Foreword to the combined volumes

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 cooperation 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 at the end of this volume if you want to send us comments.

Published by Rail Safety and Standards Board on behalf of the UK rail industry

ISBN 978-0-9551435-2-6
## Volume structure

### Volume 1  Engineering Safety Management Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Obligations and liabilities</td>
<td>4</td>
</tr>
<tr>
<td>Engineering safety management fundamentals</td>
<td>11</td>
</tr>
<tr>
<td>Putting the fundamentals into practice</td>
<td>24</td>
</tr>
<tr>
<td>References</td>
<td>25</td>
</tr>
</tbody>
</table>

### Volume 2  Engineering Safety Management Guidance

#### Part 1: Introductory Material

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>General high-level guidance</td>
<td>7</td>
</tr>
<tr>
<td>High-level guidance for projects</td>
<td>21</td>
</tr>
<tr>
<td>High-level guidance for maintenance</td>
<td>39</td>
</tr>
</tbody>
</table>

#### Part 2: Organisation Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety responsibility</td>
<td>51</td>
</tr>
<tr>
<td>Organisational goals; Safety culture</td>
<td>59</td>
</tr>
<tr>
<td>Competence and training</td>
<td>65</td>
</tr>
<tr>
<td>Working with suppliers</td>
<td>73</td>
</tr>
<tr>
<td>Communicating safety-related information; Co-ordination</td>
<td>79</td>
</tr>
<tr>
<td>Continuing safety management</td>
<td>89</td>
</tr>
</tbody>
</table>

#### Part 3: Process Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety planning; Systematic processes and good practice</td>
<td>95</td>
</tr>
<tr>
<td>Configuration management; Records</td>
<td>115</td>
</tr>
<tr>
<td>Independent professional review</td>
<td>135</td>
</tr>
</tbody>
</table>

#### Part 4: Risk Assessment Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining your work</td>
<td>151</td>
</tr>
<tr>
<td>Identifying hazards; Assessing risk</td>
<td>159</td>
</tr>
<tr>
<td>Monitoring risk</td>
<td>189</td>
</tr>
</tbody>
</table>

#### Part 5: Risk Control Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reducing risk; Safety requirements</td>
<td>195</td>
</tr>
<tr>
<td>Evidence of safety; Acceptance and approval</td>
<td>207</td>
</tr>
</tbody>
</table>

#### Appendices

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A  Glossary</td>
<td>227</td>
</tr>
<tr>
<td>B  Document outlines</td>
<td>235</td>
</tr>
<tr>
<td>C  Checklists</td>
<td>247</td>
</tr>
<tr>
<td>D  Examples</td>
<td>265</td>
</tr>
<tr>
<td>E  Techniques</td>
<td>291</td>
</tr>
<tr>
<td>F  Referenced documents</td>
<td>313</td>
</tr>
</tbody>
</table>

Feedback form                                      | 316  |

Index                                              | 317  |
Engineering Safety Management
The Yellow Book

Volume 1
Fundamentals
Issue 4

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 Crystal Mark applies to volume 1 only.

Published by Rail Safety and Standards Board on behalf of the UK rail industry
Volume 1, issue 4, was originally published on its own in 2005 and is reproduced here without change.
Foreword

Railtrack published issue 1 of the Yellow Book in 1996 as a single volume. It contained certain group standards, line standards and departmental work instructions. Together these provided a basis for carrying out Engineering Safety Management (ESM) and supported Railtrack’s customers and suppliers by giving details of some of its internal procedures for Engineering Safety Management.

The Yellow Book is now 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.

The Yellow Book has changed significantly since its first issue. It has developed so that it now provides a set of fundamentals with supporting guidance that applies to the whole railway industry.

Previous issues covered railway projects but we know that maintenance is as critical to railway safety as projects and that maintenance staff are as committed to improving railway safety as project staff. So, we have extended issue 4 to cover railway maintenance as well. We have also brought the book up to date with current legislation and good practice. We hope that railway maintenance and project staff will find the new issue helps them to work together to make the railway safer.

We are continuing to try and improve the format and content of the Yellow Book. Please use the suggestion form at the end of this volume if you want to comment on this issue.
Acknowledgements

We have prepared this document with the guidance of the following steering group members. All of these people provided their time and expertise as professionals committed to improving railway safety. Their opinions do not necessarily reflect those of their employers. We gratefully acknowledge their contribution.

Jeff Allan
Roger Aylward
Neil Barnatt
Richard Barrow
Paul Cheeseman
John Corrie
Robert A Davis
Bruce Elliott
Terry George

Eddie Goddard
Philip de Graaf
Nick Holmes-Mackie
Roger Kemp
Alan Lawton
Robert Mole
Richard Tavendale
Keith Watson

The members were drawn from the following organisations:

AEA Technology Rail
Atkins Rail
Praxis High Integrity Systems
ProRail
Rail Safety and Standards Board
Union Railways (North)

Mott MacDonald Limited
Network Rail
Lancaster University
Lloyd's Register Rail Limited
London Underground Limited
Westinghouse Rail Systems Limited

We are grateful to Plain English Campaign, Cliff Cork of Rail Safety and Standards Board, Barny Daley of Carillion, John Downes and Gab Parris of London Underground Limited, Richard Lockett of the Association of Train Operating Companies, Richard Gostling of the Railway Industry Association, Graham Smith of Network Rail and Paul Traub of CCD Design and Ergonomics for their help with this document.

We are also grateful to everyone in the rail industry who helped us to publish the Yellow Book.
Volume 1 Engineering Safety Management Fundamentals

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Purpose</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Definitions</td>
<td>1</td>
</tr>
<tr>
<td>1.3 The structure of the Yellow Book</td>
<td>2</td>
</tr>
<tr>
<td>1.4 Change and maintenance</td>
<td>3</td>
</tr>
<tr>
<td>2 OBLIGATIONS AND LIABILITIES</td>
<td>4</td>
</tr>
<tr>
<td>2.1 UK law</td>
<td>4</td>
</tr>
<tr>
<td>2.2 European law</td>
<td>5</td>
</tr>
<tr>
<td>2.3 Evidence requirements</td>
<td>6</td>
</tr>
<tr>
<td>2.4 ‘Reasonable practicability’</td>
<td>7</td>
</tr>
<tr>
<td>2.5 Standards, guidelines and good practice</td>
<td>8</td>
</tr>
<tr>
<td>2.6 Human behaviour</td>
<td>10</td>
</tr>
<tr>
<td>3 ENGINEERING SAFETY MANAGEMENT FUNDAMENTALS</td>
<td>11</td>
</tr>
<tr>
<td>3.1 Organisation fundamentals</td>
<td>12</td>
</tr>
<tr>
<td>3.2 Process fundamentals</td>
<td>15</td>
</tr>
<tr>
<td>3.3 Risk assessment fundamentals</td>
<td>18</td>
</tr>
<tr>
<td>3.4 Risk control fundamentals</td>
<td>21</td>
</tr>
<tr>
<td>4 PUTTING THE FUNDAMENTALS INTO PRACTICE</td>
<td>24</td>
</tr>
<tr>
<td>5 REFERENCES</td>
<td>25</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Purpose

We have written Engineering Safety Management (or the Yellow Book as it is more commonly known) to help people who are involved in railway engineering (either changing the railway or maintaining it) to make sure that their work contributes to improved safety and get changes to the railway accepted more efficiently. This always includes considering things outside engineering and usually includes people who are not engineers, so the Yellow Book is not just written for engineers.

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

The Yellow Book is written to help you set up a process that protects you and others from mistakes and gives documented evidence (such as a safety case) that risk is at an acceptable level. This process may well deliver other objectives, such as keeping the railway running, but the Yellow Book is only concerned with the safety aspects. The Yellow Book also helps you to keep within the law and relevant standards.

You do not have to follow the Yellow Book but there is consensus among railway engineers in the UK and elsewhere that the fundamentals represent good practice in engineering safety management. If you are involved in railway engineering and you are not putting a fundamental into practice, you should check that what you are doing is also good practice. If you are involved in other aspects of the railway, then the fundamentals may be a useful starting point, even though they may not reflect agreed good practice in your particular area of activity.

1.2 Definitions

In general we have written this volume in plain language but we use a few specialised terms. In this volume they have the following meanings.

Hazard – any situation that could contribute to an accident. Hazards should be eliminated wherever ‘practicable’, but this is not always the case. Where a hazard cannot be completely eliminated then there will be some risk.

Risk – the likelihood that an accident will happen and the harm that could arise. In many cases, risk cannot be eliminated entirely. We must accept this if we are to continually improve safety.

We use maintenance in its ordinary English sense “of keeping something fit for service” including, where necessary, replacing a worn-out part of the railway with a new part. So when we talk about maintenance, we are including what some people call ‘renewals’, ‘alterations’, ‘upgrades’ and ‘enhancements’.

We say that something is safe when the risk associated with it is controlled to an acceptable level. This level may reduce as technological advances make it practicable to reduce risk even further.

Safety case – a document that describes the measures taken to ensure the safety of some aspects of the railway. There are two main sorts of safety case:
• An **engineering safety case** presents the justification for the safety of a railway product or a change to the railway. Despite its name, an engineering safety case covers more than just engineering.

• A **railway safety case** describes the arrangements for safety management for an organisation which manages infrastructure or operates trains or stations.

### 1.3 The structure of the Yellow Book

Issue 4 of the Yellow Book is in two volumes (see note 1 below):

1. Engineering Safety Management Fundamentals
2. Engineering Safety Management Guidance

Volume 1 describes some of the safety obligations on people involved in changing or maintaining the railway. It also describes the fundamentals of a systematic approach to meeting these obligations.

There are many effective ways of putting these fundamentals into practice. Volume 2 gives guidance on ways that have proved effective.

We suggest that you read volume 1 first and refer to volume 2 if and when you find you need this guidance.

