your organisation with goods or services. You can share safety responsibilities with your suppliers but you can never transfer them completely. The safety responsibilities fundamental means that you must be clear about what safety responsibilities you are sharing.

The working with suppliers fundamental is needed to make sure that the other fundamentals do not get lost in contractual relationships.

Your organisation should set specific requirements from these fundamentals, which are relevant to the work being done, before passing the requirements on to the supplier. You also need to check that your suppliers are competent to pass requirements to their suppliers.

8.2 General guidance

This chapter is concerned with the situation where safety-related tasks are contracted out to another organisation. It is not concerned with contract personnel who work under your organisation’s supervision (Chapter 7 is relevant to that case).

Contracting out a safety-related task does not relieve your organisation of all responsibilities for that task. It is your responsibility to make sure that the supplier is competent to do the work. This responsibility is a legal duty in some circumstances. See volume 1 for further details.

The contractor should also be required to adopt good ESM practice and they should be monitored to ensure that they do.

Your organisation should also inform the supplier about hazards, risks and safety requirements which are relevant to their work. This obligation is considered further in Chapter 9.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for:

- anyone who is considering contracting other organisations to perform safety-related work.
8.2.1 Selecting suppliers

Most organisations 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 labourers; and
- services, for example outsourced repairs and specialist investigation.

Where safety could be affected, it is good practice to assess your potential suppliers and the resources you obtain before you use them. This is so that you can understand the limits of their capabilities.

You should work with your suppliers to improve safety and deal with any gaps between the competence that is needed for the work and the competence that they can bring to it. You may do this using your own resources, by bringing in additional outsourced resources or, if necessary, by stopping the work.

You should work out whether you need to do anything else to improve safety, such as establishing appropriate controls to monitor safety, such as sample checks, product inspection, supervision and audit.

8.2.2 Assessing suppliers

A supplier assessment should be proportionate and appropriate 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 organisation with competent personnel;
- the necessary equipment which is properly maintained;
- a suitable health and safety policy appropriate to the work;
- an ability and commitment to undertake suitable and sufficient risk assessments;
- effective arrangements to control the risks identified;
- 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;
- details of their accident and incident records;
- training records;
- CVs for the staff who will be performing the work;
- QA procedures;
- project review and monitoring documents;
• details of previous experience; and
• references from other customers.

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 safety performance of suppliers should be recorded and taken into account if the supplier bids for further safety-related work.

8.2.3 Specifying and monitoring work

You should produce written specifications of all safety-related work to be done by suppliers and check that the suppliers meet these specifications.

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 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 fulfil 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 properly handled, maintained and calibrated to meet your safety requirements. Similarly, you should make sure that supplied personnel fulfil 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.

Your organisation should agree methods of communication and procedures with suppliers to make sure that your requirements are both properly specified and understood.

You should monitor the safety and quality of work done by suppliers and implement the necessary measures where uncontrolled risk is found. One way of doing this is by carrying out regular audits (see Chapter 13). 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. Sometimes, this will be required by a standard.
For simple requirements it may be sufficient to directly inspect the work being done or the deliverables being produced. 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 organisation, 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.

You should check that the supplier acts on the findings of any inspection or audit.

8.2.4 Managing Human Factors

When several organisations are working together, they should agree how the Human Factors work will be shared between themselves, and ensure that they all understand their responsibilities. You should ensure that all agreements are clear and unambiguous about Human Factors work to be carried out.

Where you need your suppliers to do Human Factors work, you should ensure that contracts with suppliers are clear about what is expected and what will be delivered.

8.2.5 Supply of products

If you can establish that a product is safe by inspection of the product itself, it may not be necessary to assess the supplier. However, unless you have confidence in their processes you should continually inspect their product to check that the quality is maintained over time.

The thoroughness with which you inspect products or assess their suppliers will depend upon the potential for the product to contribute to a hazard.

8.2.6 Supply of services

Some railway organisations rely on suppliers to provide some of the support services needed to carry out their work. For example, your organisation may hire a complete team of staff to provide signalling support in connection with track renewal work. You may ask a supplier to do the work, but check the integrity of the work yourself, before the railway is returned to operational use.

In another circumstance, you may use a supplier to repair and return railway components that are worn out or broken. In this case, it is good practice to agree a repair specification, including the testing specification that will satisfy the safety requirements for re-using the component.

Where responsibility for work is to be shared with a supplier, you should agree your plans with them (see Chapter 11). 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.

8.2.7 Supply of individual staff
If supplier personnel are to be used to make up staff shortages within your own work teams, it is good practice to include the subcontract personnel within your own Safety Management System, including competence management and shift management. See Chapter 7 for guidance on managing the competence of individuals.

8.3 Additional guidance for projects
There is no specific guidance for projects.

8.4 Additional guidance for maintenance
There is no specific guidance for maintenance.

8.5 Related guidance
Chapter 7 provides guidance on assessing the competence of contract personnel who work under your supervision.
Chapter 9 provides guidance on communicating safety-related information to suppliers.
Chapter 11 provides guidance on safety planning.
Chapter 13 provides guidance on safety auditing.
Chapter 9

Communicating safety-related information; Co-ordination

Fundamental from volume 1: Communicating safety-related information

If someone tells you or your organisation something that suggests that risk is too high, you must take prompt and effective action. If you have information that someone else needs to control risk, you must pass it on to them and take reasonable steps to make sure that they understand it.

Fundamental from volume 1: Co-ordination

Whenever your organisation is working with others on activities that affect the railway they must co-ordinate their safety management activities.

9.1 Guidance from volume 1

9.1.1 Communicating safety-related information

This information may include:

- information about the current state of the railway;
- information about how systems are used in practice;
- 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 which are important to safety.

Communications within an organisation should be two-way. In particular, the people leading your organisation 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.

Your organisation should pass on any relevant information about hazards and safety requirements to its suppliers.
9.1.2 Co-ordination

There are specific legal obligations in this area. In the UK these include regulation 11 of the *Management of Health and Safety at Work Regulations 1999* and the *Construction (Design and Management) Regulations 1994*.

9.2 General guidance

Safety issues do not respect organisational boundaries. Effective communications and co-ordination are often needed to resolve them.

There is a legal duty on those involved in the UK mainline railway to co-operate in the interests of safety. For example, Group Standard GE/RT8250, ‘Safety Performance Monitoring and Defect Reporting of Rail Vehicles and Plant and Machinery’ [F.8] requires some Railway Group members to share details of safety-related defects with other members of the Railway Group.

The sources of information needed to take safety decisions may exist anywhere within your organisation, such as a report from a maintenance technician at the front line. Alternatively, information may come in to your organisation at any point from somewhere else, such as a Transport Operator, or from the general public.

Where information about safety risk could have wider implications, your organisation should have communication systems in place that allow you to pass the information to someone who has the authority to decide what action to take. This may require communication with other organisations 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, including those that are looked after by other maintenance organisations.

Decisions taken by management need to be communicated to those at the front line who have to implement the decision. You should communicate information throughout your organisation to make sure that your standards and procedures are properly implemented, particularly when work requirements change.

Decisions taken at the front line need to be communicated to management, for example, a decision to allow degraded equipment to temporarily remain in service until a replacement can be planned.

When you communicate safety information, 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.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

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.
9.2.1 What to communicate

Your organisation 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 organisation makes and any implications for users and maintainers;
- 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 assessments 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.

Your organisation should put in place arrangements to capture and record this sort of information, to decide who should receive it, and to make sure that they do receive it.

9.2.2 Communication within your organisation

Good communication is essential if you are to manage safety properly. Your organisation should have methods to communicate up-to-date information about safety of the railway to all those who need to know, at the time and place that they need it. You should have good communication systems so that information can be passed throughout your organisation. This will help the correct people to take the correct safety decisions and understand their safety responsibility (see Chapter 5).

You should make sure that everyone in your organisation knows who to tell if they find information that there is an unacceptable safety risk.

When you communicate information, you should make sure that the information has been correctly received and is understood by the recipient.

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 Case, 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.
9.2.3 Communication between organisations

Initially it is usually a good idea to pass information 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.

Considerations of commercial confidence and the expense of providing certain classes of information can make passing necessary information 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.

9.2.4 Communication systems

It is essential to establish communication systems that are capable of use in normal, degraded and emergency situations. In all cases, your organisation should have a system to record the safety information that you need to communicate (see Chapter 12 Records). This will help you to communicate the information safely and accurately to those who need to use it.

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.

The types of communication system you use should be appropriate to meet the needs of the user and the type of information to be communicated.

It is good practice for organisations to co-ordinate the flow of safety-related and time-critical information using a dedicated reporting facility (examples range from a maintenance control centre 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 prioritise 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.

When you choose a method of communication, you should consider the need to maintain a record of the communication. You should identify and select best practice where it exists within the railway industry. Some of these best practices are mandated by railway standards (such as use of the phonetic alphabet). Sometimes, it is good practice to implement anonymous or independent reporting facilities, such as CIRAS (Confidential Incident Reporting and Analysis System), particularly in order to capture information about personnel safety incidents; however you should make sure that these are only used where appropriate.
9.2.5 Written communication

Good written communications use clear language and graphics to communicate information in a consistent way. Written communication is particularly effective where consistency is required, including:

- 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 (see Chapter 10). You should make sure that the document hierarchy is clearly understood and that front line specifications and organisational policy documents are consistent with each other.

9.2.6 Spoken communication

Good spoken communication also relies on use of 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 statements.

It is good practice for message recipients to repeat spoken messages back to the sender to confirm their understanding. This is particularly important where face-to-face communication is not possible.

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 becoming future accidents.

9.2.7 Information Technology (IT) and data systems

If your company has Internet capability, mobile telecommunication and email facilities, these 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.

IT systems provide an alternative way of communicating a written message and so clarity of language is essential.

Because this method of communication is largely one way at a time, you should have procedures that require recipients to acknowledge receipt.

Your organisation should have a fall-back method to maintain communication in the event of an IT failure.

9.2.8 Co-ordinating under normal conditions

Cross-organisation working groups with a focus on safety are commonly set up in rail. They are also common in other sectors, for example in military projects (see DEF-STAN 00-56 [F.9] and MIL-STD 882C [F.10]).
Communicating safety-related information; Co-ordination

If several organisations are involved in some work, then they should set up such a working group and 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.

All co-ordination arrangements should be put in writing so that they can be audited.

Your organisation should co-operate to develop procedures and a co-ordinated work plan so that safety is not affected by the work.

9.2.9 Co-ordinating under emergency conditions

If your organisation potentially has to deal with an accident or emergency, then it should have contingency plans in place to co-ordinate responses with others to do this:

- Your organisation 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 organisation should have agreed arrangements in place for dealing with emergency services and for communicating with the general public and the media.
- Your organisation may wish to set up joint exercises with the people you will have to deal with, if there is the realistic possibility that you may have to deal with a catastrophic incident.

It is good practice that emergency plans are established appropriate to the nature of the undertakings and activities of the business. These arrangements should be sufficient to control additional risk introduced as a result of an emergency, and should be considered and 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.

Specified in company Safety Management Systems or as part of Contract Health and Safety Plans or Safety Cases, these arrangements are normally developed for incidents that may occur at buildings, offices and depots, for semi-portable locations and transient worksites and will be managed as part of the formally documented management system, reviewed regularly and updated as necessary when changes to arrangements and new risks are identified.
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;
- 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.

**Communications** will be a major consideration within emergency plans and should include arrangements for key personnel to communicate with each other and to 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 organisation and the emergency services and/or local councils etc. Interfaces with these agencies and mobilising arrangements should be described and understood by those involved. Control centres may be required from which to operate, 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 organisation 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.

### 9.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

### 9.4 Additional guidance for maintenance

Co-ordination is particularly important where your work includes maintenance at boundaries. Your organisation should co-operate with other organisations to agree and set down the arrangements for co-ordinating all of the work safely.
For example, another organisation that maintains a telecommunication infrastructure may need to disconnect a part of it for testing. The continued operation and integrity of the safety-related data carried by the data channels is the responsibility of your organisation. You should both co-ordinate the work by agreeing what needs to be done and planning together how it will be done safely. Both organisations will have to agree timescales, responsibilities for parts of the work and what information needs to be exchanged.

Similarly, train maintenance is usually managed within the controlled environment of a depot; however, where emergency maintenance or repairs are required at the trackside, you should make sure that you co-ordinate with the other parts of the railway, particularly Transport Operators.

9.5 Related guidance

Chapter 5 provides guidance on the transfer of responsibilities. There are requirements for making sure that whoever takes on responsibility is properly informed.

Chapter 12 provides guidance on configuration management.
Chapter 10
Continuing safety management

Fundamental from volume 1: Continuing safety management

If your organisation’s activities and responsibilities affect safety and it is not yet putting all these fundamentals into practice, it must start as soon as it reasonably can. It must continue to put them into practice as long as its activities and responsibilities affect safety.

10.1 Guidance from volume 1

The earlier you start to manage safety, the easier and cheaper it will be to build safety in and the sooner you will see the benefits in reduced risk.

Things never stay exactly the same. Just because you successfully controlled risk to an acceptable level in the past does not mean that you can assume that it will stay acceptable. You need to be alert to change and react to it as long as you are responsible for the safety of part of the railway.

This fundamental is related to the monitoring risk fundamental below.

10.2 General guidance

It is always more effective to build safety in than to try to retrofit it later. Decisions on the form and structure of systems start to be taken at the beginning of projects, and safety analysis should therefore start at the beginning so that safety considerations can influence the earliest decisions.

If you are not yet putting all of the Yellow Book safety fundamentals into practice, you should start as soon as you can. Once you have started to put the fundamentals into practice, you should continue to do so for as long as you are responsible for safety aspects of the railway.

Many railways are already involved with day-to-day Engineering Safety Management. Your organisation may already be using good practices in all or part of your work. If your safety culture is correct, you will already be looking for ways of improving safety further and monitoring changing risk by putting these fundamentals into practice.

It is good practice for project organisations to work closely with maintenance organisations when changes to the railway are to be introduced. Maintainers should ensure that they become involved in the project Engineering Safety Management process from beginning to end. This is so that safety is managed during stage-works and, as the project approaches its conclusion, a seamless handover of safety responsibility from the project to the maintainer can be achieved without introducing additional risk.
After the asset has been taken into use and operational experience is gained, you should challenge any assumptions made about safety, particularly where a recommended maintenance regime has been developed using predictive failure and hazard analysis. You should continue to collect and use operational data to develop a fully justified maintenance regime (see Chapter 16).

Other ESM activities also need to be performed during these phases. This chapter provides guidance on what should be done and when.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for anyone involved in starting up a project and planning the later stages.

See also Chapter 11, which provides guidance on safety planning.

### 10.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

### 10.4 Additional guidance for maintenance

There is no specific guidance for maintenance.

### 10.5 Related guidance

A generic System Lifecycle is presented in Chapter 2.

Guidance on writing a Safety Plan is provided in Chapter 11.

Guidance on configuration management and maintaining a Hazard Log is provided in Chapter 12.

Guidance on monitoring risk is provided in Chapter 16.

Guidance on establishing a Data Reporting, Analysis and Corrective Action System is provided in appendix E.
Part 3

Process Fundamentals
Chapter 11

Safety planning; Systematic processes and good practice

Fundamental from volume 1: Safety planning
Your organisation must plan all safety management activities before carrying them out.

Fundamental from volume 1: Systematic processes and good practice
Your organisation must carry out activities which affect safety by following systematic processes which use recognised good practice. It must write down the processes beforehand and review them regularly.

11.1 Guidance from volume 1
11.1.1 Safety planning
Your plans should be enough to put the fundamentals into practice. 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 may cover everything 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.

You may have plans at different levels of detail. You may, for example, have a strategic plan for your organisation which starts with an analysis of the current situation and sets out a programme of activities to achieve your objectives for safety. You may then plan detailed safety management activities for individual tasks and projects.

You may include safety management activities in plans that are also designed to achieve other objectives. For example, safety management activities should normally be taken into account as part of the planning process for maintenance activity. 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 should adjust the extent of your plans and the safety management 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.
Your organisation should use good systems engineering practice to develop and maintain safety-related systems.

Engineering needs a safety culture as much as any other activity. It is true that safety depends on the people who do the work, but it also depends on the way they do their work and the tools they use. The people leading your organisation should be aware of good practice and encourage staff to adopt it.

When choosing methods, you should take account of relevant standards. You should check that a standard 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.

11.2 General guidance

These two fundamentals complement each other and so we discuss them together.

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 components of a good plan:

1. 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.

2. how: describes the method, often referring to a specification.

3. where: describes the locations that the work will take place.

4. 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.

5. who: allocates tasks to individuals and names the people responsible for doing and checking the work.