Further information is published on the Yellow Book website, www.yellowbook-rail.org.uk, including a series of application notes describing how to put the guidance into practice in particular circumstances.

Figure 1 shows the overall structure of the Yellow Book.

![Figure 1 – Overall structure of the Yellow Book](image)

---

**Note 1.** When we published volume 1, volume 2 was not complete and we were working on providing some more detailed guidance in a temporary format. Please check the Yellow Book website, www.yellowbook-rail.org.uk, to find out what further guidance is currently available.
1.4 Change and maintenance

Before this issue, the Yellow Book only dealt with projects – activities that make significant, deliberate changes to the railway. It still does, and if you are involved in a railway project, the Yellow Book provides you with a basis on which to build safety into the change and to take good decisions about whether to go ahead with a change or not.

Maintenance is also a period of change. Some of this change, such as wear and tear, is outside the control of the maintainer and maintenance must react to it. But maintainers also make deliberate changes to the railway to improve it.

Proper maintenance is essential to keeping the railway safe and maintenance mistakes can cause accidents. Clearly, maintaining the railway needs a systematic approach to managing safety just as much as projects do. Moreover, there is no clear dividing line between projects and maintenance – some activities could be put under either heading – so these two approaches should be based on a common set of fundamentals.

For these reasons, we have extended the Yellow Book to cover maintenance as well as projects. If you are involved in maintaining trains, signalling or any other part of the railway, the Yellow Book now provides you with a basis for planning an effective response to changes outside your control and to take decisions about whether to continue with things as they are or to set some deliberate change in progress to make things safer.

All of the fundamentals apply equally to projects and maintenance but, as we explain, they are sometimes applied in different ways.
2 OBLIGATIONS AND LIABILITIES

This section describes some of the obligations that the Yellow Book helps you to carry out. It also describes some of the legal liabilities that you face and some ways of reducing them.

We discuss the main principles of UK and European law as they apply to the railways but the discussion is no substitute for detailed legal advice.

You should note that the situation is changing as we write this section and may have changed by the time you read it. You should check guidance issued by the UK Department for Transport Rail for up-to-date information. The Yellow Book website, www.yellowbook-rail.org.uk, also contains more information on European law and how it relates to the Yellow Book.

2.1 UK law

The Health and Safety at Work etc Act 1974 gives employers a duty to ensure, ‘so far as is reasonably practicable’, the health, safety and welfare of their employees and of any other people affected by their work. This often implies a need to use good practice and standards, which are discussed in section 2.5.

Employees must take reasonable care for their own health and safety and for the health and safety of anyone affected by their work.

The duties in the act can be managed using a contract but cannot be transferred completely.

Regulations can be made under the act, and those currently in force place duties on:

- employers to assess risk to those affected by their work – Management of Health and Safety at Work Regulations 1999;
- employers who share a workplace to co-operate and share information to achieve safety – Management of Health and Safety at Work Regulations 1999; and
- those involved in construction projects to control risk by planning, co-operating, sharing information and keeping certain records – Construction (Design and Management) Regulations 1994 (amended 2000).

Other regulations place duties on:

- employers to assess the competence and fitness of individuals carrying out defined ‘safety-related’ work – Railways (Safety Critical Work) Regulations 1994 (amended 2000); and
- any organisation which manages infrastructure or operates trains or stations to prepare a railway safety case for acceptance by Her Majesty’s Railway Inspectorate (HMRI), to maintain their safety case, and to follow it – Railways (Safety Case) Regulations 2000 (amended 2001 and 2003).

HMRI is the safety regulator for railways in the UK. You must obtain their approval before putting new or changed parts of the railway in service. Some of HMRI’s powers are discussed in the next section. Others are currently confirmed in the Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations 1994.
People have general responsibilities for their own safety and for the safety of others affected by their work. A member of a professional organisation will also have responsibilities under their code of conduct. The Engineering Council's Guidelines on Risk Issues gives further guidance on professional responsibilities.

A job may also carry specific safety responsibilities. These may arise from legislation, company procedures or a contract of employment.

You should make sure that you understand your safety responsibilities and meet them.

There are other relevant acts and regulations, which we do not discuss.

2.2 European law

This section contains only a very brief overview of European law as it applies to railways. As we said earlier, you should check guidance issued by the UK Department for Transport Rail for more information on how the UK has put European law into practice.

The European Union (EU) has issued directives (96/48/EC, 2001/16/EC and 2004/50/EC) on railway interoperability to make it easier to run trains across borders and to sell railway products across Europe. The Railways (Interoperability) (High Speed) Regulations 2002 (HSR) have included 96/48/EC in UK law. Further regulations are being developed to include the other directives in UK law. These directives do not apply to light rail and metros.

Where they apply, the directives say that on the trans-European high-speed and conventional rail systems, certain parts of the railway (called subsystems) and certain railway products (called interoperability constituents) must meet certain essential requirements. This is intended to make sure that the parts of the railway work together. The essential requirements include safety. The directives are supported by Technical Specifications for Interoperability (TSIs). TSIs currently apply to interoperability constituents and the following subsystems.

- Maintenance
- Infrastructure
- Energy
- Operations
- Rolling stock;
- Command, control and signalling systems

TSIs are intended to make sure that subsystems meet the essential requirements by specifying those features which are needed to meet the directives' objectives. New and upgraded subsystems must follow the relevant TSIs and will need authorisation by the safety authority (HMRI in the UK) before they can be placed into service.

Further TSIs will be introduced later.
The organisation that supplies an interoperability constituent, or wants to place a subsystem into service, appoints a **Notified Body** to check that the relevant parts of the TSIs have been met. Notified Bodies have to be accredited as competent to do this. A list of Notified Bodies and their areas of competence is maintained by each national government. The organisation needs to get **certification** before placing the product on the market or **authorisation** before putting that part of the railway into service.

Currently in the UK, the Department for Transport maintains the list of Notified Bodies and HMRI grants authorisations.

Once an interoperability constituent or subsystem has successfully been through this process for a particular application, it is illegal, within the EU, to require further safety tests and evaluations before allowing it to be used for that application.

In the case of a disagreement between European law and UK law, European law applies. So, the level of safety needed by a TSI takes priority over the UK legal requirement to ensure health, safety and welfare ‘so far as is reasonably practicable’. However, you should still look for reasonably practicable ways of improving safety in areas not covered by the TSI. (See reference 2 in section 5.)

The EU has also issued a **Railway Safety Directive (2004/49/EC)**, which will progressively introduce common targets and indicators for railway safety and common methods of delivering them. It is setting up the European Rail Agency with responsibilities for developing the TSIs as well as these safety targets, indicators and methods. UK regulations to include this directive in UK law are being prepared.

### 2.3 Evidence requirements

You will generally have to provide some evidence that you have met your obligations for managing safety. In the UK there are three main sorts of documents that are produced: the railway safety case, the engineering safety case and the technical file. There are similar requirements in other countries.

#### 2.3.1 Railway safety case

Any organisation which manages infrastructure or operates trains or stations in the UK must currently write a railway safety case and have it accepted before starting operations. The operator must then follow their safety case.

It is important to note that the legislation makes it clear that infrastructure managers and operators are always entirely responsible for their own actions and must be able to show to the safety authority in their railway safety cases that the safety risk has been controlled. Organisations must co-operate to control risk. Often this is done by following standards set by the directives or the RSSB (or both). Otherwise, their railway safety cases must describe the co-operative arrangements that have been agreed.

Among other things, the operator’s railway safety case must describe:

- its safety policy and arrangements for managing safety;
- its assessment of the risk;
- how it will monitor safety;
- how it organises itself to carry out its safety policy; and
- how it makes sure that its staff are competent to do safety-related work.
Under European law, organisations which manage infrastructure or operate railways in the EU will have to produce documents with similar content although with different names. These documents are expected to replace the UK railway safety case.

2.3.2 Engineering safety case

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. As discussed, relevant TSIs are an example of such standards. As a result, when the HSR apply and a subsystem or interoperability constituent is fully specified by the TSI, a safety case is not written. Instead, the demonstration of safety is checked by the Notified Body as described earlier.

Where the risk is not completely covered by standards, it has been normal, in the UK and some other countries, to prepare an engineering safety case for any significant change to the railway or for any new or changed railway product which could significantly affect railway safety.

Your engineering safety case should show that you have controlled risk to an acceptable level. It should also show that you have taken a systematic approach to managing safety, in order to show that your assessment of the risk is valid. Your safety case should consider the effect that the change or product will have on the rest of the railway, including the effect of any changes to operating and maintenance procedures.

Similar safety cases are required by CENELEC standards for signalling projects and products and some other projects, and so are commonly produced for these projects across Europe.

2.3.3 Technical file

A technical file contains the evidence that an interoperability constituent or subsystem meets the relevant TSIs. This is required by European directives.

2.4 ‘Reasonable practicability’

As we have explained, the Health and Safety at Work etc Act 1974 places duties on employers in the UK to ensure health, safety and welfare ‘so far as is reasonably practicable’. This section gives more guidance on this test. Other countries use different rules for taking decisions about safety. The Railway Safety Directive, described above, will mean that people take decisions about railway safety in a similar way across the EU. This way of taking decisions will replace the test of ‘reasonable practicability’, in many cases.

This test is only one aspect of UK safety law and there are other, more specific legal requirements that you have to meet. However, it has proved difficult to apply in practice so we have given it a section of its own.

If your work could contribute to an accident, you should first identify the hazards associated with your 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 so small that it is not worth considering).

You should make sure that your precautions reflect good practice, as set out in the law, guidance from the government and professional bodies, and standards. We discuss good practice further in the next section.
If following good practice is not enough to show that the risk is acceptable, you should also assess the total risk that will be produced by your new or changed product or by the change you are making. You then need to compare it with two extreme regions.

- An intolerable region where risk can never be accepted.
- A broadly acceptable region where risk can generally be accepted.