6. with: describes the resources to be used (tools, materials, plant, supplier resources etc).

7. 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.

All of your plans should be co-ordinated (See Chapter 9). See Chapter 9 also for guidance on planning for emergencies.

What constitutes good practice is relative and depends on:

- 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.

The guidance in this chapter is applicable to all phases in the System Lifecycle.
This chapter is written for:

- anyone responsible for planning ESM activities;
- anyone who will need to endorse plans for ESM activities; and
- anyone involved in performing, auditing or assessing ESM activities.

### 11.2.1 Adapting this guidance

Some of the project guidance in this chapter is designed for a situation where:

- risk cannot be controlled completely by applying standards; and
- you are compiling evidence of safety into a Safety Case.

If the risk comes completely within accepted standards that define agreed ways of controlling it (see section 2.4.3) or if your Safety Approvers require evidence of safety presented in a different way, then you will need to adapt the guidance to suit your situation.

If the work you are doing comes completely within your organisation’s Safety Management System, then the provisions of this Safety Management System may put the fundamental into practice.

### 11.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

### 11.4 Additional guidance for maintenance

The way you decide to plan your work will influence the way you set up your organisation (see Chapter 5).

Before you plan your work, you should look ahead, decide what your goals are, understand where you are now and decide what work you need to do to get where you want to be (see Chapter 6).

Your planning is key to making sure that railway assets are managed in a way that ensures continued safety and performance. If you are planning to make a significant change, you should refer to the project guidance in this chapter; however, your maintenance planning should allow for the possibility of significant changes, for example an ability to respond to an imminent environmental effect.

Safety planning should occur at all levels of your maintenance organisation to manage safety and performance properly. Planning is all about deciding how you are going to do your work in the context of the other parts of the railway that will be affected, including other maintenance organisations and Transport Operators, so that you can do the work safely.

Your maintenance plans should make sure that standby and protection systems are fit for service, as well as operational systems. This will make sure that risk mitigations that are designed into system architectures (such as system multiplication, diversity and protection) remain effective.
Whilst the failure of a component may not cause an accident in itself (‘fail-safe’ components have safety designed into their failure modes), the overall level of risk on the railway increases when trains are running during degraded operating conditions. For example, the risk associated with hand-signalling is greater than normal operations using lineside signals. Therefore, a maintenance regime should be planned to minimise the occurrence of failures.

Your maintenance plans should identify areas where you depend on others to do your work and where others depend on you.

Figure 11-1 Typical examples of maintenance plans with a safety component

11.4.1 Top-level safety planning

Your organisation should first develop a top-level plan that describes how it will fulfil its organisational goals and comply with legislation (see Chapter 6). To deliver its top-level plan, your organisation should develop plans for all of the work that you do.
Before you can effectively plan for safety and performance, you should understand how well you are doing now and then decide what your new targets will be. You should plan to collect information about safety and performance and select types and sources of information that help you to develop new targets for parts of the railway, personnel, passengers and neighbours. You should plan:

1. **what** information you are going to collect to understand the risks you are responsible for controlling;
2. **how** you are going to collect and report it;
3. **where** you are going to collect it from;
4. **when** you are going to collect it and how often you will collect it;
5. **who** will be responsible for collecting it, who will review it and who will decide whether something needs to be changed;
6. **with**: what mechanism you are going to use to collect and record the information;
7. **why**: understand what the objective is for collecting the information.

When collecting information, you should understand how accurate it is and how representative it is of the situation you are investigating. The output from this level of planning may result in changes to the way you already do your work and stimulate organisational changes.

It is good practice to review your safety and performance targets on a regular basis (such as once a year), to decide whether you need to change them. You should also review the way you plan safety and performance after an incident and whenever a significant change takes place that could affect the work that you are responsible for.

It is important to communicate your top-level Safety Plans so that people understand what they have to do. It is good practice for organisations to publish a yearly strategic plan that lists all of the safety and performance targets and identifies who is responsible for achieving each target.

### 11.4.2 Organisational level maintenance strategy

At an organisational level, you should plan how you are going to do your work to meet the safety and performance targets that you have set. You should also plan to monitor the progress of your work against your plans and key performance indicators.

Using the information that you have collected, you should plan how you are going to develop the control measures that your maintenance work will implement (see Chapter 17).

The output of this planning level will be your organisation maintenance strategy, which should describe how you are going to control the risks that you have identified. Typically, your maintenance strategy could be made up of maintenance specifications and method statements. You should also have a strategy to deal with unforeseen circumstances, including safety incidents (see Chapter 9).
11.4.3 Maintenance specifications

Your maintenance specifications should describe the maintenance work that needs to be done to each asset type and the periodicity with which it should be applied. You should take account of the assumptions made in Safety Cases and manufacturers’ documents. The level of detail that you prescribe will depend on the competence of the personnel who are going to do the work, the benefits that consistency will bring to controlling risk and the auditable records that you need to keep.

Your specifications should include information about safety tolerances.

You may have to supplement your maintenance specifications with other safety information to control risks in particular circumstances (such as references to rules and procedures necessary to manage the safety of railway operations).

Where access constraints mean that limited time is available to maintain particular assets, it is good practice to identify priority tasks such as safety-critical tests, so that they will be completed first. Any uncompleted work will therefore be less urgent and may be easier to re-schedule.

Maintenance specifications are often communicated in the format of equipment manuals, suitable for frequent use at the workplace. Where it is not appropriate to prescribe the way work is done, you should look for, and publish, good practice (for example using codes of practice documents or checklists to ensure consistency of failure investigation).

11.4.4 Method statements (work instructions)

You should supplement your maintenance specifications with method statements that describe how the work will be done, the resources that you are going to use, staff competence and the measures that are necessary to ensure safety at the interfaces (that is with other work activities, the rest of the railway, passengers and neighbours).

A good method statement is concise, clearly written and has a level of detail that reflects the competence and experience of the people that will use it. When read, a good method statement will briefly describe generic requirements and draw attention to any unusual or uncommon risks that apply in a particular situation (for example confined spaces, electrical hazards and unusual train movements).

You should communicate your method statements to personnel who do maintenance work in a way that meets their needs (see Chapter 9). Up-to-date method statements should be available for reference at the workplace and it is good practice to use a standard structure and template so that personnel know where to find information.

11.4.5 Planning to collect information

It is important to plan how you are going to collect safety and performance information so that you can decide whether your work is doing enough to control risk, and plan to change the way you specify and programme your maintenance work. This information should include achievement of the work you planned to do and effectiveness of the work in controlling the risk. Many maintenance organisations have developed procedures that require maintainers to record critical information about an asset before and after it has been maintained, for example adjustments, replenishments, repairs and replacements, degradation and any exceptional items found.
Safety planning; Systematic processes and good practice

Chapter 11

11.4.6 Detailed maintenance programmes

At a detailed level, you should develop a maintenance programme that makes sure that your maintenance strategy can be implemented effectively. A good maintenance programme will clearly identify when each asset is to be maintained and what needs to be done. It is good practice to include some flexibility to allow time for additional work and failure response, whilst not exceeding maximum maintenance periodicities.

Where your maintenance programmes could conflict with each other, you should coordinate your work to ensure that they are all fulfilled (see Chapter 9).

It is good practice, where possible, to allocate your personnel to a wide range of tasks so that they develop and retain a broad range of competence and an ability to work with a variety of asset types.

Good maintenance organisations frequently review and update their maintenance programmes so that they reflect the status of work. If your planned work cannot be completed on time, you should adjust and re-issue your maintenance programmes to reallocate your resources to tasks with a high priority.

11.4.7 Planning process

You should make it clear what planning responsibilities people have for all levels and types of plans and give them the planning resources they need. It is good practice to give responsibility for planning to the people who have responsibility for implementing your plans. For example, a track engineer should develop a strategic plan for track maintenance, depot engineers should then develop plans to implement it at specific locations, supervisors should plan how the work will be done and so on, down to team leaders who should plan the tools and equipment required to do each job.

To be able to plan properly, your planners should be competent, understand the maintenance work that needs to be done and have information about the constraints that could affect the way it is done. You should make sure that planners have information about the railway and other work that could impact on maintenance work delivery. It is good practice to develop a planning procedure to provide consistency in process and output.

You should communicate your plans so that people understand what maintenance work they have to do. It is good practice to manage your maintenance programmes using an IT system, which will allow individual jobs to be related to work teams (for instance work orders) and enable maintenance reports to be entered to monitor progress of work against the programme. The information contained on the work orders should meet the needs of those who have to do the work in the environment in which it will be used.

You should decide how you are going to manage changes to your plans to reflect changes to the railway and changing work priorities. This is particularly important where maintenance work may be delayed due to unforeseen circumstances, and missed work needs to be re-prioritised and re-planned.

Whenever you change your plans, you should re-issue them and communicate the changes to all those who need to know.
11.4.8 Plans for supervision and inspection of work done

Having decided your maintenance programme, it is good practice to make sure that the work is properly implemented and the results are effective at controlling the risks that you have identified. You should plan to check that safety of the railway, safety of personnel and safety of passengers and neighbours is being properly addressed by the maintenance work.

There are two ways of going about this and you should plan how you are going to address each:

1. supervision of personnel doing work; and
2. inspection of work done.

You should make sure that the way you plan supervision and equipment inspection promotes a ‘right first time’ philosophy amongst the people doing maintenance work and avoids a culture of ‘correction through inspection’.

When you have decided how you are going to check the safety of your maintenance work, you should build the capability into your organisation.

If you find a problem, you should record it and tell those who need to put it right. If safety could be affected elsewhere, you should tell others about it so that risk can be reduced.

**Supervision** involves observation of work whilst it is being done and is focussed on safety of personnel, passengers and neighbours by checking compliance with and the robustness of method statements. It also checks that the work is being done in accordance with the maintenance specification and work orders. You should plan your supervision to make sure that the full range of personnel (including contracted staff) are observed working within their range of tasks over a certain period of time (for instance visit each maintenance team carrying out a range of tasks during each year).

The extent and frequency of supervision should reflect the experience of your personnel and the risk associated with different types of work. It is usually appropriate to closely supervise new or inexperienced personnel at first, where they are faced with new activities and work environments. It is good practice to retain some flexibility in your plan so that supervision can be timed to coincide with significant work activities. Significant activities include working in locations with higher risk (for instance on open running lines or in the vicinity of hazardous equipment) and activities with higher safety consequences (for instance, maintenance of facing points or train braking systems).

**Inspection of work done** involves sample equipment inspections after maintenance to establish whether the maintenance work is adequately managing risk (for instance preventing system deterioration). You should plan your equipment inspections to make sure that asset populations are sampled to take into account a range of locations, ages, conditions and usage. Assets that have a higher safety risk attached to them should be given a higher priority. It is good practice to visit equipment at different times in the maintenance cycle to understand the full effect of your maintenance. For example, by visiting an asset just before a maintenance visit is due, it is possible to gather information about the robustness of the maintenance specification, the quality of the maintenance done last time and the appropriate periodicity of visits.
11.4.9 Good maintenance practices

Your maintenance organisation should seek out and use good maintenance practices. This may include following good practice maintenance specifications published by the railway industry, which set out what maintenance should be done, when and how it should be done and in what circumstances it should be done. It also includes following good practice in the way maintenance is planned, communicated and implemented for personnel safety.

Good practice may involve the use of new technologies, such as vehicle-mounted video inspection techniques and ultrasonic flaw detection. If you do choose to use a new technology, you should consider all of the hazards that the method introduces, as well as the existing hazards that it mitigates. Good practice may also involve the way you manage your work, such as restricting on-track maintenance work to periods when the railway is closed to traffic.

If you find a new good practice that improves safety, or you decide that an existing practice is not good enough to manage safety, you should change what you do and tell others about it.

Where you are implementing good practice, you should check that you are using it consistently and everywhere that you can. You should set down how you are going to implement the good practice so that you can communicate it to those who need to know. You should continue to review the way you maintain the railway to make sure that it is still good practice and that changes to parts of the railway have not reduced safety.

Whenever you decide to change the way you maintain a part of the railway, you should make sure that what you are going to do will comply with railway standards and legislation.

You should not change the way you do things if it could reduce safety. Consistent application of an existing good practice is preferable to frequent changes, which may introduce a safety risk.

11.5 Related guidance

Chapter 3 provides guidance on the System Lifecycle.

Chapter 5 provides further guidance on safety roles and responsibilities.

Chapter 6 discusses organisation goals and safety culture.

Chapter 8 provides guidance on discharging safety responsibilities through suppliers.

Chapter 9 provides guidance on planning for emergencies and co-ordination under normal and emergency conditions.

Chapter 12 provides guidance on safety documentation.

Chapter 13 deals with the independent professional review of the Safety Plan.

Guidance on performing the safety analysis activities described by the Safety Plan is provided in Chapter 14 and Chapter 15.

Chapter 17 provides guidance on Safety Integrity Levels.

Chapter 18 provides guidance on making a safety argument for software which has already been developed.
Chapter 12

Configuration management; Records

Fundamental from volume 1: Configuration management

Your organisation must have configuration management arrangements that cover everything which is needed to achieve safety or to demonstrate it.

Fundamental from volume 1: Records

Your organisation must keep full and auditable records of all activities which affect safety.

12.1 Guidance from volume 1

12.1.1 Configuration management

Your organisation should keep track of changes to everything which 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 they should let you:

- uniquely identify each version of each item;
- record the history and status of each version of each item;
- record the parts of each item (if it has any);
- record the relationships between the items; and
- define precisely actual and proposed changes to items.

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.

If you are maintaining part of the railway, your configuration management arrangements should cover that part of the railway and the information that you need to maintain it.
Your plans should be enough to put the fundamentals into practice. If there is a possibility that you may become involved in an emergency on the railway, you should have plans to deal with it.

12.1.2 Records

Your organisation should keep records to support any conclusion that risk has been controlled to an acceptable level. You should also keep records which 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 safety management activities. These records may include (but are not limited to):

- the results of design activity;
- safety analyses;
- tests;
- review records;
- records of near misses, incidents and accidents;
- maintenance and renewal records; and
- records of decisions that affect safety.

You should also create a Hazard Log which records the hazards identified and describes the action to remove them or control risk to an acceptable level and keep it up-to-date.

The number and type of records that you keep will depend on the extent of the risk.

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 fulfil your contract or meet standards.

12.2 General guidance

A convincing demonstration of safety rests on good housekeeping.

A configuration is a group of related things and the relationships between them, and configuration management is about keeping track of these things and their relationships.

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.

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.

This chapter describes how to identify items whose configuration should be recorded and kept under control. It explains why configuration management should be applied to safety-related system items and documents and how it may be monitored.

There are three main reasons for keeping records of safety-related activities:

1. to show others that you have reduced risk to an acceptable level;
2 to explain to people making future changes why decisions were taken, so that they do not undo the work that you have done; and
3 to support the handover of safety responsibilities to other people.

The two fundamentals 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.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

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.

12.2.1 Configuration management tools

Configuration management requires a means of storing and controlling 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.

12.2.2 Software configuration management

12.2.2.1 General remarks

All software programs that are deliverable, or affect the system, should be held under change control, including:
- application programs;
- 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.
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 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 analyse 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;
- Corrupation 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.

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.
12.2.2.2 Specifying configuration 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 rigour 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 maximises 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 environment (for example, increased interference from new equipment).

12.2.2.3 Managing and preparing configuration data

You should define and write down the process and tools to be used for preparing, checking and inputting the data. You should ensure that any tools used to prepare or test data have sufficient integrity that they will not compromise the integrity of the data.

You should take every practicable opportunity to introduce automated checks of data values or of relationships that should hold between data items.

You should ensure that anyone entering data at a screen is given feedback of the values that they have entered.

You should maintain data under configuration management. You should use the same methods of configuration management as you would for software of the same Safety Integrity Level.

12.2.2.4 Storing and transmitting configuration data

Data may be stored on magnetic (floppy/hard disk, magnetic tape), optical (CDs, DVDs), or solid-state (Flash RAM (Random Access Memory), Static or Dynamic RAM, [E]EPROM ([Electrically] Erasable Programmable Read-Only Memory)) media. Data may be transmitted over wires (serial, Ethernet), optical fibre, optical wireless (infra red), and radio.
Stored data may be susceptible to corruption from a range of environmental factors:

- electric or magnetic fields;
- excessive heat or cold;
- chemical reactions;
- ionising radiation; and
- unwanted modification (either human or automatic).

All storage media will deteriorate over time. You should assess the possible aspects of the environment that may affect the media on which you store configuration data. You should assess the time that data is to be stored and the possible factors that may influence the persistence of data on the media. Some media (especially magnetic and optical) will deteriorate from use, and will therefore have a lifespan determined in part by the frequency of use (both reading and writing). When selecting media you should take into account the likely frequency that data will be read and written, and choose the media appropriately. You should have procedures in place for the assessment of media being used, in order to prevent the loss of data through media deterioration.

Corruption during the read or write process may occur due to electrical or mechanical failure. In order to minimise this possibility several strategies may be used:

- Read back data that is written. Be aware that many storage devices (especially hard-drives) use temporary storage to improve performance; ensure that the version stored is read back, in order to ensure that it has been written properly.
- Write data in multiple locations on a single medium, or use redundant media. Read all copies of the data, in order to discover individual recording errors.
- Where data will not be changed often, you may wish to use some method to prevent it being accidentally overwritten. Such methods may include:
  - physically disabling the data writing component of the hardware, for example providing a switch to disable writes to memory after data is loaded;
  - using media that cannot be overwritten, such as CDs or PROMs;
  - using protection provided by operating systems.

Transmission of data is also subject to environmental influences and system failures. The environmental factors will depend on the medium:

- Both wired electrical, and radio will be subject to electromagnetic interference.
- Radio and optical will be susceptible to problems with propagation. Infrared and certain frequencies of radio will require line of sight, or will have a range that is affected by obstacles.

There are five main classes of failure for a transmission system:

1. loss of data;
2. corruption of data;
3. delay to data;
4. incorrect ordering of data; and
5. insertion of spurious data.
You may also need to consider the possibility that someone may deliberately introduce correct-looking data into the transmission channel.

There are many well-understood protocols that can manage these failures. You should use one that is appropriate for the medium, and the information that you are sending. You may also wish to consider other techniques for improving the reliability, both of the connection and the data sent across it:

- using multiple wired connections that follow diverse paths to eliminate common causes;
- using mechanisms to minimise interference such as balanced lines, or spread spectrum wireless transmission.

When sending or storing data, you should consider the use of error detecting codes. EN 50159 [F.12, F.14] provides further guidance in this area.

12.2.3 Assumptions, dependencies and caveats

The safety of systems is not usually entirely in the hands of those developing them – safety is often reliant on other people’s actions as well. As a result, the developers find themselves making assumptions and placing dependencies and caveats. Assumptions, dependencies and caveats are aspects of the interfaces between systems.

Managing these assumptions, dependencies and caveats may be regarded as part of managing these interfaces.

- **Assumptions** are made about the rest of the world, including the people and organisations with which it will interact, as well as the physical railway. For instance, certain tolerances on the supply voltage may be assumed. Someone will have to check that these assumptions hold when the system goes into service and continue to hold for the rest of its life (or deal with the situation if they do not). Assumptions are likely to be made throughout the project but many will be made near the beginning as input to the design process.

- **Dependencies** are put on people, which means that they are required to act before the system can safely be put into service. A dependency is an agreement between you and another party that they will put something in place before the system enters service. For example, if a computerised signalling system is being installed in a control centre, you may depend on someone else to upgrade the air conditioning first. Dependencies are likely to be placed throughout the project, but many may not be placed until later in the project as they are likely to be outputs from design.

- **Caveats** are placed on people. These are conditions that people must respect after the system is put into operation for it to remain safe. For instance, a certain inspection regime may be required. Caveats are likely to be placed late in the project, after detailed design has been done.

We will treat assumptions, dependencies and caveats together and call them ADCs for short.

Not all ADCs affect safety but many do. If they are not identified or are placed, but not dealt with, a hazard may result.
The railway has grown over many years without procedures for managing this information, and much of it has not been recorded. Moreover, it has been built by many different companies, adapting to different terrains, locations and environments, and different ADCs may be placed on similar systems in different places. ADCs for a line which is electrified will be different from those for one which is not.

The diagram below illustrates some of the ADCs that may be placed for a new train.

![Diagram](image)

**Figure 12-1 Examples of Assumptions, Dependencies and Caveats**

ADCs may be dealt with by standards, such as Railway Group Standards, and Technical Specifications for Interoperability. 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 ADC is fully dealt with in a standard, then showing compliance with this standard will be enough to resolve the ADC. 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 ADCs underpinning the standard into account when deciding whether or not to authorise the departure.

In addition to any economic benefits, resolving ADCs through standards will reduce the opportunities for mis-communication and the standards will generally describe tried and tested solutions. We therefore recommend resolving ADCs through standards wherever practical.

Where an ADC is not dealt with by standards with which you must comply, 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.

However, even if you are working in an area which is well-served by standards you should still look to see if there are any ADCs that you place on others or which others place on you which are not fully covered by standards. If there are any such ADCs, you should take steps to make sure that they are resolved. The rest of this section offers guidance on how to do this. If you cannot find any such ADCs, you should record this fact, as it will form part of the evidence that risk has been controlled.
12.2.3.1 Identifying ADCs that you will place on others

If you place an ADC, you should make sure that it is understood and accepted by the people who will have to deal with it. This obligation is clear from the Yellow Book fundamentals for Safety Responsibility and Communicating safety-related information. Conversely, you need to make sure that you respect any ADCs placed on you.

ADCs are identified as a natural by-product of activities at all stages of the system life cycle. In particular, ADCs 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.

All ADCs which are relevant to the safety of the system are likely to form part of the safety argument at some point, so you should consider how you will resolve them when you make or place them.

12.2.3.2 Identifying ADCs that others will place on you

Failure to respect a safety-related ADC placed on you is likely to result in a hazard, so identifying ADCs placed on you is part of hazard identification.

You should consider all the other systems with which you might interact (whether on purpose or not) and look for ADCs they may place on you.

When looking for ADCs it is important to involve people with sufficient domain knowledge of the system as a whole, and the environment, both physical and organisational, 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 ADCs, you should consult them. They may be either at the network or regional level or by discipline, such as electrification and signalling. However, you should not rely on a central register as your only source.

The checklists on the Yellow Book website for identifying hidden assumptions in risk models can also be used to identify ADCs on you.

12.2.3.3 Documenting ADCs

Within your organisation you should adopt a consistent method of recording, naming and referencing ADCs, in order to make communication and management simpler.

The storage and management of ADCs should not require excessive additional bureaucracy, or paperwork. Therefore, you should attempt to integrate any method for the recording and management of ADCs with other parts of your process, and organisation.

ADCs may be conveniently stored in a register, which is part of, or kept with, the system’s Hazard Log. If a supplier is developing a system which is subject to European interoperability legislation, then they will prepare a Technical File and the register of ADCs may be contained within that.

ADCs have a lifecycle, from the moment that they are recognised and recorded, to the moment when they are either assigned to someone who understands and takes responsibility for them, or closed in some other manner.
You should have some system for recording the ADCs you place, the ADCs that other people place on you, and tracking their progress. Where possible, the status should be recorded with the original entry, or directly referenced to and from it.

As each ADC is identified, someone or some group of people who understands it should take responsibility for resolving it.

Resolving ADCs may involve coming to an agreement with people outside the project, for instance agreeing aspects of the infrastructure maintenance regime with a maintenance contractor or agreeing operating restrictions with the organisation that operates the trains. In some cases, resolving an ADC may have business implications; in which case, whoever is responsible for this ADC should be in a position to handle this aspect of it.

Some centrally co-ordinated register or registers of ADCs held for the whole railway is desirable. If they exist, then all projects should submit their ADCs to them. Where a central co-ordinating system is used, a single indexing and management process will improve the cross-referencing of ADCs between projects.

If you are preparing a Safety Case, then assumptions and caveats will also be present in it, in order to provide context to the safety argument. If you use a specialist notation to represent your safety arguments, for example Goal Structuring Notation (GSN) [F.18] (see appendix E), Claim Structures (see appendix H of [F.19]), Toulmin [F.20], or the Adelard Safety Case Development Manual [F.21], you may be able to represent some or all ADCs directly in the safety argument using this notation.

Safety certificates will contain ADCs which the operator must monitor or act on. For example, they may include assumptions about maintenance schedules.

### 12.2.3.4 Resolving ADCs

By their nature, ADCs are not normally fully closed by the project alone. The project’s responsibility is to ensure that someone else understands and accepts each ADC. We say that an ADC is resolved when this has been done.

ADCs may be communicated in Safety Cases, Hazard Logs, correspondence, formal handover documents, operations and maintenance manuals. If you need operations or maintenance staff to be aware of an ADC, you will normally deal with it in the operations or maintenance manuals. Typically, this will be safety-related information which you will need to highlight as such. An ADC should not be considered resolved until the recipient has confirmed that they understand and accept responsibility for it.

The type of responsibility will be different for assumptions, dependencies and caveats. An assumption is resolved when someone takes responsibility for checking that it holds when the system goes into service and thereafter, or dealing with the situation if the assumption does not hold. Dependencies and caveats are actions, and are resolved when someone takes responsibility for carrying them out.

ADCs may initially be placed on 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.

However, before you pass on an ADC you should consider if you could design it out of your system. Reducing the dependency between systems 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 ADC will not be appropriate in all circumstances.
It may also help to make the interfaces of a new system the same as the old one that it replaces. This may result in a more complex interface being used than could be developed from scratch. However, it may be easier to resolve the ADCs implicit in the interface.

ADCs should be examined regularly throughout the lifetime of the system to ensure that information about them is kept up-to-date and complete, that any new ADCS which have emerged have been dealt with and that existing ADCs are still valid.

Where two or more projects share an interface, regular meetings between them may be useful to resolve ADCs. Where a new system shares an interface with an existing system, meetings between the developers of the new system and those responsible for operating the existing system may similarly be useful.

In most cases, some ADCs will be the responsibility of people within other organisations. When transferring responsibility to other organisations you may face problems identifying those with sufficient skill, and assigning the responsibility to those people. You should make the transfer of responsibility part of your process for the handover of the project, working with clients and partner organisations to ensure that an appropriate person or group of people takes responsibility for each ADC. In some situations you may not be able to assign responsibility directly to an individual. It may be necessary to assign it to the organisation as a whole, with some individual, who may not have the skills or knowledge to deal with it directly, taking responsibility to ensure that it is dealt with by someone who does.

In general, the assignment of responsibility is likely to be a difficult process and you will have to take a pragmatic approach. Most importantly, you must ensure that responsibility is never lost. If you cannot transfer responsibility to someone who is equipped to discharge it, then try to transfer it to someone who is in a position to assign it to someone else who can deal with it.

12.3 Additional guidance for projects
This section has been removed from this version but is available in the full version of the Yellow Book.

12.4 Additional guidance for maintenance
Configuration management underpins maintenance. If you are setting off to repair some points, you need to know what type of rail, what points machine and what points detection equipment is installed there, and you need to know what replacement parts you can install.

It is important to realise that some elements of the configuration may be documents or computer files. It is, for instance, important to keep training courses in step with the actual equipment installed.

If someone gives you information about a safety risk that could affect the safety of the part of the railway that you are responsible for, you might need to quickly find out whether you need to do something. Before you can take a safety decision, you will need to understand the risk and the consequences that could arise from your decision. You will also need to find accurate information to be able to take the correct decision. You should store up-to-date configuration information so that it is easily retrievable.
You should develop a pro-active, systematic configuration management system. The type of information and the amount of detail that you should keep will depend on the safety decisions you have to take and the length of time that you have to respond to situations that arise.

For example, an incident may arise that requires a component batch modification or recall. If you have up-to-date asset configuration and distribution information available, you should be able to respond quickly with minimum effort without having to commission a detailed survey to find where they all are.

12.4.1 Asset configuration

Your maintenance organisation should have up-to-date information about how the part of the railway that you maintain is configured. You need to have ‘as-built records’, which contain enough up-to-date information about the railway so that you can take the safety decisions that you need to. This may be structured as an asset register.

You should keep information about the way components and systems connect with each other to ensure safety. You should record the modification status of components, where compatibility with other parts of the railway is required to ensure safety. You should also keep information about adjustments and settings where they can affect other parts of the railway (such as point settings, signal lamp voltages and traction power supplies).

You should understand:

- asset types;
- modification states (for example, EPROMs, hydraulic valves, relay units);
- the location and population of assets;
- the status of temporary alterations and adjustments;
- the service duty and condition of strategic assets;
- how each asset is used, particularly where the number of operations is related to an asset servicing or replacement regime;
- the configuration status of spare parts to make sure that when they are used, they are of the correct type and modification state; and
- the availability, location shelf life of spare parts (including strategic spares managed by your suppliers).

Where the risk associated with connecting incompatible components is too high, you should do something to prevent this from happening. This might include making sure that incompatible components cannot be connected (for example using a pin code on plug in bases) and you should always make sure that the modification status of components is clearly identifiable.

12.4.2 Information configuration

You should make sure that technical records are up-to-date (for instance layout plans, detailed design drawings, system analyses) and available to personnel who need to use them.

You should make sure that your maintenance documentation is controlled and distributed so that your personnel have the correct, up-to-date version. It is good practice to use a computer tool to help you to manage this.
It is good practice to give someone responsibility for managing the controlled distribution of documents and technical information. You should keep information about what documents are current, their version and the locations to which they are issued. It is also good practice to maintain a master (source document) so that changes to documents can be safely controlled.

Before you take a safety decision about the railway that requires information from technical records, you should make sure that the records you are going to use are up-to-date and the correct version. If you are not sure, you should compare the record with the assets it describes before making your decision.

12.4.3 Keeping records

Your maintenance organisation should decide what records it needs to keep and then keep them. It is good practice to keep records of:

- the risks you have to control;
- asset operations;
- incidents and failures;
• your maintenance organisation;
• your maintenance process:
  – the types of maintenance you are going to do;
  – the maintenance work that you have done;
  – the resources you have used;
  – the decisions that you take about maintenance and the justification for
    the decisions (for instance decisions to defer maintenance or repairs);
  and
• your communications.

The records you keep should be clear, simple and appropriate to the decisions that
may be required in the future. You should know what you are going to do with the
records and avoid keeping records that are not needed.

The records you keep and the way you choose to keep records may be laid down in
standards and legislation.

Your maintenance organisation should review records to decide whether risk is being
controlled to a low enough level. This will help you decide whether to change the way
you do things to make things safer. You should then record the decisions you take
and the basis on which they were taken.

<table>
<thead>
<tr>
<th>Record</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your maintenance organisation</strong></td>
<td>You should keep records about the way you have set up your organisation,</td>
</tr>
<tr>
<td></td>
<td>particularly the scope and allocation of safety responsibilities, your</td>
</tr>
<tr>
<td></td>
<td>organisational goals, your safety culture and your competence. You should</td>
</tr>
<tr>
<td></td>
<td>also keep records about your suppliers.</td>
</tr>
<tr>
<td><strong>The risks you have to control</strong></td>
<td>You should keep up-to-date records of all the hazards that your</td>
</tr>
<tr>
<td></td>
<td>maintenance work is designed to mitigate.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you keep details of these hazards and the arrangements</td>
</tr>
<tr>
<td></td>
<td>to control them in a Hazard Log. You may find the guidance on structuring</td>
</tr>
<tr>
<td></td>
<td>and managing Hazard Logs in the project section of this chapter and in</td>
</tr>
<tr>
<td></td>
<td>appendix B; a useful starting point, but you should be prepared to adapt</td>
</tr>
<tr>
<td></td>
<td>the guidance to your needs.</td>
</tr>
</tbody>
</table>

*Note: some people use the term **Risk Register** to describe a document with the same purpose and scope as a Hazard Log. Others use it to describe a more general register of risks, including commercial and environmental risks.*
## Records

### Records of maintenance process – your decisions

When you decide what maintenance you are going to do, you should keep a record of the decision. Your decisions should be traceable to the risk that your maintenance is designed to control.

For example, a record of maintenance shows that a piece of equipment is defective and may pose unacceptable risk. A decision has to be taken whether to allow the equipment to remain in service until it can be repaired or replaced, or to take the system out of service. Your decision will depend on a balance of risk between the effect of taking the equipment out of service and the risk of further degradation. The decision may require reference to other records (such as as-built records, spares records, component specifications) and standards. The decision and the justification (based on available information) should be recorded and retained for future reference.

When you take a decision that will change the way you plan and carry out your work (for instance an increased inspection regime in connection with an outstanding defect), you should ensure that the decision is recorded in a way that can be communicated to those who need to implement the decision.

### Communications

You should keep records of safety-related communications so that you can review events to support incident investigation, audit and support learning. This includes personnel briefing records, including attendance, content and required actions.

Verbal communications that include messages about operational railway safety should be recorded to allow replay at a later date.

You should decide and record how long you need to keep records of verbal communications and implement a rotation system to manage the recording media (for example, four-weekly rotation).

Written communications relating to safety should be archived in accordance with your company policy and to comply with any appropriate regulations and standards.