To decide whether or not to accept a risk:

1. check if the risk is in the 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; and
3. if the risk lies between these two regions, accept it only after you have taken all ‘reasonably practicable’ steps to control the risk.

You should consider ways of making the change or product less likely to contribute to an accident. You should also consider ways of preventing accidents. You do not have to take steps that are outside your control. However, if there is a problem that someone else needs to deal with, you should bring it to their attention.

Your work should maintain safety standards, if not improve them.

If you are not certain about the risk, you should be cautious – uncertainty does not justify not taking action.

To decide whether a step that would control risk is reasonably practicable, you must balance the reduction in risk against any other factors, including time, money and trouble. It may be necessary to estimate the costs and benefits if the costs are high and the balance is unclear. Usually it is possible to establish where the balance lies without doing this.

In *Reducing Risks, Protecting People*, the Health and Safety Executive (HSE) suggested that you could use a figure of £1 million (at 2001 prices) as a ‘benchmark’ – an indication of what it is reasonably practicable to spend to reduce risk by one fatality. *How Safe is Safe Enough*, published by RSSB, contains full and up-to-date guidance on this.

All benchmarks are only rough reflections of the values held by society. If there is significant public concern about a hazard, you should take this into account in your decision-making and it may justify precautions that would not be justified otherwise.

RSSB publishes guidance on the figures that are suitable for railway decisions. Following this guidance will help you make objective decisions and show how you reach those decisions. It also helps you make sure that you are using limited resources in the best way.

### 2.5 Standards, guidelines and good practice

The main reason for using good practice is to control risk. However, if you face a civil action for damages after an accident, you may want to show that you used good practice and met relevant standards and guidelines. This could help your defence against a charge of negligence and reduce other legal liabilities.
The Yellow Book is generally in line with standards and guidelines described below and following the Yellow Book guidance will help you meet them. However, the Yellow Book takes a wide view of good practice and does not say that you have to follow any one standard or guideline.

2.5.1 The role of standards

We distinguish a standard, which says what you must do, from a guideline which gives you more general information.

Sometimes the risk comes completely within accepted standards that define agreed ways of controlling it. As we said in section 2.2, where the HSR apply and a subsystem or interoperability constituent is fully specified by the TSI, the level of safety set by the TSI takes priority over the UK current legal requirements on health safety and welfare. In that case, showing that you have met these standards will be enough to meet your legal obligations. In a different example, the electrical safety of ordinary office equipment is normally shown by meeting electrical standards.

However, where the risk is not completely within accepted standards, you cannot rely on them to achieve safety on their own. They may not properly cover your situation or there may be reasonably practicable improvements on them that reduce risk further. 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.

Over time, as more TSIs are agreed, more and more decisions about what risk is acceptable will be settled by meeting these standards. Other initiatives the European Rail Agency is working on may have a similar effect.

2.5.2 Relevant standards

The standards that are relevant to you will depend upon what you are doing but the following generally apply.

**TSIs** were described in section 2.2 above.

Most railways maintain their own standards. RSSB maintains a series of *Railway Group Standards*, which cover some aspects of the UK main line railway. London Underground Limited maintains a similar series of standards for its railway.

Also, if your work involves electronic systems then the following will generally apply:

- **International Electrotechnical Commission (IEC) Standard 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.** This is an international standard that applies to all sectors of industry. It describes a general safety lifecycle, which includes analysing hazards and risks, and setting safety requirements.

- **CENELEC**, the European Committee for Electrotechnical Standardization, has published European standards for railway applications and is working on others.

The law or your contract may say that you have to meet some of these standards. Where you have to meet several standards, some may take priority over others.
2.5.3 Relevant guidelines

HMRI's *Railway Safety Principles and Guidance* (the ‘Blue Book’) currently gives advice on designing, constructing and altering works, plant and equipment, while maintaining railway safety. It sets out safety principles and the factors affecting how to put them into practice. It also gives advice on detailed aspects of railway construction. It deals with the end result of design and construction rather than the processes themselves.

The Engineering Council’s *Guidelines on Risk Issues* give practical and ethical guidance to engineers and managers on how to meet their social responsibilities by controlling risk. They discuss:

- the legal and professional restrictions on the engineer;
- the concepts behind managing risk; and
- implications for education and public awareness.

The Hazards Forum’s document *Safety-related Systems – Guidance for Engineers* gives professional engineers an overview of the professional, practical and legal aspects of working on safety-related systems. It applies particularly to computer-based systems.

2.6 Human behaviour

Even the most highly automated systems are designed, installed and maintained by people. Everybody makes mistakes. People’s behaviour plays a part in most, if not all, accidents. If you have not considered people’s behaviour in your work, it will be difficult to show that you have controlled risk properly. Understanding how people behave when things go wrong is important in understanding the risk.

Some of the ways people behave and some of the reasons for their mistakes are understood. Some ways of preventing or controlling these mistakes are known.

People prevent accidents as well as contributing to them, and you should also take this into account.

You should consider all the people whom your work will affect when applying each of the Yellow Book fundamentals, including customers, the general public, installers, operators and maintainers. You should do what you can to help them avoid mistakes and prevent accidents. Volume 2 provides guidance on doing this.
3 ENGINEERING SAFETY MANAGEMENT FUNDAMENTALS

A systematic approach to ESM plays an essential part in making sure that the railway is safe.

You do not need to carry out a full programme of ESM activities if you can show that your work involves only a very low level of risk, or no risk, or that the risk is fully covered by standards. However, you should monitor the risk to check that this remains the case.

If you need to carry out an ESM programme, it should have some fundamental features. We can look at these under four headings. These are:

- **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 fundamentals identify what needs to be done within the context of railway engineering to manage the safety of the railway. They do not say who is responsible for what. You need to work out what responsibilities you have and plan your work to meet them.

If your work involves introducing some railway product that has been used elsewhere, you may find that some of these fundamentals were not put fully into practice beforehand, or, if they were, that you do not have evidence of it. On the other hand the product may be covered by a TSI or you may have direct evidence that the product has performed safely in the past in similar circumstances. You will need to balance these two factors and consider their effect on risk in order to decide how far you need to apply the risk control and risk assessment fundamentals. You should take account of any differences between the way the product was used before and the way you are planning to use it. The organisation and process fundamentals will remain relevant to the work you are doing.

Each fundamental is shown in a box, followed by an explanation and a justification.
3.1 Organisation fundamentals

3.1.1 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.

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.

3.1.2 Organisational goals

Your organisation must have safety as a primary goal.

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.

3.1.3 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.

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.

3.1.4 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.

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.

3.1.5 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.

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.
3.1.6 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.

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.

3.1.7 Co-ordination

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

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.

3.1.8 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.

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.

As discussed in section 1.4 above, 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.
3.2 Process fundamentals

3.2.1 Safety planning

Your organisation must plan all safety management activities before carrying them out.

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.

3.2.2 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.

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.
3.2.3 Configuration management

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

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.

3.2.4 Records

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

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.

3.2.5 Independent professional review

Safety management activities that your organisation carries out must be reviewed by professionals who are not involved in the activities concerned.

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.
3.3 Risk assessment fundamentals

Risk assessment provides information on which to base good decisions about safety. For projects, these decisions will include whether or not to put a new part of the railway into service and under what conditions. For maintenance, these decisions will include whether or not to take unscheduled action to prevent failure. In both cases, these decisions involve balancing the risk arising from doing the work against the risk arising from not doing the work. Both these risks may include risk to railway operation and risk to the people doing the work.

3.3.1 Defining your work

Your organisation must define the extent and context of its activities. 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.

3.3.2 Identifying hazards

Your organisation must make a systematic and vigorous attempt to identify all possible hazards related to its activities and responsibilities.

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 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.

### 3.3.3 Assessing risk

Your organisation must assess the effect of its activities and responsibilities on overall risk on the railway.

In most countries, you will have a legal duty to assess risk. In the UK, this duty is set out in regulation 3 of the *Management of Health and Safety at Work Regulations 1999*.

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.

### 3.3.4 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.

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.
3.4 Risk control fundamentals

3.4.1 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.

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 section 2.4 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.

3.4.2 Safety requirements

Your organisation must set and meet safety requirements to control the risk associated with the work to an acceptable level.

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.
3.4.3 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.

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. See section 2.3 above.

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.


3.4.4 Acceptance and approval

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

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

In some cases the safety authority may approve your organisation’s overall processes and then allow it to approve its own work.

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.
4 PUTTING THE FUNDAMENTALS INTO PRACTICE

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. You do not have to use the approach described there and it is not the only effective approach, but it has been proven in practice.

You might also find the following further reading helpful:

   (Analysis of weaknesses in management at the root of one of the worst recent British railway accidents.)

   (Analysis of causes of one of the worst recent British railway accidents.)

   (An in-depth discussion of the organisational factors which contribute to accidents.)

   (Thorough guidance on the duties imposed by the Construction (Design and Maintenance) Regulations 1994.)

   (A readable and thoughtful survey of accidents on the UK railway since the beginning of the railway era.)

   (Presentation of options for reforming UK railway safety law.)

   (Provides a framework for systematic and co-ordinated management of physical assets in order to meet defined goals.)
5 REFERENCES

This section provides full descriptions of documents, except directives, acts and regulations, we have referred to in the text.


<table>
<thead>
<tr>
<th>Your suggestions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your name and address:</strong></td>
</tr>
<tr>
<td><img src="image1.png" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Your suggestions for changing the Yellow Book:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Image" /></td>
</tr>
</tbody>
</table>

**Please photocopy this sheet and send or fax your comments to:**

<table>
<thead>
<tr>
<th>ESM Administrator</th>
<th>Phone: +44 (0)20 7904 7777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail Safety and Standards Board</td>
<td>Fax: +44 (0)20 7557 9072</td>
</tr>
<tr>
<td>Evergreen House</td>
<td><strong>Or you may email your comments to:</strong></td>
</tr>
<tr>
<td>160 Euston Road</td>
<td><a href="mailto:info@yellowbook-rail.org.uk">info@yellowbook-rail.org.uk</a></td>
</tr>
<tr>
<td>London NW1 2DX</td>
<td><strong>For our use</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Suggestion number:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image4.png" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status (open or closed):</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image5.png" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reply sent:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image6.png" alt="Image" /></td>
</tr>
</tbody>
</table>
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.
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
Bombardier Transportation
ERA Technology
Mott MacDonald Limited
Lloyd's Register Group
Porterbrook Leasing
Rail Safety and Standards Board
Technical Programme Delivery Limited
University of York

Atkins Rail
Channel Tunnel Rail Link (UK) Limited
Hitachi Rail Group
London Underground Limited
Network Rail
Praxis High Integrity Systems
Scott Wilson Railways Limited
Tube Lines
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
This page has been left blank intentionally
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.\footnote{RSSB’s work in this area is ongoing. You may wish to check the RSSB web-site for later guidance.}

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.
This page has been left blank intentionally
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.
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.
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

3.1 Introduction

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

We present a series of diagrams, each of which, with its supporting text, takes one phase, suggests a series of activities that are appropriate at this phase and relates these to the underlying fundamental and to the possible techniques and tools for implementing it.

Note when reading this chapter that:

- The full guidance on the topics mentioned is provided in later chapters. This chapter provides a summary which may be useful for initial orientation but there is not enough space to deal with the topics fully. You should read the later chapters before trying to put this guidance into practice or you may miss some important points.

- You should check whether or not the activities recommended for the previous phases have been carried out; if they have not, then you should consider remedial work to deal with this.

- It will generally be necessary to maintain the outputs of work carried out in previous phases; that is to update this work if something material should change.

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

Note: it is often the case, particularly with infrastructure projects, where access to the railway may only be possible overnight and at weekends, that the Implementation phase may be carried out in a series of small steps. Some people refer to this as carrying out ‘stage-works’, others refer to a ‘migration’ from the initial state of the railway to its final state. If this is the case, you need to assure yourself that risk has been controlled to an acceptable level whenever the railway is returned to service after an intermediate stage. This may be relatively straightforward compared with showing that risk has been controlled to an acceptable level in the final railway, in which case it can be demonstrated using simpler processes. However, you cannot ignore this issue and need to include it in your planning from the outset.
3.1.1 Adapting this guidance

This chapter provides guidance on an illustrative set of ESM activities that could be carried out in each phase. 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.

The activities described below are appropriate to a project where:

- risk cannot be controlled completely by applying standards or procedures;
- you are compiling evidence of safety into a Safety Case; and
- there are some significant Human Factors issues.

If the risk comes completely within accepted standards that define agreed ways of controlling it (see section 2.4.3), then you may not need to carry out all of the activities described.

If the work you are doing comes completely within your organisation’s Safety Management System then the provisions of this Safety Management System may replace some or all of the activities described.

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

It is crucial to take account of Human Factors but, if they are straightforward, you may be able to do so quite adequately within the context of more general activities.
3.2 The Concept and Feasibility phase

3.2.1 Defining your work

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

You should also establish:

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

There is more guidance on these topics in section 2.4.
3.2.2 Evidence of safety; Acceptance and approval

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 railway’s procedures (for example, Railway Group Standards);
- consult the guidance provided on national and international approval requirements (for example, 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]).

You should agree with your Safety Approvers how you will present the evidence for safety. 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.

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.

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.

3.2.3 Identifying hazards; Assessing risk

You should look for hazards that the system may pose to people, including hazards specific to intermediate stages, if there any. You should also look for hazards concerned with the process of building the system. The Yellow Book is primarily designed to help with the former but we do recommend that you co-ordinate the two hazard identification activities.

A preliminary hazard analysis should be carried out in this phase. This is a first-pass hazard identification and risk assessment intended to determine:

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

At the start of a project, design detail will almost always be limited, so the results of preliminary hazard analysis (in particular the depth of application of ESM) should be backed up and re-assessed by carrying out a full analysis and risk assessment later.
Preliminary hazard analysis should be carried out before any significant design activity begins. It requires a full high-level description of the system’s function and construction and its interfaces to people and other systems.

The risk assessment activity carried out during preliminary hazard analysis should consist of annotating identified hazards with an initial appraisal of their severity and likelihood. Ideally, the preliminary hazard analysis should support the process of initial safety requirements setting and, therefore, should provide targets for the likelihood of each of the identified hazards.

The results of the preliminary hazard analysis should be used to decide where further quantified analysis is required.

The findings of preliminary hazard analysis and the decisions that result should be documented in a report.

The preliminary hazard analysis should be improved and extended in subsequent phases as more information becomes available.

3.2.4 Safety planning

The safety management activities on a safety-related project should be planned and one way of doing this is to produce a Safety Plan for the project. The Safety Plan performs two main functions:

1. it provides a detailed schedule of how safety risks will be reduced to an acceptable level (or shown already to be at an acceptable level); and

2. it provides a means of demonstrating that this has been done.

The Safety Plan describes a programme of work which will ensure the safety requirements are identified and met. It should also state and justify the allocation of key staff and resources to carry out this programme.

The Safety Plan is an evolutionary document. In this phase the Safety Plan will be a Preliminary Safety Plan and will describe the safety analysis activities needed to derive safety requirements. As the project progresses, a Safety Plan will describe activities to meet these safety requirements.

A Preliminary Safety Plan may be produced at this stage.

The Preliminary Safety Plan will be a short, high-level version of the Safety Plan, produced as early in the project as possible, and will describe the overall strategy and approach to reducing safety risks.

3.2.5 Independent professional review

Review of safety-related work by professionals independent of the work is an important contribution to the confidence in the safety of the work. One way of structuring these reviews which may be suitable if you are preparing a Safety Case is 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.

As part of safety planning you will have identified the requirements for auditors and assessors. For significant projects, you may appoint auditors and assessors and they may start their work during the phase.
3.3 The Requirements Definition phase

**Figure 3-2 The Requirements Definition phase**

<table>
<thead>
<tr>
<th>Guidance</th>
<th>Fundamental</th>
<th>Techniques &amp; Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure system requirements are clearly specified; Make explicit assumptions</td>
<td>Defining your work (ch 14)</td>
<td>ADC Register</td>
</tr>
<tr>
<td></td>
<td>Systematic processes and good practice (ch 11)</td>
<td>Seven-stage process</td>
</tr>
<tr>
<td></td>
<td>Identifying hazards (ch 15)</td>
<td>Hazard identification checklists (App C)</td>
</tr>
<tr>
<td></td>
<td>Assessing risk (ch 15)</td>
<td>Hazard ranking matrix (App D)</td>
</tr>
<tr>
<td></td>
<td>Records (ch 12)</td>
<td>HAZOP (App E)</td>
</tr>
<tr>
<td></td>
<td>Reducing risk (ch 17)</td>
<td>FMEA (App E)</td>
</tr>
<tr>
<td></td>
<td>Safety requirements (ch 17)</td>
<td>Task analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fault Tree Analysis (App E)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk assessment checklists (App C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example risk assessment (App D)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cause-consequence diagrams (App E)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Human error modelling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>State transition diagram</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Likelihood-severity matrix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outline Hazard Log (App B)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checklists—Updating the Hazard Log (App C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fault Tree Analysis (App E)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outline Safety Plan (App B)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checklists—Safety planning (App C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checklists—Safety audit; safety assessment (App D)</td>
</tr>
</tbody>
</table>

| Set human factors requirements and integrate with system requirements     | Safety planning (ch 11)                          |
|                                                                          | Acceptance and approval (ch 18)                  |
|                                                                          | Independent professional review (ch 13)          |

| Prepare full Safety Plan to include all human factors work. Submit to Safety Authorities. | Auditors and assessors start project review      | Checklists—Safety audit; safety assessment (App D) |
3.3.1 Defining your work

Understanding the aims, extent and context of a change is fundamental to successful ESM. Any change to the railway can be regarded as introducing a new system, or changing 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). You should obtain a clear understanding of the system and its boundaries during this phase. You should also make sure that you are clear about the responsibilities for safety that you have, as well as the responsibilities for safety of other people with whom you will be working.

The aims, extent and context of a change should already be defined in a requirements specification but, if they are not, you should clarify them before starting to proceed with safety analysis. If there is not sufficient information available to completely define the change, then explicit assumptions should be made. These assumptions will need to be confirmed at some later stage in the lifecycle of the change and this confirmation should be planned.

3.3.2 Identifying; hazards Assessing risk

During this phase you should refine your understanding of the hazards of the system, the system’s effect on overall risk on the railway, taking into account the effects of the environment on the system. This should include improving and extending the preliminary hazard analysis as more information becomes available.

The seven-stage process as depicted in Figure 3-3 is the approach recommended by this volume. There are alternative, effective techniques.

**Hazard Identification** involves identification and ranking of hazards.

**Causal Analysis** involves establishing the primary Causal Factors which may give rise to a hazard and estimating the likelihood of occurrence of each hazard.

**Consequence Analysis** involves establishing the intermediate conditions and final consequences, which may arise from a hazard, and estimating the likelihood of accidents arising from each hazard.

Causal and Consequence Analysis may be undertaken in parallel.

The consequences of each hazard may be associated with a range of losses (that is harm to people, damage to the environment or commercial detriment). **Loss Analysis** requires estimation of the magnitude of the safety losses (that is harm to people), before considering options to reduce risk.

Risk reduction and control requires identification of a range of potential risk reduction measures for each hazard. **Options Analysis** comprises determination of such measures and assessment of their implementation costs.

**Impact Analysis** involves assessing the net benefits associated with implementation of each risk reduction measure, in terms of the reduction in risk. This is achieved by revising the previous stages to allow for the effects of the measure.