### Asset operations

It is good practice to monitor and record some equipment operations. Sometimes, these facilities will be designed into the system you are responsible for maintaining (such as level crossing event recorders and electronic interlockings) and you will have to manage the records that they produce. In other circumstances, you might decide to connect temporary monitoring equipment to record the behaviour of equipment that is alleged to be faulty. You should make sure that the test instrumentation that you connect to safety-critical systems is approved for use in the manner you are using it and that your staff are competent to install and use it.

You should decide what you are going to record, the format in which it will be recorded and how you will record the information to make sure that it can be analysed.
Incidents and failures
You should keep records of safety-related incidents and near misses. You should review them so that you can decide whether to change the way you do things to make things safer.

Maintenance process - what you are going to do
When your organisation decides how it will do maintenance work, you should record it in a format that will allow the decision to be properly implemented.

Maintenance process - what you have done
When you maintain a part of the railway, you should record what was done so that you can compare it with what you planned to do.

Maintenance process - resources you have used
You should keep records so that you can find out later on what resources you have used for your work. You might need to do this as part of an incident investigation or as part of an audit. The amount of detail you keep should reflect the need for traceability.

You should improve accessibility to records by making sure that they are available at the locations and in such a format that those who need to use or communicate information about them can do so. The format you choose may be subject to legal requirements (for example, a requirement to keep paper copies of test certificates containing signatures).

If people working on equipment need to refer to records, you should make sure that the records are available at the place that the work is being done. For example, equipment test results should be made available to maintainers and other maintenance organisations to analyse tolerance drifts over time and help with fault rectification work.

You should protect records against loss, for instance by keeping back-up copies.

12.5 Related guidance
Chapter 5 provides guidance on transferring safety responsibility.
Chapter 15 and Chapter 17 provide guidance on assessing and mitigating any safety implications of changes.
Safety Audits and Assessments of safety documentation are described in Chapter 13.
Appendix B provides an outline Hazard Log.
Appendix C provides checklists for updating the Hazard Log.
Appendix E provides guidance on GSN.
Chapter 13

Independent professional review

Fundamental from volume 1: Independent professional review
Safety management activities that your organisation carries out must be reviewed by professionals who are not involved in the activities concerned.

13.1 Guidance from volume 1
These reviews may be structured as a series of Safety Audits and Safety Assessments. Audits provide evidence that you are following your plans for safety. Assessments provide evidence that you are meeting your safety requirements. So, both support the Safety Case. 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 a safety management activity is done many times, it may be better to specify it precisely and review the specification rather than the activities themselves. For example, you might have the procedure for replacing a signal bulb reviewed. You should then check that the specification is being followed.

13.2 General guidance
Review of safety-related work by professionals independent of the work is an important contribution to the confidence in the safety of the work for both projects and maintenance. However, the guidance that we offer on implementing this fundamental differs quite significantly between projects and maintenance.

13.2.1 Limitations of this guidance
In the UK, the 'Railways (Interoperability) Regulations 2006' [F4] and the 'Railways and Other Guided Transport Systems (Safety) Regulations 2006' ('ROGS regulations') [F3] both require independent verification, which is a form of professional review, but based upon a rationale and processes which are different from the project guidance in this chapter. The interoperability directives require verification by 'Notified Bodies' and the ROGS regulations call for a process of 'Safety Verification'.

These are not the only relevant pieces of UK legislation. See volume 1, section 2.1, for further information.
The law takes precedence over guidance such as the Yellow Book. If your work falls within the scope of legislation you should follow the guidance associated with the legislation. In case of conflict with the guidance in the Yellow Book, the guidance associated with the legislation will take precedence. At the time of writing, the interpretation of the Interoperability regulations and ROGS regulations was evolving, so, if you refer to guidance on the legislation, you should make sure that you have the latest version.

We intend, in the next version of Yellow Book, to make the guidance on putting the Independent professional review fundamental into practice fully consistent with the requirements of the Interoperability regulations and ROGS regulations and the guidance on these regulations issued by the Department for Transport (DfT) and ORR.

13.2.2 Adapting this guidance

The project guidance in this chapter is designed for a situation where:

- risk cannot be controlled completely by applying standards; and
- you are compiling evidence of safety into a Safety Case.

If the risk comes completely within accepted standards that define agreed ways of controlling it (see section 2.4.3), then the fundamental may be put into practice in different ways, for instance by an independent check that the standards have been met.

If your Safety Approvers require evidence of safety presented in a different way, then you will need to adapt the guidance to suit your situation.

13.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

13.4 Additional guidance for maintenance

Independent review of safety management activities is just as important for maintenance, but, good practice in maintenance is to integrate independent professional review into the routine activities, so the guidance on maintenance can be shorter than for projects.

Your maintenance organisation should plan a hierarchy of independent professional review activities, such as Safety Audits, document reviews and inspections, to make sure that all of your maintenance plans and the way they are implemented and reviewed is achieving the required level of safety. These activities should be structured around the requirements contained in standards and planned in the context of your top-level strategy. You should include your suppliers in your Safety Audit hierarchy. The project guidance above may be helpful in setting up a Safety Audit but you should be prepared to adapt it.

The type, frequency and extent of the independent professional review activities that you carry out should be proportionate to the risk you are managing. It is good practice to include a level of independence within these activities. When we talk about independence, we mean using people who are independent of thinking and independent of delivery. The people you choose to use may be part of your own organisation or from an external agent.
Not all of your professional review needs to be independent. Supervision and inspection is a form of internal professional review, which should be seen in the wider context of the safety assurance regime.

The people you use should be sufficiently competent, familiar with the risk being managed and have the authority to recommend changes where they are required. They should understand the risk that is being controlled and be competent to decide whether your maintenance is sufficiently controlling it.

It is good practice to ensure consistency by using checklists; however, you should develop these so that they prompt the checker to ask questions around process and meeting requirements rather than just prescribing what should be checked.

All findings should be formally recorded. If you find a safety or compliance problem, it is good practice to issue a written instruction to the person responsible for putting it right. This should specify the actions that you need to put into place to fulfil immediate, short-term and longer-term safety planning documents.

You should communicate the results to people responsible for work planning and implementation so that they can take decisions about whether things need to be changed elsewhere.

It is good practice to change the scope and frequency of independent professional review activities to reflect what you find. Additional follow-up audits are a good way of verifying that audit corrective actions and recommendations have been implemented.

The findings of independent professional review activities should be used as input to the activities that you carry out to implement the Monitoring risk fundamental (See Chapter 16).

13.5 Related guidance

Chapter 11 provides guidance on safety planning.
Chapter 15 provides guidance on risk assessment.
Chapter 16 provides guidance on monitoring risk.
Chapter 17 provides guidance on the Safety Requirements Specification and Safety Integrity Levels.

Appendix B provides outline audit and assessment remits and reports.
Appendix D provides an example assessment remit and example audit and assessment checklists.
Part 4

Risk Assessment Fundamentals
Chapter 14
Defining your work

Fundamental from volume 1: Defining your work
Your organisation must define the extent and context of its activities.

14.1 Guidance from volume 1
If you are in doubt 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.

If you are maintaining the railway, these things are often defined in a contract or a scope document. These documents may be based on assumptions. If so, you should check these assumptions later.

If you are maintaining the railway, the extent of your activities will include the part of the railway you are maintaining and the sorts of maintenance you do on it. The context might include traffic levels, the things your part of the railway might affect, and the things that might affect your part of the railway.

You should find out who will have to approve your Safety Case.

14.2 General guidance

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

The guidance in this chapter is principally relevant in the Concept and Feasibility; Requirements Definition and Operations and Maintenance phases of the System Lifecycle.

This chapter is written for:

• Project Managers, and
• anyone involved in performing or reviewing a risk assessment.
14.2.2 General remarks

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

Figure 14-1 illustrates the relationship between the system boundary, hazards and accidents.

The system or equipment may consist of software, hardware, people and procedures. The environment consists of anything that could influence, or be influenced by, the system or equipment. This will include anything to which the system connects mechanically, electrically or by radio, but may also include other parts of the railway that can interact through electromagnetic interference, or thermal interchange. The environment will also include people and procedures that can affect, or be affected by, the operation of the system or equipment.

When specifying a system you may find it useful to check that you have specified clearly for every aspect of the system:

- Its function
  Not just what it does, but also what it must not do, in normal and degraded modes.
- Its interfaces
  With other systems, and with people and the organisation.
- Its environment
  Relevant parameters may include ambient temperature ranges, levels of electro-magnetic interference, and organisational aspects, such as the level of training of users.
- The quality of the service it must provide
  The standard to which the functional requirements are to be fulfilled. Relevant criteria include safety, reliability and availability.
• Other contractual and related issues

Any relevant issues of intellectual property, licences, patents, spares, manuals and so on. If you do not take these into account you may find that they limit your ability to react to problems in the future.

The following list provides examples of what might be included under each heading.

• Its function:
  – facilitate operation to the timetable;
  – provide capacity for agreed levels of service recovery;
  – provide control facilities under failure and emergency conditions and their recovery;
  – enforce the safety principles;
  – protect staff;
  – provide fault alarms and operation logging;
  – provide customer and management information;
  – facilitate efficient use of traction energy.

• Its interfaces:
  – organisation (operators, maintainers, management, customers, emergency services);
  – trains (human drivers or automatic systems, train protection, vehicle health monitoring);
  – permanent way (train detection, points, indicators, bridges, tunnel ventilation etc);
  – electrical traction power (supply distribution control);
  – neighbours (level crossings, other railways);
  – station and terminal services, depots, technical (positional references, loadings, earthing policy, heat dissipation);
  – chemical interfaces – (dissimilar metals);
  – data formats and information flow.

• Its environment:
  – organisation (staff competence – select, train, resource, authorise, motivate, monitor);
  – railway rules and procedures;
  – weather;
  – shock and vibration;
  – electromagnetic interference;
  – noise;
  – local conditions and lighting;
  – faulting and maintenance support policy;
  – vandalism/terrorism/malicious acts.
• The quality of the service it must provide:
  – 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;
  – 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.

• Other contractual and related issues:
  – patents and copyright;
  – licences (jigs, tools, templates, software use and alteration);
  – spares and special test/diagnostic equipment;
  – documentation and manuals;
  – certification;
  – training.

14.2.3 The supplier chain

Any railway involves a network of stakeholders. The ultimate services to the public are provided by the Transport Operator. However, they rely on suppliers in order to do this, their suppliers rely on other suppliers and so on.

It may be the case that the overall safety of the railway depends upon the weakest link in this chain.

Figure 14-2 shows an example of this state of affairs. A Transport Undertaking, an organisation that runs train services, relies on a train supplier to provide them with trains. The train supplier, in turn relies on other companies to supply train components, such as the driver’s display. Of course, this is just a small fragment of a much more complex network of suppliers.
There is a hierarchy of systems associated with this network of suppliers, as illustrated in Figure 14-3. 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.

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.

System B provides the environment for system A. The supplier of system B should, therefore, provide the supplier of system A with information that the latter needs to carry out ESM, including relevant hazards, risks and safety requirements associated with System B. This is discussed further in Chapter 9.
Note: we use the phrase ‘sub-system’ in a general sense to mean any small system which is part of a larger system. You should also note that other publications, particularly those discussing European interoperability legislation, use the word in a more limited sense to refer to one of a fixed list of parts of the railway.

### 14.2.4 Legal framework and acceptance regime

As we explained in section 2.4, this volume does not assume any particular legal framework or approvals regime. This means that, before you can use the guidance, you will have to 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 more guidance on these topics in section 2.4 and there is further guidance in Chapter 18 on establishing who will approve your work, that is, who your Safety Approvers are.

### 14.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

### 14.4 Additional guidance for maintenance

If your maintenance organisation is responsible for the part of the railway that you maintain, you should have an up-to-date asset register (See Chapter 12). Likewise, if you are maintaining a part of the railway for someone else, you should have an asset register and then agree it with them.

You should understand and record the context in which your maintenance will be done and any assumptions that could affect how you will do it. Examples include:

- available access to parts of the railway;
- traffic types, levels and speeds;
- the railway environment; and
- the way other parts of the railway are managed.

If you are maintaining a part of the railway for someone else’s organisation, you should find out how they will approve your safety planning documents and what work your organisation can approve.

In some areas, all of this is defined in a document called an ‘Asset Maintenance Regime’.

Where your work interfaces with other parts of the railway or organisations, you should consider what work they do (see Chapter 5).

### 14.5 Related guidance

Chapter 5 provides guidance on safety roles and responsibilities.
Chapter 9 provides guidance on the information that should be provided to suppliers, to allow them to carry out effective safety analysis.

Chapter 12 provides guidance on maintaining an asset register.
15.1 Guidance from volume 1

15.1.1 Identifying hazards

Identifying hazards is the foundation of safety management. 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 get rid of 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 you might contribute to the hazard when carrying out your activities and responsibilities.

You should not just consider accidents which might happen during normal operation, but those which might happen when things go wrong or operations are not normal or at other times, such as installation, testing, commissioning, maintenance, decommissioning, disposal and degraded operation.

When identifying hazards, you should consider:

- the people and organisations whom your activities and products will affect; and
- the effects of your activities and products on the rest of the railway and its neighbours.

You may identify a possible hazard which you believe is so unlikely to happen that you do not need to do anything to control it. You should not ignore this type of hazard; you should record it, together with the reasons why you believe it is so unlikely to happen and review it regularly.

You should consider catastrophic events that do not happen very often and the effects of changes in the way the railway is operated.
15.1.2 Assessing risk

In most countries, you will have a legal duty to assess risk. Risk depends on the likelihood that an accident will happen and the harm that could arise. You should consider both factors. Your organisation should also consider who is affected.

Some things are done specifically to make the railway safer, that is to reduce overall railway risk, at least in the long run. You should still assess them in case they introduce other risks that need to be controlled.

Your risk assessment should take account of the results of the activities described in the monitoring risk fundamental below.

15.2 General guidance

15.2.1 Adapting this guidance

The project guidance in this chapter is designed for a situation where risk cannot be controlled completely by applying standards. If the risk comes completely within accepted standards that define agreed ways of controlling it, then you may be able to control the risk and show that you have done so without carrying out all of the activities described in this chapter. See section 2.4.3 for more guidance on this situation.

15.2.2 Background

We introduced the concept of hazard and risk in Chapter 2. 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 assessment entails a systematic analysis of the potential losses associated with the work and of the measures for reducing the likelihood or severity of loss. It enables losses to be aggregated and compared against the cost of measures.

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

The guidance in this chapter enables you to establish the facts on which you have to take a decision that involves risk. The extent to which you use formal risk assessment methods depends on the specific situation, as described in section 2.4.

When you assess risk you will normally find that you have to make assumptions. There is guidance on managing these assumptions in Chapter 12.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for:

- anyone involved in performing or reviewing a risk assessment.
15.2.2.1 Quantitative and qualitative analysis

The seven-stage process that we introduced in Chapter 3 presents a uniform framework for assessment of the full range of risks associated with any given undertaking. Within this framework, the analysis may be performed to different depths. Qualitative risk assessment is appropriate for the smaller risks and quantitative risk assessment for the larger risks. It is also possible to adopt hybrid approaches.

It is acceptable, in both approaches, to adopt approximations, provided that they are conservative, that is, that they do not underestimate risk.

Qualitative risk assessment relies mainly upon domain expert judgement and past experience. It addresses the risks of an undertaking in a subjective and coarse manner. There is not a complete lack of quantification, but order of magnitude estimates are generally used. Its advantages are that:

- it does not require detailed quantification, data collection or analytical work;
- it is relatively simple; and
- it is less expensive than quantitative risk assessment.

Its disadvantages are that:
- the assumptions require thorough documentation; and
- it is inadequate as the sole basis for assessment of major risks, including those arising from low loss incidents of high frequency, as well as from low frequency incidents associated with high losses.

Quantitative risk assessment employs rigorous analytical processes. Whilst based upon the same fundamental principles as qualitative risk assessment, quantitative risk assessment will typically employ modelling, using objective and validated data; explicit treatment of the uncertainty associated with input data; and explicit treatment of the dependencies between significant factors contributing to risk. Its advantages are that:

- it is more accurate than qualitative risk assessment;
- it helps identify hidden assumptions; and
- it provides a better understanding of the potential causes and consequences of a hazard.

Its disadvantages are that:
- it is complex;
- it requires expertise;
- it requires a lot of objective data;
- it is difficult to quantify the probability of Systematic Failures;
- it is more expensive than qualitative risk assessment; and
- it can require significant computing resource.
Qualitative risk assessment is likely to suffice for most hazards. However, hazards, with the potential to lead to major or catastrophic consequences, may require quantitative risk assessment. A quantitative approach may also be justified for novel systems where there is insufficient experience to support an empirical, qualitative approach.