**Demonstration of Acceptability** involves determining which risk reduction measures should be implemented and justifying the acceptance of any remaining risk. This is done by selecting those that are required to meet legal criteria for acceptable risk or safety targets.
Figure 3-3 The seven-stage process

Human error is usually a significant source of risk. You should seek to identify, model and control human error.

3.3.3 Safety requirements

You should set safety requirements to control the risk during this phase.

A project carrying out safety-related work should identify the hazards and accidents that may result from the work, assess the risk associated with these, control the risk to an acceptable level and set safety requirements to ensure this level of risk is met. There is a legal requirement to assess the risks involved in safety-related work. Safety requirements should also be consistent with agreed targets for safety.

Safety requirements may be quantitative or qualitative. Good engineering practice for meeting integrity requirements for components, such as software and complex electronics, for which Systematic Failure is a particular concern, is to use Safety Integrity Levels (SiLs). SiLs are described in Chapter 17.

The Safety Requirements Specification consolidates information provided by these activities into specific requirements, which form the basis against which the safety of the system is tested and assessed.
If you set numerical safety targets, this is normally done by working from a fault tree (or similar representation of cause and effect logic) and the event probabilities to:

a) derive numerical accident targets which conform to the legal criteria for acceptable risk;

b) derive hazard occurrence rate and/or unavailability targets which are consistent with (a);

c) if applicable, derive SILs for the system functions that are consistent with (b).

The requirements may be apportioned further to sub-systems of the hierarchy and aligned with the system design. In general, targets for Systematic Failure should not be set below sub-system function level. Refer to IEC 61508 [F.5] or BS EN 50129:2003 [F.6] for further guidance on this decomposition.

Any functional requirements on the system or equipment that are necessary to reduce risk to an acceptable level should be incorporated as qualitative safety requirements.

The analyst may set other qualitative safety requirements such as conformance to external standards and should do so whenever:

- such conformance is assumed in the calculation of safety targets; or
- such conformance is otherwise required to control risks to an acceptable level.

If the seven-stage process described in Chapter 15 is being used, then some requirements will arise from the fifth step, Options Analysis. However, requirements may also arise from relevant regulations, standards and codes of practice.

### 3.3.4 Safety planning

You may prepare a full Safety Plan during this phase.

This section describes the information that should be contained within a full Safety Plan. The following structure is recommended:

1. Introduction;
2. Background and Requirements;
3. ESM Activities;
4. Safety Controls;
5. Safety Documentation;
6. Safety Engineering;
7. Validation of External Items.

The size and depth of the Safety Plan will depend on the complexity and level of risk presented by the project. For simple and low-risk projects a brief Safety Plan defining the project personnel and justifying a simple approach may be sufficient. *Note that, if you assume a project is low-risk, you should make this assumption explicit and take action to confirm it. The Safety Plan should be endorsed by the relevant Safety Approvers, regardless of the level of complexity or risk.*

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

- the previous work used good practice;
• it covered all of the project risk; and
• there is little novelty in development, application or use.

The last condition may be relaxed slightly, to allow limited novelty for low-risk projects.

You should plan all Human Factors work. At the beginning of a project you should develop a high-level strategy for the integration of Human Factors into the safety process. This will describe the general approach that will be taken throughout the project. Once project safety requirements are known, you should produce a plan for the Human Factors work that describes in detail the techniques to be used, the skills needed and the points at which different activities will be carried out with details of their implementation.

You should integrate Human Factors planning into the general safety planning. You should also ensure that consideration of Human Factors is integrated into the overall design process.

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

3.3.5 Independent professional review

If they have not started already, your auditors and assessors will normally start their review of your project in this phase.
3.4 The Design phase

The activities of the previous phase continue into this one:

- The risk assessment and the design should contribute to each other. As the design proceeds it will produce additional input information which may extend or replace the basis on which the risk assessment was originally done, allowing the risk assessment to be refined and corrected. The risk assessment should inform the design, and decisions taken to reduce risk further should be captured as additional safety requirements.
- The Safety Plan should be updated as necessary.
• Safety Audit and Assessment will continue.
• If you have not already done so, you should start to compile evidence of safety. One way of doing this is by preparing a Safety Case. If you are preparing a Safety Case, you should define its format and start to compile it.

3.5 The Implementation phase

Figure 3-5 The Implementation phase

The activities of the previous phase continue into this one:

- The risk assessment, safety requirements and Safety Plan should be updated, as necessary.
- Safety Audit and Assessment will continue.
- Compilation of the Safety Case will continue.
Activities associated with the decommissioning and disposal of a system being replaced may be incorporated into this phase.

3.6 The Installation and Handover phase

Figure 3-6 The Installation and Handover phase

The activities of the previous phase continue into this one:

- The risk assessment, safety requirements and Safety Plan should be updated as necessary.
- Safety Audit and Assessment will continue.
3.6.1 Evidence of safety; Acceptance and approval

The Safety Approvers for a project will grant Safety Approval on the basis of inspecting evidence for safety. The Project Manager is responsible for ensuring that this evidence for safety is prepared, maintained, and submitted to the Safety Approvers. They may delegate the preparation to a Project Safety Manager but should retain overall responsibility.

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

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

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

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

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

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

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

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

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

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

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

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

If this is not the case, then the decommissioning and disposal of the system may be regarded as a change in its own right. In that case we suggest that you employ the following simplified version of the lifecycle used for building a system.

![Diagram of Decommissioning and Disposal phase]

**Figure 3-7 The Decommissioning and Disposal phase**

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

Figures 3-8 and 3-9 illustrate a typical programme of activities.

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

**Guidance**
- Plan for safely decommissioning the system at the end of its life and disposing of it.
- Identify hazards arising from decommissioning and removing the system or equipment from the railway and assess the risk to the railway.
- Identify contribution of human error to risk.

**Fundamental**
- Safety planning (ch 11)
- Identifying hazards (ch 15)
- Assessing risk (ch 15)
- Records (ch 12)
- Reducing risk (ch 17)
- Safety requirements (ch 17)

**Techniques & Tools**
- Checklist of decommissioning and disposal considerations (App C)
- Hazard identification checklists (App C)
- Techniques and tools listed against identifying hazards and assessing risk at the Requirements Definition phase may be applicable here.
- Risk assessment checklists (App C)
- Outline Hazard Log (App B)
- Checklists - Updating the Hazard Log (App C)
- Outline Safety Plan (App B)
- Checklists - Safety planning (App C)
- Checklists - Safety audit; safety assessment (App D)
- Recommended safety case structure (Table 18.1)

---

Figure 3-8 Planning Decommissioning and Disposal
Figure 3-9 Performing Decommissioning and Disposal

- **Guidance**
  - Transfer safety responsibilities
  - Handover human factors records
  - Handover Hazard Log

- **Fundamental**
  - Safety responsibility (ch 5)

- **Techniques & Tools**
  - Nothing specific but the tools and techniques of the previous phase may be applicable in cut-down form
This page has been left blank intentionally
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**

- Risk
  - Acceptable level of risk
  - Achieved level of risk
  - Maintenance implemented as planned
  - Change to maintenance plan implemented
  - Change detected
  - Degradation detected
  - Maintenance plans not co-ordinated – work not being completed

**Example of risk arising from project work**

- Risk
  - Acceptable level of risk
  - Achieved level of risk
  - Maintenance implemented as planned
  - Change to maintenance implemented for project
  - Potential risk during project work
  - Improved level of risk resulting from project
  - Change to maintenance implemented at commissioning

*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.

![Diagram of maintenance cycles](image)

**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)

**Planning Maintenance (Strategic)**

- **Guidance**
  - Establish context in which your work will be done, boundaries and interfaces
  - Identify stakeholders
  - Identify hazards associated with the parts of railway that you are responsible for and the work that you are doing
  - Record hazards in Hazard Log
  - Modify safety requirements to take account of changes (in legislation, due to faults etc.)
  - Derive maintenance strategy to meet safety requirements
  - Develop top level plan to meet organisational goals and comply with legislation.
  - Review safety and performance targets and revise as necessary
  - Review and ensure implementation of good practice and plan audits
  - Ensure you have approvals and comply with conditions
  - Develop a pro-active, systematic configuration management system / change control process

- **Fundamental**
  - Defining your work (ch 14)
  - Identifying hazards (ch 15)
  - Safety requirements (ch 17)
  - Organisational goals (ch 6)
  - Safety planning (ch 11)
  - Systematic processes and good practice (ch 11)
  - Independent professional review (ch 13)
  - Acceptance and approval (ch 18)
  - Configuration management (ch 12)

- **Techniques & Tools**
  - Asset register
  - Hazard identification checklists (App C)
  - Hazard ranking matrix (App D)
  - HAZOP (App E)
  - FMEA (App E)
  - Task analysis
  - Outline Hazard Log (App B)
  - Checklists – Updating the Hazard Log (App C)
  - Outline Safety Plan (App B)
  - Checklist – Safety audit (App D)
  - Asset register

**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)

**Figure 4-6 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)
  - Records (ch 12)

- **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).

4.9 Reviewing maintenance (strategic)

**Figure 4-7 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)
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 so 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

5.3.1 Project Manager

Some of an organisation’s work may be grouped into projects, with Project Managers taking overall responsibility for the work. The Project Manager’s safety role is to ensure the safety of the work done under their direction.

The Project Manager’s safety responsibilities may include:

- ensuring that the project conforms to all relevant ESM standards and procedures;
- ensuring that all safety activities are carried out and documented in accordance with good engineering practice; and
- ensuring that the risk associated with all project deliverables is controlled to an acceptable level.

The Project Manager will generally report to the Head of Safety on all safety issues and to the Line Manager on all management issues.