Quantitative risk assessment is more expensive than its qualitative counterpart and should only be applied if it is justified by the increased confidence achieved.

15.2.2.2 Use of historical data

Risk assessment always relies on some form of extrapolation from the past to the future. Historical data is used at many stages 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 assessment.

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.

15.2.2.3 Documenting the process

Typically, the results of a risk assessment study will be compiled into a Risk Assessment Report so that they can be subject to review and endorsement.

Once risk assessment results have been reviewed and endorsed they should be immediately incorporated into the Hazard Log, which is described in Chapter 12.

15.2.2.4 Using likelihood-severity matrices to simplify repeated assessments

If you have to carry out a series of risk assessments of applications of a system which are similar, then you may find that a likelihood-severity matrix can save repeating the same work. The matrix may be produced by the Transport Operator or by the system supplier from information provided by the Transport Operator or some other authority.
A likelihood-severity matrix has the following general format:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insignificant</td>
</tr>
<tr>
<td></td>
<td>Marginal</td>
</tr>
<tr>
<td></td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Frequent</td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td></td>
</tr>
<tr>
<td>Incredible</td>
<td></td>
</tr>
</tbody>
</table>

Table 15-1 Example format of likelihood-severity matrix

Table 15-1 is only an illustrative example. It shows the column and row headings suggested in EN 50126 [F.11]. Other headings may be used.

The two components of risk – frequency (or likelihood) and consequence (or severity) – are partitioned into broad order or 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 acceptability category is written into the cell.

Note: it is also possible to split the frequency or likelihood into two components:

- the frequency or likelihood of a hazard occurring;
- 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 a hazard but, of course, the tables become three-dimensional and more difficult to handle.

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 likelihood, severity and risk acceptability 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, its hazards, its environment, its mode of use and the number of systems in service; and
- guidelines for the use of the matrix.

When using the matrix, you should provide justification of the likelihood and severity categories assigned to each hazard.
To avoid possible later problems with use of the matrices, you should submit the matrix with your justification that it meets these criteria for endorsement by any Safety Approver whom you may later ask to endorse a safety argument using the matrix.

15.2.2.5 Risk assessment and broader decision making

Risk assessment is focussed 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. The seven-stage process will assist you in eliminating alternatives which do not comply with your obligations. The seven-stage process can be extended to help control non-safety losses (such as environmental and commercial losses) but that is beyond the scope of this book.

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. Techniques such as Weighted Factor Analysis [F.16] provide a basis for balancing the factors in such decision making.

This chapter presents a systematic framework for:

- identifying hazards;
- assessing risk, and
- reducing risk.

The next section provides some further background.

15.2.2.6 UK Law and the ALARP Principle

The ‘Health and Safety at Work etc Act 1974’ places duties on employers to ensure health, safety and welfare ‘so far as is reasonably practicable’. This section gives more guidance on this test. It is based on the Health and Safety Executive (HSE) publication ‘Reducing Risks, Protecting People’ [F.17].

This test is applicable to some but not all railway decisions and, at the time of writing, this aspect of UK law was being clarified. You should establish whether or not it applies to your work before following the guidance below.

If you are carrying out work on the railway, you should first identify the hazards associated with the work. You should make sure that you have precautions in place against each hazard within your control, unless you can show that the risk arising from the hazard is negligible.

You should make sure that your precautions reflect good practice, as set out in the law, government guidance and standards. If the risk is low and completely covered by authoritative good practice, showing that you have followed it may be enough to show that the risk is acceptable. For instance, the electrical safety of ordinary office equipment is normally shown by certifying it against electrical standards. However, before you decide that just referring to standards is enough, make sure that:

- the equipment is being used as intended;
- all of the risk is covered by the standards; and
- the standards cover your situation.

If following good practice is not enough to show that the risk is acceptable, you should also assess the total risk that will be associated with the work. You then need to compare it with two extreme regions:
• An unacceptable (or intolerable) region where risk can never be accepted.
• A broadly acceptable region where risk can always be accepted.

To decide whether or not to accept a risk:
1. Check if the risk is in the unacceptable (or intolerable) region – if it is, do not accept it.
2. Check if the risk is in the broadly acceptable region – if it is, you will not need to reduce it further, unless you can do so at reasonable cost, but you must monitor it to make sure that it stays in that region.
3. If the risk lies between these two regions, accept it only after you have taken all ‘reasonably practicable’ steps to reduce the risk.

Figure 15-1 illustrates the principle described above. This is often referred to as the **ALARP Principle**, because it ensures that risk is reduced to ‘As Low As Reasonably Practicable’.

You should consider ways of making the work less likely to contribute to an accident. You should also consider ways of making the work more likely to prevent an accident. You do not have to consider steps that are outside your control.

---

**Figure 15-1 The ALARP Principle**
If you are making a change, you will generally expect the risk to be lower after the change than it was beforehand; if it is higher, it is unlikely that you have reduced risk as low as reasonably practicable.

If you are uncertain about the risk, then you should err on the side of caution – uncertainty does not justify inaction.

The principle should be interpreted intelligently. Sometimes it may be necessary to accept a modest increase in risk in the short-term to achieve sustained decrease in risk in the long-term.

To be suitable and sufficient, the sophistication and depth of risk assessment should be proportionate to the level of the risk.

When using likelihood-severity matrices to justify an ALARP decision, it is common practice to employ categories which reflect the regions of the ALARP guidance (see next section), that is Intolerable, Tolerable and Broadly Acceptable. An additional categorisation may also be found useful, in which the Tolerable category is split into two, one towards the Intolerable end of the range and one towards the Broadly Acceptable end.

Before using the matrix to justify an ALARP decision, you should show that it meets all the following criteria:

- If all hazards of the system are assessed as Tolerable, then it follows, using the explicit assumptions, that the total risk presented by the system to any affected group of people falls in the Tolerability Region and is consistent with agreed overall risk targets.
- If all hazards of the system are assessed as Broadly Acceptable, then it follows, using the explicit assumptions, that the total risk presented by the system to any affected group of people falls in the broadly acceptable region.
- The matrices can be used to support a justification that risk has been reduced to an acceptable level. The guidelines should emphasise that the final judgement relates to the total risk arising from the system as a whole. In particular, if the ALARP Principle is being employed, they should advise that:
  - Partitioning the risk across hazards and evaluating each hazard against a chosen matrix alone may lead to each hazard being considered as Broadly Acceptable or Tolerable, whereas the total system risk may be in a higher category.
  - The total risk should be reduced so far as is reasonably practicable. So, if the total risk is in the Tolerable region, but the classification from one particular hazard is Broadly Acceptable, the risk from this hazard should still be reduced further if it is reasonably practicable to do so.

15.2.3 Failure detection and modelling

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 mitigate each other’s hazards provides network resilience: the railway as a whole is safer and more reliable than any of the individual systems. This is not just a product of automatic functions only, communications systems may facilitate failure or emergency messages to be made in accordance with Rules and Regulations. The manner in which human beings and the organisation as a whole behave will affect the safety of the system.

It is possible to inadvertently degrade this network resilience if this is not recognised. 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.

The **Assessing risk** fundamental requires that ‘Your organisation must assess the effect of its activities and responsibilities on overall risk on the railway’. You need to take account of failure detection in two ways to do this:

- Firstly, you need to understand how the railway can detect and respond to hazardous failures of your system in order to estimate the time at risk, and the time between entering and leaving the dangerous state. This can be a major factor in the assessment of the risk associated with the system. The risk associated with signal filament failure is generally assessed to be low, for instance, because the time at risk is short.

  This chapter describes the process by which you assess risk arising from a system using Cause and Consequence Analysis. As part of Consequence Analysis it is important to look for factors that can mitigate hazards. In many cases the ability of other systems, mechanical or otherwise to successfully mitigate a hazard will be dependent on the time taken to react. In order to assess fully the risk in the system, you need to be able to assess the time at risk, and decide the probability of an accident occurring during that time.

- Secondly, you need to understand how your system can reduce risk arising from other causes by detecting or mitigating hazards elsewhere.

You can reduce overall system risk by increasing the system’s ability to detect hazards in the rest of the railway. However, when you remove an old system, you may also inadvertently reduce the ability of the network to detect failure. If you are replacing an older system you will generally wish to ensure that the new system is at least as capable of detecting hazards as the old one. If you cannot achieve this, then you should look for measures that can be taken to compensate for the loss of network resilience. It is important that the overall safety of the network is not reduced; any loss of failure detection should be weighed against possible improvements in safety that may result in an overall improvement.

In order to understand the effect that a change will have on the safety of the system, it is important to identify those systems that have dual roles, both functional and safety. You should identify how the system that is being modified may provide safety functions to the network as a whole. You should characterise how it behaves when faced with a potentially hazardous sequence of events and how quickly it reacts. You should identify the manner in which the railway as a whole reacts to the failure of a single component.
Where an existing system 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 to identify the systems (including such things as track) with which it interacts, and identify the failure modes of these systems.

In all the examinations of the interaction of the system with the railway as a whole, you should make use of any assumptions, dependencies or caveats (ADCs) associated with the system (see Chapter 12). 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, each transition potentially being the result of a different system. State-transition diagrams and the Unified Modeling Language (UML) can provide useful notations for capturing these scenarios.

Figure 15-2 (below) is an example state transition diagram. The round cornered boxes represent the states of the system, and the arrows represent the transitions between those states. This example models debris being on a track, and the driver of a train on the neighbouring track spotting it, and notifying the control centre. All the states within the box are ones for which the railway is at risk.

![State Transition Diagram](image)

**Figure 15-2 Example State Transition Diagram**

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. It is acceptable to be approximate provided that approximations are conservative, that is that they do not underestimate risk.
If you have modelled 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.

15.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

15.4 Additional guidance for maintenance

15.4.1 Hazards that inform development of your maintenance strategy

Your maintenance organisation should do its best to predict and identify all of the hazards associated with the parts of the railway that you are responsible for. If you are already following good practice, you should have an up-to-date register of risks and understand the nature of the risks you are managing. If you do not have all of the information about the hazards that your maintenance is designed to eliminate, you might not be able to manage all of the risk. You should remember that hazards may exist:

- within the equipment that makes up part of the railway (for instance failure modes);
- as a result of the way equipment is used;
- as a result of the way equipment connects to other parts of the railway;
- at the place the equipment is located (for example within a confined space or adjacent to exposed electrical conductors); and
- as a result of the way the part of the railway is maintained.

Hazards may affect all sorts of people, including operational personnel, maintenance personnel, passengers and neighbours.

15.4.2 New hazards that arise during the asset life cycle

When you have implemented your maintenance strategy, you should keep looking for new situations that are not addressed by your existing maintenance plans and programmes.

For example, a significant system failure may require a temporary method of degraded railway operations using equipment in a different way from that which the maintenance strategy is designed to manage (such as diversion of trains onto a route that is usually only lightly used). In these circumstances your maintenance organisation should work with all the other organisations involved to develop maintenance plans that will ensure the railway will be safe for the duration of the changed circumstances.

When this happens, you should identify all of the hazards that arise from the change of use and then look at the risk level associated with each hazard. Temporary control measures arising from the example above could include additional equipment inspections, enhanced maintenance, spot renewal of components and re-allocation of fault teams to ensure rapid response targets are met. They might also include placing limits on the way the asset is used (for example a speed restriction or a restricted signal aspect).
15.4.3 Identifying hazards

Before you identify hazards, you should decide what information you need and gather it from dependable sources. You should gather information about:

- how the part of the railway works and what it is supposed to do;
- how it is going to be used;
- where it is going to be used;
- possible failure modes;
- how other parts of the railway affect it when they operate normally and when they fail;
- how it will affect other parts of the railway when it operates normally and when it fails; and
- how it has to be maintained.

You should also identify all of the additional hazards that arise from doing maintenance, such as hazards associated with using tools and equipment as well as the hazards arising from the maintenance activity. Doing maintenance incorrectly can also be a hazard. Before you decide how to maintain a part of the railway, you should understand:

- the hazards that affect your maintenance personnel; and
- the hazards that affect other parts of the railway, including railway operations.

You should record all of the hazards so that they can be reviewed in the future, for example using a Hazard Log. You should also record the assumptions on which the hazards are based so that you can re-assess risk as part of a future risk review.

If hazards associated with part of the railway have already been identified as part of a project, you should make sure that you know what they are before accepting safety responsibility for the asset. You might still have to identify other hazards that result from the way you plan to do your maintenance work.

15.4.4 Understanding risk

When you have captured all of the hazards, you should work out the risk that arises from each hazard. The risk level is derived from the likelihood that a hazardous event will occur and the consequence of the event occurring. Some of the techniques that will help you to do this are described fully in appendix E (for instance FMEA and FMECA). You may also find the project guidance above useful, if the risk that you are trying to understand is high or the issues are complex.

It may be sensible to place hazards in broad categories according to their consequences. If so, then you can categorise all failures using the same categories, but extending them to add one or more categories for failures which cannot contribute to an accident.

When you understand the risk, you should look for measures of controlling the risk. Remember that the measures you put in place can introduce additional hazards that need to be taken into account.
15.5 Related guidance

Chapter 12 describes the maintenance of a Hazard Log, which will act as a repository for risk assessment data. It also provides guidance on managing assumptions, dependencies and caveats (ADCs).

Chapter 14 provides guidance on defining the boundaries of a system as a prerequisite to risk assessment.

Chapter 15 explains how risk assessment is used to set safety requirements in general and Safety Integrity Levels in particular.

Appendix C provides supporting checklists.

Appendix E describes some relevant techniques.
Chapter 16

Monitoring risk

Fundamental from volume 1: Monitoring risk

Your organisation must take all reasonable steps to check and improve its management of risk. It must look for, collect and analyse data that it could use to improve its management of risk. It must continue to do this as long as it has responsibilities for safety, in case circumstances change and this affects the risk. It must act where new information shows that this is necessary.

16.1 Guidance from volume 1

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;
- how closely people are following procedures; and
- the circumstances within which the railway operates.

You should consider collecting and analysing data about:

- incidents, accidents and near misses;
- suggestions and feedback from your staff;
- failures to follow standards and procedures;
- faults and wear and tear; and
- anything else which may affect your work.

If safety depends on assumptions and you have access to data which you could use to check these assumptions, then you should collect and analyse these data. If you analyse incidents, accidents and near misses, you should look for their root causes because preventing these may prevent other problems as well.

You should ask your staff to tell you about safety problems and suggest ways of improving safety.

If you are a supplier, you may not be able to collect all of these data yourself. If so, you should ask the organisations using your products and services to collect the data you need and provide them to you.

This fundamental is related to the continuing safety management fundamental above.
16.2 General guidance

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. When you decide what you are going to monitor, you should consider risk to personnel, risk to the public and risk to parts of the railway. When you have decided what you are going to monitor, you should make sure that you do it and communicate the information you gather to those who need it (see Chapter 9).

If your organisation shares responsibility for the railway with other organisations, collecting some of the data that you will need in order to monitor risk is likely to require co-ordination between these organisations. In the UK, for example, RSSB collects data on behalf of all of the organisations involved in running main line services.

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 and near misses. 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 behaviour of the system that you are responsible for in order to improve its behaviour or to react to degradations in its behaviour. 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 data. 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’.

The part of the railway that you are responsible for will be frequently affected by the changes that you plan to make and by changes to other parts of the railway. Some changes are easy to identify but others are subtle and may result in unintended change that could reduce safety if not identified.

Your organisation should decide what things it needs to monitor and then continue to monitor them as long as you maintain 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 railway change. You should decide which other parts of the railway you need to monitor for changes as well.

You should take account of the condition of equipment: if it is nearing the end of its life you may need to monitor it more often. For example, you may need to monitor cables more often if the insulation is starting to break down.

You should decide what data you are going to collect, how you are going to collect it and store it, and how you are going to analyse it to decide whether your work continues to control all of the risk.
It is important to decide who is going to collect and analyse the data and make sure that they do it correctly. It is good practice to share data with other organisations and your suppliers, where it is needed to monitor risk.

You should decide how you are going to use the results of your analysis and who will decide whether to act on the results.

Your organisation should also collect data, so that you can check that the assumptions that you originally made are still valid. See Chapter 12 for guidance on managing assumptions.

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, organisations 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 safety 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.

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for anyone responsible for monitoring levels of risk.

16.3 Additional guidance for projects
There is no specific guidance for projects.

16.4 Additional guidance for maintenance
There is no specific guidance for maintenance.

16.5 Related guidance
Chapter 9 provides guidance on communicating safety-related information.
Chapter 12 provides guidance on managing assumptions.
Part 5

Risk Control Fundamentals
Chapter 17

Reducing risk; Safety requirements

Fundamental from volume 1: Reducing risk
Your organisation must carry out a thorough search for measures which control overall risk on the railway, within its area of responsibility. It must decide whether it is reasonable to take each measure. It must take all measures which are reasonable or required by law. If it finds that the risk is still too high after it has taken all measures, it must not accept it.