5.3.2 Project Safety Manager

For larger projects, there may be a need for a Project Safety Manager, who will take the safety responsibilities from the Project Manager. However, the Project Manager will typically retain overall accountability for the safety of the project.
5.3.3 Other roles

There may also be individuals or organisations who carry out independent professional review, such as Independent Safety Auditors and Assessors; the ‘Notified Bodies’ required by European railway interoperability directives and the ‘Competent Persons’ called for by the ‘The Railways and Other Guided Transport Systems (Safety) Regulations 2006 Guidance on Regulations’ [F.3]. The roles and responsibilities of Independent Safety Auditors and Assessors are described in Chapter 13. ORR publishes guidance on the roles and responsibilities of Notified Bodies and Competent Persons.

5.3.4 Transferring safety responsibilities within an organisation

Transfer of safety responsibilities may occur within an organisation in a number of circumstances including, the following:

- one Project Manager replaces another;
- (within a product organisation) a Project Manager hands over a completed development to a manager with a product support role; and
- (within a Transport Operator) a Project Manager hands over a completed project to the operating function.

Typically, the manager accepting responsibility will take on all the safety responsibilities that the relinquishing manager had, although the relinquishing manager will remain accountable for his or her past actions.

Many different situations may occur, but two fundamental points should be observed:

No responsibility should be transferred until the accepting manager confirms in writing that they are prepared to accept it.

The relinquishing manager should make sure that all relevant safety information is recorded and that the records are up-to-date.

Typically, the relinquishing manager will do this by assuring himself or herself that the Hazard Log for the project is up-to-date and comprehensive, and, in particular, that it records all assumptions and unresolved issues, and then by endorsing the Hazard Log (see Chapter 12 for more details on managing assumptions and on the Hazard Log).

5.3.5 Transferring safety responsibilities between organisations

Typically this occurs when a supplier completes a contract for the supply of a safety-related system. Exactly which areas of safety responsibility are transferred to the customer and which remain with the supplier will be determined by the law and the contract. The contract may leave the supplier with responsibility for maintenance, for instance, in which case associated safety responsibilities will also remain with the supplier.

In any case, the supplier will remain accountable for their past actions.

Many different situations may occur, but two fundamental points should be observed:

No responsibility should be transferred until the accepting organisation confirms in writing that it accepts the responsibility.

The supplier should make sure that all relevant safety information is recorded and that the records are up-to-date (see section 5.3.6 below).
The supplier may do this in a Safety Case, if they are preparing one. A Safety Case should include a comprehensive list of assumptions, limitations on use and any other caveats on which the conclusions of the Safety Case are based (see Chapter 18).

The information may be recorded in other places. For instance, if a supplier is developing a system which is subject to European interoperability legislation, then they will prepare a Technical File which will contain much of the information that needs to be handed over.

5.3.6 Passing on information

When a system is handed over, all information relevant to the safe operation of the system should be passed on to the organisation accepting the system. This is the responsibility of the Project Manager. In the UK, there is a legal obligation in the 'Health and Safety at Work etc Act 1974' for suppliers of safety-related articles to ensure that there is adequate information for the articles to be put into safe use.

The information handed over will typically include the following:

- system description, including details of interfaces and environmental requirements;
- hazards, precautions and safety features of the system;
- safety information for operators of the equipment or system;
- detailed instructions for the operation, servicing and maintenance of the equipment, including operating and technical handbooks, parts and spares identification lists, drawings, and so on;
- installation details, including calibration, verification testing, training requirements, inspection schedule, and decommissioning requirements;
- details of responsibilities to be transferred, including Hazard Log maintenance, training, system maintenance, and so on;
- details of items to be transferred, including hardware, software, and documentation;
- procedures for fault reporting and change control, including approval; and
- details of training requirements, including routine operation, emergency procedures, maintenance, and so on.

The Hazard Log and the Safety Case are often the most important documents. They describe the risks and how they are controlled. The system suppliers usually retain a copy, and agreement is needed on who will hold the master document.

5.3.7 Managing Human Factors

If there is a significant volume of Human Factors work within a project or programme, then a person competent in managing Human Factors should be responsible for coordinating it. The co-ordinator may be the project or programme manager, or someone appointed by them.
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 reassessment 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

In addition to project-specific and non-safety criteria, Project Managers on safety-related projects and Project Safety Managers should generally:

- have received training in ESM; and
- be a Chartered Engineer or full member of another professional organisation.

Anyone taking a leading role in the design or operation of a safety-related system should be familiar with:

- the applicable law and standards; and
- current good practice.

Some tasks may also require certain personal attributes, such as the resolve to resist any pressure to compromise safety.

### 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.
This page has been left blank intentionally
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.
This page has been left blank intentionally
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 on verbally, so that misunderstandings can be quickly resolved. However, communication of safety-related information should be done auditably, so it should be confirmed in writing afterwards.

Considerations of commercial confidence and the expense of providing certain classes of information can make passing necessary information around slow and expensive. To avoid this happening, it is often a good idea to enter into non-disclosure agreements and to agree who will pay for what at the outset of any partnership.

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]).
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

9.3.1 Managing Human Factors

You should communicate the broad range of information relating to Human Factors work.
It is common for a single individual on the railways to use a number of systems. When designing a system, the user’s interaction with other systems should be taken into account. A failure to adequately communicate information between projects may result in decisions being taken that are detrimental to the safety of the system as a whole, for instance by introducing unnecessary and unwanted inconsistencies between systems used by one person.

Key information includes:

- **Characteristics of end users, their capabilities and limitations.** In order to understand how safely a system will be used, you need to understand those who will use it.

- **How the system is intended to be used.** The manner of use and context of the system will have a significant impact on the safety of a system.

- **Details of existing and/or similar systems.** In order to identify Human Factors safety requirements, you need to understand how existing or similar systems are used.

If you employ people who will be affected by a change, you should provide those performing the Human Factors work with access to them. It is difficult to perform assessment of the Human Factors issues in a project without access to these people.

You should co-ordinate Human Factors work with the other parts of the project.

Where the same individuals use multiple systems it is important that work is co-ordinated to ensure that one system does not adversely affect their ability to use the other systems safely. For example, where two systems use the same noise to alert the driver to a problem, confusion is likely to result.

Where multiple projects are part of a wider programme you should have a programme-wide Human Factors co-ordinator. This will improve communication and visibility of Human Factors within a programme consisting of many projects. The programme-wide Human Factors co-ordinator will be responsible for making sure that projects co-ordinate their activities, and also aid the discovery of conflicts (see Chapter 5).

### 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.
This page has been left blank intentionally
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 on 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

At the beginning of a project it is necessary to decide whether the risk can be controlled through standards or whether a detailed hazard analysis or risk assessment will be needed. If it is clear that the risks can be controlled through standards, then further hazard analysis and risk assessment may not be required.

Otherwise, as decisions on the scope, functionality and design of the system are taken it is possible to improve the identification of hazards and, if necessary, to analyse their causes and consequences and, eventually, to assess the risks. In each phase of the project, the analysis should be taken as far as the available information permits, in order to provide the best support for decisions taken during that phase.

An iterative approach to analysis should therefore be taken, and the analysis will be improved and extended in step with the specification and design, with constant interaction between the two.

10.3.1 Project lifecycle

To schedule ESM activities, it is necessary to know the lifecycle of your project (that is, the sequence of phases into which it is divided).

Different lifecycles are appropriate for different sorts of project. You should adopt a lifecycle that has been proven for the sort of work that is being undertaken and relate it to the generic System Lifecycle presented in Chapter 2.

Table 10-1 shows, as an example, a relationship between the generic System Lifecycle and the lifecycle presented in CENELEC standard BS EN 50126 [F.11].
### Table 10-1 The relationship between the generic lifecycle and the lifecycle presented in CENELEC standard EN 50126

<table>
<thead>
<tr>
<th>50126 phase</th>
<th>Generic lifecycle phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Concept and Feasibility</td>
</tr>
<tr>
<td>System Definition and Application Conditions</td>
<td>Requirements Definition</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>System Requirements</td>
<td></td>
</tr>
<tr>
<td>Apportionment of System Requirements</td>
<td>Design</td>
</tr>
<tr>
<td>Design and Implementation</td>
<td>Implementation</td>
</tr>
<tr>
<td>Manufacture</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>Installation and Handover</td>
</tr>
<tr>
<td>System Validation</td>
<td></td>
</tr>
<tr>
<td>System Acceptance</td>
<td></td>
</tr>
<tr>
<td>Operations and Maintenance</td>
<td>Operations and Maintenance</td>
</tr>
<tr>
<td>Modification and Retrofit</td>
<td></td>
</tr>
<tr>
<td>Performance Monitoring</td>
<td></td>
</tr>
<tr>
<td>Decommissioning and Disposal</td>
<td>Decommissioning and Disposal</td>
</tr>
</tbody>
</table>

The relationship may be more complex. For instance:

- There may be submissions of interim, incomplete Safety Cases.
- With the staged introduction of a signalling scheme, there may be multiple Installation and Handover phases with Implementation activities in-between.
- There may be a period when the new system is running in parallel with the old one.

#### 10.3.2 Reacting to modifications and new information

Your configuration management arrangements (see Chapter 12) should establish baselines and then provide a procedure for assessing, authorising and tracking changes to these baselines. This procedure should assess the affect on safety of any proposed change and should ensure that, when a change is authorised, any necessary changes to ESM documents, including the Hazard Log, are made.

Your configuration management arrangements should provide a procedure for assessing faults discovered in baselines, defining any corrective action and then following this through. This procedure should include assessing whether any faults show the need to amend any ESM documents, including the Hazard Log, and if so ensure that the amendments are made. These procedures should make use of a Data Reporting, Analysis and Corrective Action System (see appendix E).
When the system or equipment is introduced to the railway, your management of the Hazard Log (see Chapter 12) should include a procedure for logging any incidents that occur, assessing them and defining any corrective action that is necessary to prevent them from recurring. This procedure should also assess the need to change any ESM documents.

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
This page has been left blank intentionally
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

11.3.1 Initial remarks

We recommend that any significant change to the railway should be run as a project. The safety management activities on a safety-related project should be planned and one way of doing this is to produce a Safety Plan for the project.

The Safety Plan performs two main functions:

1. it provides a detailed schedule of how safety risks will be reduced to an acceptable level (or shown already to be at an acceptable level); and
2. it provides a means of demonstrating that this has been done.

The Safety Plan should state and justify the ESM approach to be applied to the project, so that it may be considered and endorsed.

The Safety Plan may be combined with reliability, maintainability and availability plans into a System Assurance Plan. However, it is usually kept separate so that it may be submitted to the relevant Safety Approvers, who will want to focus on the safety aspects of the project and do not need to see other plans.

This chapter describes the different types of Safety Plan that may be required during a project, the process for preparing a Safety Plan, and its content.

The other chapters of this volume describe good practice in ESM activities, such as safety analysis and preparing a Safety Case.

11.3.2 The depth of safety planning

The size and depth of the Safety Plan will depend on the complexity and level of risk presented by the project. For simple and low-risk projects a brief Safety Plan defining the project personnel and justifying a simple approach may be sufficient.
Note: if you assume a project is low-risk, you should make this assumption explicit and take action to confirm it. The Safety Plan should be endorsed by the relevant Safety Approvers, regardless of the level of complexity or risk.

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

- the previous work used good practice;
- it covered all of the project risk; and
- there is no novelty in development, application or use.

The last condition may be relaxed slightly, to allow limited novelty for low-risk projects.

### 11.3.3 The safety planning process

A typical approach to the safety planning process is as follows:

1. Develop a Preliminary Safety Plan to set out an overall approach to managing safety on the project. In particular, the Preliminary Safety Plan should describe the approach for carrying out a full safety analysis and justify the competencies of key staff allocated to undertake these activities.

2. Seek endorsement of the Preliminary Safety Plan from the relevant Safety Approvers.

3. Carry out the safety analysis and produce a set of safety requirements.

4. Prepare a Safety Plan to describe how the safety requirements are to be met.

5. Seek endorsement of the Safety Plan from the relevant Safety Approvers.

6. Update this version of the Safety Plan, as appropriate, and seek re-endorsement.

Note: it may save time to seek comments from the Safety Auditor before submitting a strategy or plan to the Safety Approver.

The Project Manager is responsible for preparing the Preliminary and full Safety Plans. The Project Manager may delegate the preparation of these documents to suitably qualified and competent personnel but should retain overall responsibility.

The Safety Plan should be scoped according to the information available and the organisation of the project. It may be split into smaller plans that cover particular stages of the lifecycle, activities to be carried out by particular disciplines or the entire project. However, every project safety activity should be covered by a Safety Plan.

The primary purpose of a Safety Plan is to plan out a programme of activities to control risk. However, it is also an opportunity to inform the Safety Approvers, that is any individuals or organisations which will ultimately approve the change, of the project’s intentions and to obtain their feedback on them. Therefore, the Safety Plan should normally be submitted to the Safety Approvers for endorsement.

The Safety Plan should be updated throughout the project to reflect any changes to the planned activities that arise as a result of undertaking safety activities. Following significant updates, the Safety Plan should be re-submitted for endorsement.
Note: it is often the case, particularly with infrastructure projects where access to the railway may only be possible overnight and at weekends, that the Implementation phase may be carried out in a series of small steps. Some people refer to this as carrying out ‘stage-works’, others refer to a ‘migration’ from the initial state of the railway to its final state. If this is the case, you need to assure yourself that risk has been controlled to an acceptable level whenever the railway is returned to service after an intermediate stage. This may be relatively straightforward compared with showing that risk has been controlled to an acceptable level in the final railway, in which case it can be demonstrated using simpler processes. However, you cannot ignore this issue and need to include it in your planning from the outset.

11.3.4 Content of a Preliminary Safety Plan

This section describes the information that should be contained within a Preliminary Safety Plan.

The Preliminary Safety Plan will be a short, high-level version of the Safety Plan, produced as early in the project as possible, and describing the overall strategy and approach to reducing safety risks.

The following structure is recommended:

1 Introduction and Background;
2 Safety Analysis;
3 Key Staff;
4 Safety Audit and Assessment;
5 Safety Documentation;
6 Safety Engineering.

Each section should be brief; detailed planning will be carried out after safety requirements have been set, and documented in the Safety Plan.

The Introduction and Background should describe the aims, extent and context (see Chapter 14) of the change to be made to the railway.

The Safety Analysis section should describe the techniques to be adopted to determine the risk presented by the system or equipment and to establish safety requirements. This section should detail the competencies of key staff allocated to carry out hazard identification and analysis activities.

The Key Staff section should identify those members of staff proposed for key safety roles and justify their competence.

The Safety Audit and Assessment section should identify the competence and independence requirements for auditors and assessor. If they are known, they should be identified and shown to meet the requirements.

The Safety Documentation section should detail the documentation that will be produced. The list should include Hazard Log, Safety Plan and the safety analysis documentation and also state whether an incremental or non-incremental Safety Case is to be used.

The Safety Engineering section should describe, at a high-level, mainstream engineering steps that are being taken to reduce risk (such as redundancy, protection systems, fail-safe design principles).
11.3.5 Content of a Safety Plan

This section describes the information that should be contained within a full Safety Plan. The following structure is recommended:

1. Introduction;
2. Background and Requirements;
3. ESM Activities;
4. Safety Controls;
5. Safety Documentation;
6. Safety Engineering;
7. Validation of External Items.

A more detailed suggested outline for the Safety Plan is provided in appendix B. If another structure is used, it should cover the information described for each of the sections listed above.

For large or complex projects it may be appropriate to prepare separate plans covering one or more of these sections.

11.3.5.1 Introduction

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

11.3.5.2 Background and Requirements

This section should:

a) justify the approach taken, with reference to ESM guidance, such as this book and safety policy;
b) describe or reference a description of any safety principles underpinning the approach to safety;
c) describe the aims, extent and context (see Chapter 14) of the change to be made to the railway, and provide or refer to a summary of the system or equipment, including interfaces to other systems or projects;
d) state or provide a reference to the Safety Requirements Specification;
e) briefly describe the risk assessment criteria that will be used to derive targets for risk tolerability;
f) describe or reference the process for assigning safety functions to system elements; and

g) list any assumptions or constraints on the project or system.

Items c) and d) may be omitted from early issues, but should be included when the appropriate activities have been carried out.

11.3.5.3 ESM Activities

This section should address the following ESM issues, to the extent necessary:

1. Safety Roles and Responsibilities;
2. Safety Lifecycle;
3. Safety Analysis;
4 Safety Deliverables;
5 Safety Standards;
6 Safety Assessment;
7 Safety Audit;
8 Safety Case and Safety Approval;
9 Supplier Management;
10 Configuration Management;
11 Project Safety Training;
12 System Operation, Modification and Maintenance;
13 Decommissioning and Disposal.

The following sections describe what the Safety Plan should say about these issues.

**Safety Roles and Responsibilities**

This section should identify the key safety personnel of the project, their roles, responsibilities, qualifications and experience and the reporting lines between them.

In particular, this section should identify the personnel allocated to manage and perform the following safety activities:

- defining safety requirements;
- leading the design, implementation or validation activities;
- performing safety analysis; and
- liaising with regulatory bodies such as HMRI.

*Note: suppliers will normally liaise with HMRI via the Transport Operator.*

The Project Manager should be responsible for:

- producing a Safety Plan;
- submitting the Safety Plan to the relevant Safety Approvers;
- where necessary, attending any meetings which decide whether risk is acceptable or not;
- ensuring safety documentation is produced, as planned;
- commissioning Safety Audits and Assessments, as planned;
- initiating ESM activities, as planned;
- ensuring that all project staff have read and understood the Safety Plan;
- obtaining and allocating sufficient resources to implement the Safety Plan;
- ensuring competence of key staff; and
- co-ordinating safety activities with other parts of the organisation, and with the client.

If there is a Project Safety Manager, they will typically be delegated responsibility for:

- producing a Safety Plan;
- submitting the Safety Plan to the relevant Safety Approvers;
where necessary, attending the endorsement meeting;
ensuring safety documentation is produced, as planned;
commissioning Safety Audits and Assessments, as planned; and
initiating ESM activities, as planned.

This section should define the specific safety responsibilities of the Safety Auditor and Safety Assessor.

The Safety Auditor should audit the project to check for adequacy of the Safety Plan and compliance with the Safety Plan and any referenced standards or procedures.

The Safety Assessor should assess the project to check the adequacy of the safety requirements and that the safety requirements are being met.

Chapter 5 provides guidance on safety roles and responsibilities and Chapter 13 provides guidance on carrying out Safety Audits and Assessments.

**Safety Lifecycle**

This section should define a project lifecycle that describes the major phases of the project, and a Safety Lifecycle that specifies the order in which the safety tasks are to be carried out. The Safety Lifecycle should be derived from the guidance given in Chapter 3 on scheduling ESM activities, and should be tailored to the specific requirements of the project. The relationship between the project and Safety Lifecycles should be specified (that is, at what points in the project the safety activities will be performed).

**Safety Analysis**

This section should define the process of safety analysis to be used to determine the safety requirements for the project. The process should be tailored to each individual project.

Guidance on performing safety analysis is provided in Chapter 15 of this handbook.

For each safety analysis activity, this section should provide details of responsibilities, documentation and timing of deliverables. This section should also state the criteria used to establish the tolerability for the identified risks.

**Safety Deliverables**

This section should detail the safety-related items (other than safety documentation, see section 11.3.5.5) that are to be delivered during the project. They should include safety-related hardware and software, but may also include other items such as maintenance procedures.

**Safety Standards**

Any safety-related work should be performed within a defined Quality Management System (QMS), which is compliant with an ISO-9000 series standard.