Fundamental from volume 1: Safety requirements
Your organisation must set and meet safety requirements to control the risk associated with the work to an acceptable level.

17.1 Guidance from volume 1

17.1.1 Reducing risk
In order of priority, you should look for:

1 ways to get rid of hazards or to reduce their likelihood;
2 ways to contain the effects of hazards; and
3 contingency measures to reduce harm if there is an accident.

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.

See Chapter 15 for the rules used in the UK for deciding when you have done enough.

If you are a maintainer, you should regularly reassess the risk and decide whether you need to do anything more. In many countries you will have a legal duty to do this. In the UK, this duty is set out in section 2 (1) of the Health and Safety at Work etc Act 1974.
17.1.2 Safety requirements

Safety requirements may specify:

- actions to control risk;
- specific functions or features of a railway product or a part of the railway;
- features of maintenance or operation practices;
- features of design and build processes; 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 and clear, and that you can check they have been met. You should check they are being met. If they are not being met, you should do something about it.

17.2 General guidance

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 specification 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 specification should include both what the system must do, and what it must not do.
- The specification should be correct. As a minimum, every requirement should have been verified by both the stakeholder it comes from and someone capable of judging that the system specified is safe.
- The specification 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 verifiable. There should be some process by which the developed software can be checked to ensure 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.

The following is a widely accepted order of precedence for reducing risk:

1. Re-specify or redesign to eliminate hazards or reduce their likelihood.
2. Reduce risk in the design by adding safety features.
3. Reduce risk by adding warning devices.
4 Reduce risk through procedures and training.
5 Reduce risk by adding warning signs and notices.

For any given hazard you should first seek to set safety requirements to eliminate it. Only where this is not possible should you proceed to set safety requirements on the design of the system. And only when all practicable risk reduction has been accomplished on the design should you consider procedures and training as risk reduction options.

Safety requirements may arise directly from requirements within applicable standards that control risk.

You should review the standards which are applicable to your work. If the risk comes completely within accepted standards that define agreed ways of controlling it, evidence that you have met these standards may be enough to show that you have controlled the risk, but before you decide that just referring to standards is enough, make sure that:

- the equipment or process is being used as intended;
- all of the risk is covered by the standards;
- the standards cover your situation; and
- there are no obvious and reasonably practicable ways of reducing risk further.

If a standard does not completely cover the risk, its provisions may still provide a useful starting point for measures that do cover the risk.

You should not just consider standards with which you must comply. If you are looking for measures to control a hazard, you may find tried and tested solutions which will be effective in optional standards.

If at any point you discover that the measures in a standard are not effective for controlling risk when applied as intended, you should bring this to the attention of the body issuing the standard.

17.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

17.4 Additional guidance for maintenance

The way you plan, implement and review your work should make sure that the part of the railway that you are responsible for stays within the parameters required to keep it safe.

17.4.1 Reducing risk through maintenance tasks

When you have collected all of the risk data, you should decide what maintenance work you need to do to control risk. You should also decide when you are going to do it. Examples of maintenance work that you should consider are:

- checking tolerances using calibrated gauges and measuring instruments (sometimes tolerances may be checked by automatic equipment such as track recording equipment);
- examining equipment for damage and wear;
- non-destructive testing;
• observing that equipment does what it is supposed to; and
• running tests.

You should also decide what action should be taken to correct safety problems that you find during maintenance and to restore optimum functionality. Examples include:

• cleaning and adjusting equipment;
• replenishing consumable items;
• refurbishing and replacing worn and damaged parts;
• modifying parts;
• changing the way parts are connected together; and
• taking a part out of use.

When you decide that you need to do something to control a hazard, you should also identify all of the hazards that arise from doing the work and control them as well. Typically, these hazards may affect the safety of your staff and other parts of the railway. You may be able to remove some hazards by changing the way that you do maintenance to remove the opportunity to make mistakes. For instance, if you provide a spanner of the correct size for a task instead of an adjustable spanner, you remove the opportunity to misadjust or damage an asset.

You might need to agree with other organisations how you are going to change a part of the railway or change the way the railway is operated to make sure it is safe enough to maintain. For example, you might have to provide additional facilities or restrict train movements so that your staff can safely access parts of the railway.

When you have put all of these actions into practice, you should regularly review your safety record. The way you monitor risk will help you to decide whether you are still reducing risk to a low enough level (See Chapter 16).

17.4.2 Reducing risk when assets fail

If you are achieving your organisational goals, you should be minimising the number of failures that occur. Where a part of the railway for which you are responsible does fail, it is important that your decisions and the actions you take minimise the effect of the failure on safety.

It is important to understand what constitutes a failure. In the simplest sense, a failure becomes apparent when an asset is unable to deliver one or more of its functions during normal operations. However, you should also look for hidden failures, which are those events that occur that could contribute to a failure when something else happens. If an asset moves outside a defined safety tolerance, it may contribute to a failure. For example, loose permanent way components within a point layout may only become apparent when the point operating equipment fails (see Chapter 16). Ideally, your maintenance programme will address this, although it is not always practicable to do this.
When assets fail, you should make sure that you collect enough information about the circumstances of the failure so that you can identify the cause. When you decide what needs to be repaired, you should consider both the equipment that has failed and other parts of the railway that could have contributed to the failure. To help you to prioritise your response to failures, it is good practice to classify failures based on the risk arising (for example, high-, medium- or low-risk failure). It is also good practice to apply a hazard rating to failures to reflect the context of the failure (such as associated line speed, type and level of traffic and location). Many organisations have created registers of asset types, failure modes and locations to ensure consistency of classification and hazard rating and therefore of prioritisation and failure response.

When you repair an asset, you should restore the defective components to working order within the safety tolerances that apply. This might include adjusting and resetting components or replacing a broken component with a new one. Before you return an asset to service, you should make sure that it safely performs the function for which it is intended.

If you have to make a temporary repair, you should look for additional risk and decide whether you need to make any changes to your maintenance programme or impose restrictions. You should make sure that a permanent repair is completed or arrange for a permanent change to ensure safety. For example, when a broken point switch rail is removed, signalling circuits may have to be temporarily altered. You should make sure that any temporary wiring is clearly identified and maintained until the points are restored to use or a full recovery is made to abolish the points.

17.4.3 Reducing risk to staff

Your organisation should plan your work to reduce risk exposure to staff to an acceptable level. Where safety incidents occur, you should collect enough information about the circumstances so that you can identify the cause. You should encourage your staff and your suppliers to report all safety incidents and near misses that occur. Remember that near misses are a valuable contribution to understanding the circumstances that could lead to accidents.

It is good practice to carry out workplace risk assessments and then review them regularly and whenever circumstances or conditions change.

Many organisations have implemented a ‘Work-safe Procedure’, which encourages personnel to stop work and report if they decide that something is unsafe.

17.4.4 Safety requirements for maintenance

Your safety requirements should be closely linked to your safety planning documents (see Chapter 11) and should define the operating parameters necessary to ensure that assets meet the safety and reliability targets you have set.

For example, if one of your strategic goals is to reduce the number of broken rails, your maintenance strategy may include periodic visual inspections of track, rail-head profile and side-wear gauging, ultrasonic testing of welds and analysis of train wheel-flats using lineside detection systems. It is important to define what is acceptable in terms of condition, gauge and test values, so that you can decide whether the assets for which you are responsible are safe when maintained and will remain safe until the next maintenance takes place.
Your maintenance specifications should clearly describe the safety requirements for each asset that you maintain, and include information about the absolute limits that equipment is designed to operate safely within; it should also describe the preferred operating conditions to ensure performance.

Typical limits and settings could include:

- torque settings for nuts and bolts;
- electrical voltage and frequency ranges, minimum and maximum current levels;
- clearance and proximity gauges;
- visibility and audibility ranges and colour;
- motion settings; and
- time settings.

It is also good practice to set tolerances for your maintenance periodicities so that you can build some flexibility into your planning and anticipate a degree of late maintenance visits, without incurring additional risk.

You should determine absolute safety limits for each component and then decide how much tolerance you should build in to your maintenance specifications to allow for system degradation between each maintenance visit.

Historically recommended settings and maintenance periodicities should be available from standards or from operation and maintenance manuals provided by manufacturers. If you are going to be responsible for maintaining new equipment, you should find out where these are specified. The tolerances you set and the risks that you have to control will influence how frequently you will maintain the equipment that you are responsible for.

It is good practice to apply risk-based maintenance techniques to help you decide what to do and when to do it. This technique considers how assets can fail and the consequence in terms of safety and cost compared with implementing maintenance tasks. This should allow you to tailor your maintenance specifications and maintenance periodicities to cater for different levels of risk (for example, high risk, medium risk and low risk). This will help you to use your maintenance resources more efficiently and reduce risk to your maintenance staff by reducing their exposure to the railway environment.

Some types of asset may also benefit from a condition-based maintenance regime, particularly where asset age, location and use varies. In this case, the maintenance that you do and the frequency that you do it should be related to wear and the age of the asset.

If you decide to set a single maintenance specification and maintenance periodicity for each different asset type, you should make sure that the worst-case degradation is taken into account.

### 17.5 Related guidance

Chapter 11 provides guidance on safety planning.

Chapter 15 provides guidance on the safety analysis processes which should be carried out before setting safety requirements.

Chapter 16 provides guidance on monitoring risk.
Chapter 18

Evidence of safety; Acceptance and approval

Fundamental from volume 1: Evidence of safety

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

Fundamental from volume 1: Acceptance and approval

Your organisation must obtain all necessary approvals before it does any work which may affect the safety of the railway.

18.1 Guidance from volume 1

18.1.1 Evidence of safety

You should show that:

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

You should check that the evidence for your conclusions is reliable. You should record and check any assumptions 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 have accepted responsibility for doing it.

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

The arguments and evidence for safety are often presented in a Safety Case. The type of Safety Case you should prepare will depend on what you are doing.
If you are maintaining a part of the railway covered by a Safety Case, you should tell whoever is responsible for the Safety Case about any changes which might affect it or any events which might show that it is wrong. You should take account of the activities described in the monitoring risk fundamental when doing this.


18.1.2 Acceptance and approval

You may need approval from the railway Safety Authority (HMRI in the UK). Safety Approval will normally be based on accepting the Safety Case or a report accompanied by the technical file.

The Safety Approver may produce a certificate, setting out any restrictions on how the work is carried out or how the railway can be used afterwards.

You may also need to agree with the organisation that manages the infrastructure or those that operate trains that the risk has been properly controlled.

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 Safety Approval. Large or complicated projects may need additional approval before they change the railway – for example, for a Safety Plan or for safety requirements.

If you are maintaining the railway, you may need to get your maintenance plans and procedures approved before you put them into action. You may also need approval to put the equipment you have been working on back into service or to bring plant and equipment onto the railway.

18.2 General guidance

When planning or carrying out work on the railway, it is necessary to gain Safety Approval for the work from one or more Safety Approvers. The Safety Approvers may be within your organisation or outside it, or both. You should identify the Safety Approvers for the change you are making (see section 2.4.1 above).

To find out who the Safety Approvers are, you should:

- Check your own organisation’s requirements.
- Consult the procedures which apply on the railway that you are changing.
- Consult the guidance provided on national and international approval requirements (for example, in the UK, the Office of Rail Regulation’s (ORR’s) document ‘The Railways and Other Guided Transport Systems (Safety) Regulations 2006 Guidance on Regulations’ [F.3] and the ‘Railways (Interoperability) Regulations 2006 Guidance’ [F.4].

The guidance in this chapter is applicable to all phases in the System Lifecycle.

This chapter is written for:

- anyone compiling a document presenting safety evidence; and
- anyone reviewing such a document.
18.2.1 Limitations of this guidance

In the UK, the 'Railways (Interoperability) Regulations 2006' and the 'Railways and Other Guided Transport Systems (Safety) Regulations 2006' ('ROGS regulations') both require approval of railway works but define processes which are different in some respects from the project guidance in this chapter.

These are not the only relevant pieces of UK legislation. See volume 1, section 2.1, for further information.

The law takes precedence over guidance such as the Yellow Book. If your work falls within the scope of legislation you should follow the guidance associated with the legislation. In case of conflict with the guidance in the Yellow Book, the guidance associated with the legislation will take precedence. At the time of writing, the interpretation of the Interoperability regulations and ROGS regulations was evolving, so, if you refer to guidance on the legislation, you should make sure that you have the latest version.

We intend, in the next version of Yellow Book, to make the guidance on putting the Acceptance and approval fundamental into practice fully consistent with the requirements of the Interoperability regulations and ROGS regulations and the guidance on these regulations issued by the DfT and the ORR.

18.2.2 Adapting this guidance

The project guidance in this chapter is designed for a situation where risk cannot be controlled completely by applying standards. If the risk comes completely within accepted standards that define agreed ways of controlling it (see section 2.4.3), then the Evidence of safety fundamental may be put into practice in different ways, for instance by relying on processes which provide assurance of compliance with these standards.

If you are making a change to the railway, you should agree with your Safety Approvers how you will present the evidence for the safety of this change. This volume provides guidance on the compilation of this evidence into a Safety Case. A Safety Case is one way of presenting this evidence which is good practice in certain circumstances. But there are other ways of presenting evidence for safety which are also effective. Some organisations:

- use different names for such a document, including ‘Case for Safety’ and ‘Safety Report’;
- make a distinction between documents whose evidence is based on demonstration and those whose evidence rests primarily on analysis; or
- present evidence for safety in the same document as evidence for compliance with non-safety requirements.

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

If the work you are doing comes completely within your organisation’s Safety Management System, then the provisions of this Safety Management System may put the fundamental into practice.
It is perfectly possible to implement the Evidence for safety fundamental fully while using the terminology and practices described above and, indeed, in other ways as well. You may still find the guidance in this section useful if your organisation chooses to present evidence for safety in a different way, but you should be prepared to modify the guidance to suit your practices.

However you present evidence for safety and whoever your Safety Approvers are, you should plan to collect this evidence and agree it with your Safety Approvers as the project proceeds. Ideally, you and your Safety Approver 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.

18.3 Additional guidance for projects

This section has been removed from this version but is available in the full version of the Yellow Book.

18.4 Additional guidance for maintenance

18.4.1 Evidence of safety

Good maintenance organisations make sure that safety requirements are met and look for ways of improving safety further. It is good practice to monitor the safety of the work that you do and the safety of the railway (see Chapter 16) to gather evidence that you are safe enough.

Examples of things to look for include:

- completeness of failure investigations;
- improving failure trends;
- a reduction in staff safety incidents and near misses;
- achievement of your plans for safety;
- demonstrating that you are complying with standards and legal requirements; and
- meeting your safety targets.

It is good practice to make someone responsible for looking for evidence of safety. You should make sure that the evidence that you gather gives a true representation of safety.

18.4.2 Existing approvals

If you are already maintaining a part of the railway, you should understand what approvals you already have. Where your work is already approved, you may not have to look for approval unless you decide that you need to change something.

If you find that you are doing something that is not approved, you should compare what you are doing with the standards that tell you what you should be doing. If you find a difference, you should either change what you do to comply with the standard or look for approval to continue what you are doing. You might have to request a non-compliance or derogation to do this.
18.4.3 Making changes to what you do

Before you start your maintenance work or implement a change, you should make sure that you have all the necessary approvals. You might have to produce a Safety Case to demonstrate that you have done enough to reduce risk on the railway and that your work can be done safely. You should look for standards that tell you which approvals you need.

If you have to produce any evidence of safety, you should consider all of the fundamentals in this volume and use the guidance to help you to put it together. If you have met all of the safety fundamentals, you should be able to demonstrate that you are safe enough.

You should obtain approvals for:

- your maintenance strategy; maintenance specifications and method statements;
- your maintenance programmes; and
- your organisation structure.

Your organisation should understand who is responsible for approving the work that you do. The person responsible for approving your work should have sufficient competence and experience to be able to use their professional judgment to decide whether the work will be safe enough.

In some cases, your organisation will be able to approve some types of work. In this case, you should give someone the responsibility and authority necessary to do this. For example, someone should be given responsibility for approving your maintenance programmes. The person giving approval should make sure that the maintenance programme is capable of fulfilling the maintenance strategy and addresses all of the required assets.

Where you cannot meet the requirements set down in a standard, you should apply for a non-compliance or derogation and provide the evidence to show that you have alternative measures in place to manage risk to a low enough level. You should make sure that the non-compliances and derogations are approved before you go ahead with the affected work.

18.5 Related guidance

Chapter 11 provides guidance on an appropriate programme of Human Factors activities.

Chapter 12 provides guidance on managing assumptions.

Chapter 16 provides guidance on monitoring risk.

Chapter 17 provides guidance on establishing safety requirements.
Appendices
Appendix A

Glossary

This glossary defines the specialised 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 minimise 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.

A.1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>Assumption, Dependency, Caveat</td>
</tr>
<tr>
<td>ALARP</td>
<td>As Low As Reasonably Practicable</td>
</tr>
<tr>
<td>BCS</td>
<td>British Computer Society</td>
</tr>
<tr>
<td>CFC</td>
<td>Chlorofluorocarbons</td>
</tr>
<tr>
<td>CIRAS</td>
<td>Confidential Incident Reporting and Analysis System</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off The Shelf</td>
</tr>
<tr>
<td>CTRL</td>
<td>Channel Tunnel Rail Link</td>
</tr>
<tr>
<td>DfT</td>
<td>Department for Transport</td>
</tr>
<tr>
<td>DRACAS</td>
<td>Data Reporting Analysis and Corrective Action System</td>
</tr>
<tr>
<td>[E]EPROM</td>
<td>[Electrically] Erasable Programmable Read-Only Memory</td>
</tr>
<tr>
<td>ESM</td>
<td>Engineering Safety Management</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Mode and Effects Analysis</td>
</tr>
<tr>
<td>FMECA</td>
<td>Failure Mode, Effects and Criticality Analysis</td>
</tr>
<tr>
<td>FRACAS</td>
<td>Failure Reporting Analysis and Corrective Action System</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>GSN</td>
<td>Goal Structuring Notation</td>
</tr>
<tr>
<td>HAZOP</td>
<td>Hazard and Operability Study</td>
</tr>
<tr>
<td>HMRI</td>
<td>Her Majesty’s Railway Inspectorate</td>
</tr>
<tr>
<td>HSE</td>
<td>Health and Safety Executive</td>
</tr>
<tr>
<td>IET</td>
<td>Institution of Engineering and Technology</td>
</tr>
<tr>
<td>IMechE</td>
<td>Institution of Mechanical Engineers</td>
</tr>
</tbody>
</table>
A.2 Specialised terms

Specialised terms are written in initial 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**
An unintended event or series of events that results in harm.

*Note: this broadly corresponds to a ‘hazardous event’ in the RSSB Safety Risk Model.*

**accident likelihood**
The likelihood of an accident occurring. May be expressed as numeric probability or frequency or as a category.

**accident sequence**
A potential progression of events that result in an accident.

**accident severity**
A measure of amount of harm. May be expressed as a financial value or as a category.

**Accident Trigger**
A condition or event which is required for a hazard to give rise to an accident.

*Note: this broadly corresponds to a ‘precursor (consequence)’ in the RSSB Safety Risk Model.*

**ALARP Principle**
The principle, applicable to some safety decisions in the UK, that no risk in the Tolerability Region can be accepted unless reduced to ‘As Low As Reasonably Practicable’.

*See Chapter 15.*
| **Barrier** | (In the context of risk assessment) anything which may act to prevent a hazard giving rise to an accident. Barriers may be physical, procedural or circumstantial. |
| **Causal Factor** | Any event, state or other factor which might contribute to the occurrence of a hazard. |
| **compliance** | A demonstration that a characteristic or property of a system, product or other change satisfies the stated requirements. |
| **consequence** | The results arising from the addition of energy, or exposure, to a hazard. These may range from benign results to accidents. Several consequences may be associated with a hazard. |
| **Data Reporting, Analysis and Corrective Action System (DRACAS)** | A closed-loop system for ensuring that failures and other incidents are thoroughly analysed and that any necessary corrective action, particularly if it affects safety, is identified and carried through.  
*See appendix E.* |
| **endorse** | Approve a document, piece of equipment, etc, as being fit for purpose. |
| **Engineering Safety Management (ESM)** | The activities involved in making a system, product or other change 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** | A deviation from the intended design which could result in unintended system behaviour or failure. |
| **event** | A significant happening that may originate in the system, product or other change or its domain. |
| **Event Tree Analysis** | A method of illustrating the intermediate and final outcomes which may arise after the occurrence of a selected initial event. |
| **failure** | A 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)** | A process for hazard identification where all known failure modes of components or features of a system, are considered in turn and undesired outcomes are noted.  
*See appendix E.* |
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Appendix A</th>
</tr>
</thead>
</table>
| **Failure Mode, Effects and Criticality Analysis (FMECA)** | An extension to FMEA in which the criticality of the effects is also assessed.  
*See appendix E.* |
| **Failure Reporting, Analysis and Corrective Action System (FRACAS)** | Another name for Data Reporting, Analysis and Corrective Action System |
| **fault** | A fault is a defect in a system, product or other change which may cause a failure. |
| **Fault Tree Analysis (FTA)** | A method for representing the logical combinations of various states which lead to a particular outcome (top event).  
*See appendix E.* |
| **Goal Structuring Notation (GSN)** | A method for representing safety arguments in diagrammatic form.  
*See appendix E.* |
| **handover** | Used to mean the process of handing over part of the railway to the Infrastructure Manager so that it can put into, or back into, service.  
*Note: this process is referred to as ‘Handback’ within the main line railway.* |
| **hazard** | A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product.  
*Note: this broadly corresponds to a ‘precursor (cause)’ in the RSSB Safety Risk Model.* |
| **Hazard and Operability Study (HAZOP)** | A study carried out by application of guide words to identify all deviations from the design intent with undesired effects for safety or operability.  
*See appendix E.* |
| **Hazard Log** | A document which records details of hazards and potential accidents identified during safety analyses of a system, product or other change and logs safety documentation produced. |
| **Head of Safety** | A person responsible for dealing with general safety issues throughout an organisation. |
| **Human Factors** | The 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. |
| **incident** | Unplanned, uncontrolled event, which under different circumstances could have resulted in an accident. |
Individual Risk
The Individual Risk experienced by a person, is their probability of fatality per unit time, usually per year, as a result of a hazard in a specified system.

Infrastructure Manager
An organisation responsible for managing railway infrastructure.

Intolerable Risk
A risk which cannot be accepted and must be reduced.

loss
A measure of harm.

maintenance
The activities that need to be carried out to keep a system fit for service, so that assets (sub-systems, components and their parts) continue to be safe and reliable throughout the operational lifecycle phase.

Potential Equivalent Fatality (PEF)
A convention for aggregating harm to people by regarding major and minor injuries as being equivalent to a certain fraction of a fatality.

Project Manager
The person in overall control of a project. Also responsible for the safety of the products produced during the project, although may delegate this role to a Project Safety Manager (but remains accountable).

Project Safety Manager
The person responsible for safety on a project and for producing all safety-related documentation.

Random Failure
A failure resulting from random causes such as variations in materials, manufacturing processes or environmental stresses.

reliability
The probability that an item can perform a required function under given conditions for a given time interval.

remit
Terms of reference, in particular for a Safety Audit or Safety Assessment.

Right-side Failure
A failure which does not result in the protection provided by a signalling system being reduced.

risk
Combination of the likelihood of occurrence of harm and the severity of that harm.

risk assessment
Making an assessment of the risk arising from one or more hazards.

Risk Assessment Report
A document containing an analysis of the risk arising from one or more hazards.

safety
Freedom from unacceptable risk.

Criteria for accepting risk are described in Chapter 15.
safety analysis  A general term encompassing identifying hazards, analysing hazards and assessing risk.

Safety Approval  Any process by which someone reviews the evidence that risk has been controlled and takes an explicit decision as to whether it has been controlled to an acceptable level or not.

Note: some other people distinguish different sorts of approval and give some sorts different names, such as ‘acceptance’ or ‘endorsement’.

Safety Assessment  The process of analysis to determine whether a system, product or other change to the railway has met its safety requirements and that the safety requirements are adequate.

Safety Assessment Remit  A form capturing a request for a Safety Assessment and the terms of reference.

Safety Assessment Report  A report on the activity carried out to check that the safety requirements are being met on a project.

Safety Assessor  The person who carries out Safety Assessments.

Safety Audit  An activity to check and ensure that a project is being run according to its Safety Plan. It will also address the adequacy of the Safety Plan.

Safety Audit Remit  A form capturing a request for a Safety Audit and the terms of reference.

Safety Audit Report  A report on the activity carried out to check that the Safety Plan and safety management procedures are being carried out on a project.

Safety Auditor  The person appointed to carry out Safety Audits on a project.

Safety Approver  Any individual or body from whom Safety Approval must be sought before a change to the railway may be put into service.

Note: a Safety Approver may be part of your own organisation or of a different organisation.

Safety Authority  A body appointed by government with statutory authority for railway safety.

The ORR is a safety authority in the UK.
<p>| <strong>Safety Case</strong> | A formal presentation of evidence, arguments and assumptions aimed at providing assurance that a system, product or other change to the railway has met its safety requirements and that the safety requirements are adequate. <em>Early issues may present analysis and assessment information, plans and requirements.</em> |
| <strong>Safety Certificate</strong> | A certificate authorising system, product or other change for use. |
| <strong>Safety Control</strong> | A quality control with the potential to reveal hazardous faults. |
| <strong>Safety Engineering</strong> | The application of technical methods to ensure achievement of the safety requirements. |
| <strong>Safety Integrity</strong> | The likelihood of a system, product or other change satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. |
| <strong>Safety Integrity Level (SIL)</strong> | Discrete level (1 out of a possible 5) for specifying the Safety Integrity requirements of the safety functions to be allocated to a system, product or component, where Safety Integrity Level 4 has the highest level of Safety Integrity, and Safety Integrity Level 0 is reserved for functions which are not relied upon at all to control risk. |
| <strong>Safety Lifecycle</strong> | The additional series of ESM activities carried out in conjunction with the System Lifecycle for safety-related systems. |
| <strong>Safety Management System</strong> | A systematic and documented approach to managing safety. |
| <strong>Safety Plan</strong> | A document detailing the activities to be carried out, and responsibilities of people to ensure the safety of work being carried out. |
| <strong>safety planning</strong> | An activity to define the activities to be carried out and the staff responsibilities to be assigned to ensure the safety of work to be carried out. Results in the preparation of a Safety Plan. |
| <strong>Safety Records Log</strong> | A reference to every safety document produced and used by a project. |
| <strong>Safety Requirements Specification</strong> | Specification of the requirements that a product, system or change to the railway must satisfy in order to be judged safe. |
| <strong>safety standard</strong> | A document which establishes criteria or requirements by which the safety of products or processes may be assessed objectively. |</p>
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Appendix A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety Value</strong></td>
<td>The monetary value of reductions in safety losses likely to be achieved by implementation of a risk mitigation option.</td>
</tr>
<tr>
<td>safety-related</td>
<td>An item is safety-related if any of its features or capabilities has the potential to contribute to or prevent an accident.</td>
</tr>
<tr>
<td>severity</td>
<td><em>See accident severity.</em></td>
</tr>
<tr>
<td>standard</td>
<td>An authorised document, including specification, procedure, instruction, directive, rule or regulation, which sets requirements.</td>
</tr>
<tr>
<td>System Lifecycle</td>
<td>A sequence of phases through which a system can be considered to evolve.</td>
</tr>
<tr>
<td>system supplier</td>
<td>Any organisation supplying systems or products to be used on the railway.</td>
</tr>
<tr>
<td>Systematic Failure</td>
<td>Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.</td>
</tr>
<tr>
<td>Tolerability Region</td>
<td>A region of risk which is neither high enough to be unacceptable nor low enough to be broadly acceptable. Risks in this region must be reduced ALARP (see ALARP Principle).</td>
</tr>
<tr>
<td>Transport Operator</td>
<td>An Infrastructure Manager or Transport Undertaking.</td>
</tr>
<tr>
<td>Transport Undertaking</td>
<td>An organisation that operates passenger or freight train services.</td>
</tr>
<tr>
<td>Upper Limit Of Tolerability</td>
<td>A measure of the average Individual Risk of fatality per annum, defined for each group, and representing the boundary between tolerable and Intolerable Risk for the group.</td>
</tr>
<tr>
<td>Value of Preventing a Fatality (VPF)</td>
<td>A defined monetary figure which is used to indicate what it is regarded as necessary to spend in the expectation of preventing a single fatality.</td>
</tr>
<tr>
<td>Wrong-Side Failure</td>
<td>A failure that results in the protection provided by a signalling system being reduced or removed.</td>
</tr>
</tbody>
</table>
Appendix B

Document outlines

This appendix has been removed from this version but is available in the full version of the Yellow Book.
Appendix C

Checklists

This appendix provides checklists to support the following activities:

1. Hazard Identification and Risk Assessment (see Chapter 15)
2. Safety planning (see Chapter 11)
3. Updating the Hazard Log (see Chapter 12)
4. Maintenance

There are also checklists in appendix D which support audit and assessment.
C.1 Hazard identification and risk assessment

C.1.1 Hazard identification checklists

Example checklists are supplied below which may be used if there are no existing, well-established checklists. They may be applied to the whole system or to a component of it. Each item should be interpreted as widely as circumstances permit in the endeavour to unearth possible hazards. No checklist can be exhaustive and the analyst should bring his or her full experience to bear in searching for hazards.

The Functional Checklist should be applied to a functional specification of the item being considered in an attempt to unearth hazards arising from unspecified functionality or specified functionality in unforeseen circumstances:

a) Alarms and warnings,
b) Indication of failure,
c) Interlocks,
d) Maintenance and support,
e) Point setting,
f) Signal aspects,
g) Terrorist action,
h) Software malfunction,
i) Software crash.

The Mechanical Checklist should be applied to mechanical drawings to unearth hazards involving physical interactions:

a) Corrosion,
b) Cryogenic fluids,
c) Derailment,
d) Exhaust gases,
e) Fire,
f) Foreign bodies and dust,
g) Insect, rodent or mould damage,
h) Lasers,
i) Overheating,
j) Pressure systems,
k) Shock and vibration,
l) Vandalism,
m) Ventilation.

The Construction Checklist should be applied to civil engineering drawings and plans to unearth construction hazards:

a) Access hazards at site,
b) Site preparation hazards,
c) Construction hazards,
d) Environmental effects,
e) Vandalism,
f) Interference with normal railway operating procedures,
g) Training and control of contractors.
The **Electrical Checklist** should be applied to circuit diagrams to unearth hazards involving electrical interactions:

a) Electromagnetic interference and compatibility,
b) Fire and explosion initiation,
c) Insulation failure,
d) Lightning strikes,
e) Loss of power,
f) Traction current,
g) Protection against earth faults,
h) Indirect and direct contact,
i) Emergency switching and isolation,
j) Overcurrent protection and effects of disconnection,
k) Current rating.

The **Operation and Support Checklist** should be applied to operating and maintenance instructions to unearth hazards occurring during, or triggered by, operating and maintenance activities:

a) Accessibility for maintenance,
b) Documentation,
c) Failure to activate on demand,
d) Human Factors,
e) Inadvertent activation,
f) Lighting,
g) Manuals,
h) Spares,
i) Training,
j) Start-up,
k) Close down,
l) Re-setting.

The **Occupational Health Checklist** should be applied to a general description to unearth hazards to personnel installing, operating, maintaining or disposing of the item:

a) Asbestos,
b) Asphyxiates,
c) CFCs (Chlorofluorocarbons),
d) Corrosive materials,
e) Cryogenic fluids,
f) Electrocution,
g) Exhaust gases,
h) Fire,
i) High temperatures,
j) Injury from moving parts,
k) Lasers,
l) Noise,
m) Pressure systems,  
n) Radioactive materials,  
o) Toxicity,  
p) Electrical overheating.

C.1.2 Operation and maintenance responsibilities checklist

This checklist may be used to assist in thorough control of risks related to operation and maintenance.

Actions to be taken by the Project Manager:
   a) Define responsibilities for operation and support in project requirements;  
   b) Establish communications on operation and support with users.

Operating Information and Documentation checklist:
   c) Provide operating instructions prior to commissioning, emphasising safety aspects and precautions, as appropriate;  
   d) Consider need to alter current operating instructions and advise Users accordingly;  
   e) Include instructions to be followed in event of system or equipment failure;  
   f) Include instructions to be followed to render system safe and to maintain operational capabilities, where possible;  
   g) Include instructions to be followed in the event of an accident resulting from a system or equipment failure;  
   h) Define requirements for review and exercising of the safety aspects of operating instructions.

Operator interface design checklist:
   i) Consider safety aspects of man-machine interface in system or equipment;  
   j) Check that required operating tasks are within intended operators' physical and mental capabilities;  
   k) Ensure that implications of emergency actions are clearly defined in operating instructions.

Operational safety features checklist:
   l) Check that operator safeguards have been considered;  
   m) Check clarity of instructions for operator safety systems;  
   n) Consider requirements for periodical safety checks, by operating and maintenance personnel.

Operational Record checklist:
   o) Determine requirements for failure reporting;  
   p) Issue instructions for the recording and analysis of failures;  
   q) Define procedures for the incorporation of alterations to systems and equipment for safety reasons.
Checklists

Operator Training and Competence checklist:
   r) Determine requirements for operator safety training;
   s) Consider need for training aids and facilities;
   t) Define skill levels and calibre of operators and maintainers.

Maintenance Instructions checklist:
   u) Provide maintenance specifications and identify safety-related requirements;
   v) Define fault-diagnosis, condition monitoring and test equipment;
   w) Provide maintenance task instructions;
   x) Define skill levels required;
   y) Provide maintenance schedules;
   z) Provide a maintenance recording system;
   aa) Provide a defect reporting system;
   bb) Provide a system for the incorporation of changes to a design.

System Definition and Spares Identification checklist:
   cc) Create a database of system and equipment support information;
   dd) Identify safety aspects of spares and support equipment;
   ee) Define safety requirements for packaging, handling, storage and transport of spares.

Maintenance Specifications and Mandatory Items checklist:
   ff) Identify mandatory preventive maintenance;
   gg) Define Data Reporting, Analysis and Corrective Action system;
   hh) Designate team of specialists for monitoring data reports.

Safe Maintenance Practices and Accessibility checklist:
   ii) Provide instructions for gaining safe access to systems for repairs;
   jj) Provide instructions for the promulgation of safety precautions;
   kk) Provide instructions for a 'permit-to-work' procedure.

Change Control checklist:
   ll) Establish procedures for the safe management of changes and alterations to systems;
   mm) Define requirements for testing and commissioning after changes have been incorporated.

Checklist of regulations and guidance on safety in operation and support:
   nn) DD IEC/TS 60479-1:2005 [F.32];
   oo) EN 41003:1999 [F.33];
   pp) IEE Wiring Regulations 16th edition (BS 7671:2001) [F.34];
C.1.3 Checklist of decommissioning/disposal considerations

This checklist may be used to assist in thorough control of risks related to decommissioning and disposal.

Checklist of actions to be completed:

a) Has the hazard listing identified possible hazards in decommissioning, dismantling and disposal?

b) Has the hazard analysis classified the severity or consequences of any potential accidents in decommissioning or disposing of a system or equipment at the end of its life?

c) Has the system been designed to eliminate potential hazards of disposal?

d) Has guidance for the safe disposal of systems and equipment been included in the Hazard Log and the Safety Case?

e) Does the Safety Plan cover the decommissioning of systems and equipment?

f) Is there any risk due to interaction between a decommissioned system and any remaining systems?

g) If any parts of systems have been designated for salvage on decommissioning, have instructions for re-certification been prepared?

h) Are all decommissioning and disposal procedures defined along with any special testing requirements they imply?

Checklist of hazardous components (not exhaustive):

i) Flammable substances,

j) Explosives,

k) Asphyxiates, toxic, corrosive or penetrating substances,

l) Allergenic substances,

m) Pressurised systems,

n) Electrical sources or batteries,

o) Radiation sources,

p) Rotational machinery, moving parts,

q) Hazardous surfaces,

r) Cutting edges and sharp projections,

s) Heavy weights.

C.1.4 Checklists of installation and handover considerations

This checklist is intended to be used to check whether or not all required safety management activities have taken place prior to Safety Approval:

a) Have any incidents with safety implications been reported during the site trial?

b) Has the Safety Case been updated to reflect the validation activities?

c) Has the Safety Case been reviewed by the Safety Assessor and issued for approval?
C.2 Safety planning

This section has been removed from this version but is available in the full version of the Yellow Book.

C.3 Updating the Hazard Log

This section has been removed from this version but is available in the full version of the Yellow Book.

C.4 Maintenance

C.4.1 Suggested contents of job descriptions

The job description / safety responsibility statement should contain information such as:

a) the scope of work activity, including information about boundaries and asset registers;

b) where the post fits into the organisation hierarchy;

c) responsibilities for collecting and passing on information about safety;

d) personal safety responsibility and safety responsibility for others;

e) safety responsibility allocated to others associated with the work;

f) safety decision making authority;

g) deputising arrangements;
h) competence and certification requirements for safety;  
  i) safety equipment; and  
  j) controlled safety documentation issued to the post holder and the source of  
other controlled documents.

C.4.2 Suggested competence and fitness requirements

Personnel who are responsible for doing maintenance work:

a) knowledge and experience of the railway parts that they maintain and the way  
   they interface with other parts of the railway;  
  b) knowledge of safety procedures (including any 'work safe' procedures);  
  c) knowledge of maintenance procedures;  
  d) an ability to safely do maintenance work in accordance with the requirements,  
   including use of tools and materials;  
  e) an understanding of how the maintenance work that they do could affect the  
   safe operation of the railway;  
  f) an ability to identify failures or degradation that could reduce safety;  
  g) knowing how to respond to incidents;  
  h) an ability to communicate information about work, including information about  
   work status and safety risk;  
  i) knowledge of the limits of their safety responsibility and the safety responsibility  
   of others; and  
  j) an ability to work as part of a team.

Fitness should include:

k) appropriate physical strength (including stamina and manual-handling abilities);  
  l) mobility;  
  m) eyesight; and  
  n) hearing.

People who take decisions about safety:

a) knowledge of the parts of the railway they are responsible for;  
  b) knowledge of the information that is required to take decisions and where to find  
   it;  
  c) knowledge of standards and legislation that influence decisions;  
  d) an understanding of how the safety risk being managed could affect other parts  
   of the railway;  
  e) an ability to assess risk;  
  f) an ability to take correct decisions based on the information available;  
  g) confidence and integrity to defend their decisions;  
  h) an ability to communicate decisions to others who need to know; and  
  i) an ability to make sure that required work is implemented properly.
C.4.3 **Examples of communications required for maintenance**

Examples of information that starts at the front line of a maintenance organisation:

a) details of completed work;

b) details of additional reports and maintenance work requirements;

c) test results;

d) requests for authorisation to proceed with work;

e) details of problems affecting completion of work; and

f) reports of safety hazards.

Examples of information that should be communicated through a maintenance organisation and with your suppliers:

a) information about changes to maintenance procedures and standards;

b) information about work being done on other parts of the railway that may affect your work;

c) details of required work;

d) details of required special inspections;

e) technical information that is relevant, including results of special investigation reports, audits, inspections and reviews;

f) information about safety hazards and safety alerts;

g) changes to organisation and reporting lines;

h) changes to safety rules; and

i) changes to the part of the railway you are responsible for.

Examples of information that is passed between maintenance organisations include:

a) details of failures and hazards that affect more than one part of the railway; and

b) details of work in progress where more than one maintenance organisation is involved at a maintenance boundary.

Examples of information that passes between a project and a maintenance organisation:

a) information that the project needs from the maintenance organisation, so that the project can be safely implemented; and

b) information that the maintenance organisation needs from the project, so that the maintenance requirements contained in the engineering Safety Case can be implemented.

C.4.4 **Suggested contents for an incident response plan**

A safety incident plan should include information about:

a) what the incident plan covers (such as SPAD and ‘Wrong-Side Failure’ investigation), what information needs to be collected, secured and recorded;

b) how you will manage safety and security when an incident occurs; how you will obtain and manage the resources you will need; how information will be collected, secured, recorded and communicated to those who need to take decisions;
c) when you will implement the plan;

d) who will be responsible for co-ordinating incident response; who will be responsible for making decisions and providing resources to do the work;

e) with - the resources that you have identified that are necessary to manage the incident;

f) where the resources can be obtained from; and

g) why - your organisational target, such as response time.

C.4.5 Detailed maintenance programmes

Your maintenance programme should address:

a) what work you are going to do;

b) how the work will be done and recorded;

c) where you will do the work;

d) when the work will be done, including timescales and safety priority;

e) who will do the work, who will check the work and who is responsible for making sure the work is completed on time;

f) with – list the tools, equipment and materials required for the work; and

g) why the work is being done, such as relating to a company target or standard.

C.4.6 Suggested records required for failure management

Examples of the records you should keep include:

a) details of the reported event (who reported it, what the symptoms were and when the failure was found);

b) details of the investigation;

c) the results of the investigation;

d) the root cause of the event;

e) the level of risk caused by the event;

f) who was responsible for the investigation;

g) who decided what action to take; and

h) how the risk was eliminated or mitigated.
C.4.7 Suggested maintenance records

For recording what maintenance you are going to do, examples of good practice include:

a) formal work orders;
b) activity specific method statements;
c) maintenance test plans;
d) failure investigation test plans and checklists;
e) maintenance specifications, including tests;
f) equipment manuals and technical handbooks;
g) inspection and surveillance checklists.

For maintenance that you have done:

Examples of what you should record include:

a) the date you maintained it;
b) what maintenance you have done;
c) the results of measurements and tests;
d) the status of any additional work that was required; and
e) details of outstanding defects.

Examples of good practice for recording work done include:

a) maintenance record cards and logbooks that are kept with the asset;
b) completed work orders that record the status of work and additional requirements;
c) checklists to record actions taken and information collected (such as failure investigation checklists);
d) marked-up drawings with dates and signatures (such as testing copy drawings);
e) verbal reports to a central control point (for instance, a fault control); and
f) electronic reporting using portable IT equipment, which can then be downloaded to a database.

Examples of good practice for recording use of resources include:

a) the people involved in planning, doing and checking the work and their competence;
b) the test and measuring equipment used, including reference to calibration data; and

c) the materials used to support traceability and configuration management.

C.4.8 Suggested content for a maintenance audit

When you audit maintenance, you should check that:

a) you are using a complete, accurate and up-to-date asset register;
b) an up-to-date Hazard Log is available;
c) sufficient competent staff are available and consistently allocated to safety-critical work;
d) correct resources (materials, calibrated tools and equipment) are obtained from approved suppliers, available and used correctly during maintenance work;

e) tools and equipment are correctly used;

f) detailed maintenance programmes are planned and delivered in accordance with your organisation maintenance strategy;

g) planned changes are fully justified;

h) where maintenance programmes are not fulfilled, changes to the maintenance programmes are fully supported by justified safety decisions;

i) the people doing the maintenance work are complying with the relevant maintenance specifications, method statements and safety procedures;

j) the maintenance specifications and safety procedures, when properly applied, control risk to the required level. This includes checking that the part of the railway is safe and the way your personnel do the maintenance work is safe;

k) all of the correct maintenance records are being managed to allow information about maintenance to be traced and reused;

l) your maintenance is achieving the required outcome;

m) supervision and inspection plans comply with your organisation maintenance strategy;

n) surveillance is effective and any actions are being managed; and

o) interfaces to other parts of the railway are understood and managed safely, including handover and hand-back between maintenance and projects.

C.4.9 Suggested data to be collected to support monitoring

Examples of data that you should collect include:

a) data about how well you are meeting your maintenance plan;

b) data about the quality of your maintenance work;

c) data about asset condition;

d) data about repair and rectification work arising from maintenance visits;

e) data about failures in parts of the railway that you are responsible for;

f) data about failures in other parts of the railway that could be connected to your work;

g) data about safety incidents, accidents and near misses involving personnel;

h) data about how well your staff personnel are complying with your procedures and instructions

i) data about safety that you are given, including feedback from your own staff and information that other organisations give to you.

j) the type, speed and density of rail traffic;

k) the way the railway is managed; and

l) the effect of the environment on your maintenance work and the part of the railway you maintain.
C.4.10 Suggested data to be stored in an asset register

Examples of data that you should store include:

a) asset types;
b) asset locations;
c) size of asset populations;
d) the status of temporary alterations and adjustments;
e) the service duty and condition of strategic assets;
f) how each asset is used, particularly where the number of operations is related to an asset servicing or replacement regime;
g) the configuration status of spare parts to make sure that when they are used, they are of the correct type and modification state; and
h) the availability, location shelf life of spare parts (including strategic spares managed by your suppliers).
Appendix D

Examples

This appendix has been removed from this version but is available in the full version of the Yellow Book.
Appendix E

Techniques

This appendix provides additional guidance on the execution of the following techniques:

1. Failure Mode and Effects Analysis (FMEA) (see Chapter 15)
2. Hazard and Operability Studies (HAZOP) (see Chapter 15)
3. Fault Tree Analysis (see Chapter 15)
4. Cause Consequence Diagramming (see Chapter 15)
5. Data Recording and Corrective Action System (DRACAS) (see Chapter 11)
6. Goal Structuring Notation (GSN) (see Chapter 18)
E.1  Failure Mode and Effects Analysis (FMEA)
This section has been removed from this version but is available in the full version of the Yellow Book.

E.2  Hazard and Operability Studies (HAZOP)
This section has been removed from this version but is available in the full version of the Yellow Book.

E.3  Fault Tree Analysis
This section has been removed from this version but is available in the full version of the Yellow Book.

E.4  Cause Consequence Diagramming
This section has been removed from this version but is available in the full version of the Yellow Book.

E.5  Data Reporting Analysis and Corrective Action System (DRACAS)
The Data Reporting Analysis and Corrective Action System (DRACAS), sometimes referred to as a Failure Reporting Analysis and Corrective Action System (FRACAS), is a closed loop data reporting and analysis system. The aim of the system is to aid design, to identify corrective action tasks and to evaluate test results, in order to provide confidence in the results of the safety analysis activities and in the correct operation of the safety features.

Its effectiveness depends on accurate input data in the form of reports documenting incidents. These reports should therefore document all the conditions relating to the incident.

The Project Manager or Project Safety Manager should be part of the team that reviews the incidents, in order that their impact on the safety characteristics of the system can be quickly assessed and any corrective actions requiring design changes quickly approved.

The DRACAS process is illustrated in Figure E-2 and may be summarised as follows:

1. The incident is raised and recorded on a database.
2. A data search is carried out for related events.
3. The incident is reviewed. If the incident is a new hazard it is recorded as such in the Hazard Log.
4. Information concerning the incident is communicated to those that need to know, in order to control risk.
5. Corrective actions are recommended, as necessary.
6. If no corrective action is required the database is updated and the process ends.
7. The corrective action is authorised and implemented and assessed for success.
8. If the corrective action is successful, the database is updated and the process ends.
9. If the corrective action is unsuccessful, the incident is re-reviewed (the process returns to step 5).
Incident raised and recorded
Search for related events

Review incident

YES

Communicate information as necessary

Corrective action necessary?

YES

Authorise, implement and assess action

Corrective action successful?

NO

NO

Update database

Figure E-2 The DRACAS process

E.6 Goal Structuring Notation
This section has been removed from this version but is available in the full version of the Yellow Book.
Appendix F

Referenced documents

This appendix provides full references to the documents referred to in the body of this volume.


F.4 Department for Transport, *Railways (Interoperability) Regulations 2006 Guidance*


F.11 EN 50126:1999, *Railway applications – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)*

F.12 EN 50159-1:2001, *Railway Applications – Communications, signalling and processing systems – safety related communication in closed transmission systems*

F.13 *Understanding Human Factors: A Guide for the Railway, issue 1.0 RSSB*

F.14 EN 50159-2:2001, *Railway Applications – Communications, signalling and processing systems – safety related communication in open transmission systems*
Referenced documents

F.15 ISO 10007:2003, Quality management systems. Guidelines for configuration management


F.17 Health and Safety Executive, Reducing Risk, Protecting People, 2001, ISBN 0 7176 2151 0


F.25 The Railway Strategic Safety Plan 2006, RSSB

F.26 EN 50128:2001, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems


F.28 Health and Safety Executive, Methods for assessing the safety integrity of safety-related software of uncertain pedigree (SOUP), 2001

F.29 German Federal Railways Standard Mü 8004

F.30 Railway Industry Association, Safety related software for railway signalling (RIA 23), 1991


F.33 EN 41003:1999, Particular safety requirements for equipment to be connected to telecommunications networks

F.34 BS 7671:2001, Requirements for electrical installations. IEE Wiring Regulations. Sixteenth edition


F.42 University of York, *Freeware GSN Add-on for Microsoft Visio*, available from URL: www.cs.york.ac.uk/~tpk/gsn/gsnaddoninstaller.zip


F.44 *GSN User Club Web Site*, URL: www.origin-consulting.com/gsnclub

F.45 Tim Kelly and Rob Weaver, *The Goal Structuring Notation – A Safety Argument Notation* 2004
The feedback form and index have been removed from this version but are available in the full version of the Yellow Book.