This section should state the procedures and standards to be followed by the project. Procedures may include references to project quality and technical plans and industry, national or international standards. The plan should state the order of precedence of these procedures and standards, in case they are in conflict.
Safety Assessment

This section should schedule a series of Safety Assessments. Alternatively, the section may describe arrangements for ongoing interaction between the Safety Assessor and the project throughout the project’s duration. Either way, the activities should be sufficient to provide an authoritative, independent opinion on whether or not a project will meet its safety requirements.

The Safety Assessor should be independent of the development team. Chapter 13 provides guidance on commissioning Safety Assessments and the independence of the Safety Assessor.

This section should address the Safety Assessment of suppliers, where suppliers are involved in safety-related work for the project.

Safety Audit

This section should schedule a series of Safety Audits to check compliance of the safety processes with the Safety Plan. The Safety Auditor should be independent of the development team. This section should also address the Safety Audit of suppliers, where suppliers are involved in safety-related work for the project. Chapter 13 provides guidance on commissioning Safety Audits and the independence of the Safety Auditor.

Safety Case and Safety Approval

This section should provide or reference the completion criteria for the safety-related aspects of the project. This should include the procedures and approvals mechanisms to be adopted.

This section should make provision for the Safety Approval of the system. An endorsed Safety Case may be required for Safety Approval, in which case this section should state who will write the Safety Case, when it should be written, and which Safety Approvers will need to endorse it.

The project may agree to deliver evidence of safety in some form other than a Safety Case. For example, it is possible that a third-party safety certificate and a Safety Assessment Report may be sufficient. Any such agreement should be recorded here.

Note: if the project is developing a product, it may not be possible to identify all Safety Approvers who will approve its application in advance.

Supplier Management

This section should make provision for ensuring that the work of suppliers is managed such that the parts of the system for which they are responsible meet the overall safety requirements. Suppliers should certify their products as compliant with the appropriate specifications. Their test plans should adequately demonstrate safety features. Where appropriate, references to test plan documentation should be made from the certification documentation.

Contracted items should be subject to the same safety analyses as those built in-house. Analyses and assessments conducted by suppliers should be used as an input to system level analyses. Safety targets for contracted work should be set by the Project Manager and agreed by the supplier. The Project Manager should require the supplier to produce a Safety Plan compliant with this guidance, which the Project Manager should endorse.
This section should schedule Safety Audits and Safety Assessments of suppliers. It should include activities for assessing suppliers’ ESM and Quality Management Systems where work is being carried out under the suppliers’ systems, to ensure that they are of an acceptable standard. Chapter 8 provides guidance on discharging safety responsibilities through suppliers.

**Configuration Management**

This section should specify how configuration of system deliverables will be managed, normally referring to a separate configuration management plan for detail. This section should specify how systems, components and other equipment will be labelled to ensure that safety is not compromised by the use of faulty or untested equipment. Chapter 12 provides guidance on configuration management.

**Project Safety Training**

This section should define any training requirements of personnel scheduled to perform safety-related activities and provide a plan for a programme of training that meets the requirements.

**System Operation, Modification and Maintenance**

This section should outline processes for analysing system operation to ensure compliance with requirements. It should also describe the process and approval mechanisms for system modification and maintenance. A checklist of items to consider is provided in appendix C.

**Decommissioning and Disposal**

This section should outline plans for safely decommissioning the system at the end of its life and disposing of it. A checklist of items to consider is provided in appendix C.

11.3.5.4 Safety Controls

This section should specify all aspects of quality controls that contribute to safety, normally referring to a separate quality plan for detail. It should identify any requirements for the use of equipment in restricted areas or restrictions to be imposed on the use of equipment in open areas. These requirements may cover training, security clearance or the use of specific safety-related procedures or controls.

This section should also record the signatories for each safety deliverable produced by the project. The signatories should include:

- the originator of the deliverable;
- the approver (that is, the person who professionally accepts the technical work in the deliverable); and
- the authoriser (that is, the person who is managerially responsible, normally the Project Manager).
11.3.5.5 Safety Documentation

This section should specify whether an incremental or non-incremental Safety Case is to be used and list the safety documentation to be produced. It should also specify when it is to be produced and the personnel to be responsible for producing it. This section should provide or reference a specification of the form, content, distribution and required endorsement for each document.

11.3.5.6 Safety Engineering

This section should specify mainstream engineering steps that are being taken to reduce risk (such as redundancy, protection systems, fail-safe design principles). The engineering activities specified should be appropriate to the level of integrity that you are designing into the system.

For each phase of the project, this section should identify the methods to be used, describe how traceability, verification and validation will be addressed and identify the documentation to be produced. Each phase should be concluded with a planned verification activity (for example a programme of testing, a review or an inspection). Appendix C provides checklists for further guidance.

If the details above are specified in a separate quality plan, then this section should just refer to that plan.

The provision of specific engineering guidance is beyond the scope of this guidance. The Project Manager should draw on his or her engineering experience and competence to determine the appropriate engineering tasks for a particular project, and on best practice engineering, as defined in the relevant standards.

This section should describe how a Data Reporting Analysis and Corrective Action System (DRACAS) will be implemented. This is a system for reporting, collecting, recording, analysing, investigating and taking timely corrective action on all incidents. It should be applied from the point at which a version of the system approximating to the final, operational version is available until the system is decommissioned. It should be used by suppliers, although the supplier may implement their own DRACAS. Appendix E describes a DRACAS.

11.3.5.7 Validation of External Items

This section should specify adequate controls to ensure that the risk arising from safety-related external items (such as tools, equipment and components that have been previously developed or purchased) has been reduced to an acceptable level.

This section should specify an approval procedure for the use of external items. The procedure should include the following steps:

1. determine the extent to which the item in question will be used in a safety-related manner;
2. obtain all documentation relevant to the item;
3. assess the documentation;
4. identify the item’s capabilities and limitations with respect to the project’s requirements;
5. test the item’s safety-related features, both with, and independent to, the new system;

The acronym FRACAS is sometimes used instead

---

Uncontrolled When Printed
Document withdrawn as of 01/01/2012
6 perform a risk assessment of the use of the item; and
7 perform a Safety Assessment of the supplier of the item.

The use of external items not subject to such an approval procedure should be justified in the Safety Plan. Non-approval may be justified in the following cases:

- non-safety-related items justified as such by the reference to the Hazard Log;
- items for which there is extensive operational experience under the same conditions as the current system or equipment; or
- items for which the relevant Safety Approver has granted Safety Approval in the application in question.

A similar procedure should apply to approving the upgrade or modification of previously approved external items already in use on the project.

This section should describe the means for ensuring that any tools and equipment, on which safety relies, have been approved. It should specify any analyses, tests or demonstrations by the supplier of any external items that are carried out to satisfy the approval procedure requirements listed above. It should also identify personnel responsible for approving the specified approach to evaluating previously developed or purchased components.

### 11.3.6 Planning a safety argument for software

#### 11.3.6.1 What is and is not software?

Most of the time this is not a difficult question: it is quite clear what is software and what is not. In general, software is a sequence of instructions that are carried out by some item of hardware, normally a general-purpose computer processor.

However, there are grey areas. For example, Field Programmable Gate Array (FPGA) devices are reconfigurable logic gate networks. They are programmable, may have internal states and have complex software-like functions, and are configured using something that looks very much like a programming language.

Other systems have behaviour that is defined by configuration data, which may have many of the features of software.

The question arises whether items such as the FPGA ‘programme’ or the configuration data should be considered as software. To provide a useful answer to this question it is worth reviewing the differences between hardware and software.

Simple hardware systems have few internal states. It is generally possible to demonstrate that such systems perform as expected, through the use of logical analysis of the design, and exhaustive testing of the implementation.

Software, due to its sequential mode of operation, can change its behaviour radically based on input data. As the size of software grows, the number of states it can be in, and number of possible paths through it can grow at an exponential rate. Even for relatively simple software, the number of paths through will be very large. To fully test all the paths through the software, with all possible inputs and stored states, becomes intractable for all but the smallest programs.

This is especially the case with real-time software that uses interrupts, in which the flow of control for the software is harder to model. Systems such as interlockings are even more complex to test because there may be several distinct ‘states’, for example where there are two independent trains in the interlocked area.
We recommend a practical approach to this question. It is the complexity of software that makes it necessary to use standards like EN 50128 [F26]. Because it is generally impossible to test and/or analyse every possible path through the software, it is necessary to rely on the process used, as well as the design itself to make a safety argument.

As a rule of thumb, we suggest that if a device has few enough internal stored states that it is practical to cover them all in testing, it may be better to regard it as hardware and to show that it meets its safety requirements by analysis of the design and testing of the completed device, including exhaustive testing of all input and state combinations.

If the programmable device has the complexity of software, then some at least of the guidance in EN 50128 and IEC 61508 [F5] is likely to be useful. However, this guidance may not be applicable without modification. Several requirements (see for instance table entries A20.4, A19.3 and A12.3) assume a procedural language and so would not be directly applicable to programs written in other languages. In these cases, EN 50128 may be useful as a guide, but you will have to replace inapplicable requirements with other tools, techniques and measures that meet the same underlying need.

11.3.6.2 The safety argument for software

If the system that you are building contains software, then you will have to consider the software in the system Safety Case. You will have to include a software safety argument in the system Safety Case, unless you can show that the system design is such that:

- the behaviour of the software cannot conceivably contribute to a hazard; and
- the system does not rely on the behaviour of the software to mitigate hazardous events.

You should consider the form of this argument from the outset when designing the system and the software. A Safety Case should show that 'you have set adequate requirements and met them'. Generally, to support such a claim, you will need to show in the software safety argument that:

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

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

We consider that EN 50128 represents good practice for development of railway software, including software outside the strict scope of the standard.

Chapter 18 provides guidance on making a safety argument for software which has already been developed.
Following EN 50128 will deliver evidence that the software meets its safety requirements. However, following EN 50128 is not sufficient to demonstrate that these requirements are adequate and the safe behaviour of the software will depend upon hardware provisions. Therefore, software safety activities must be undertaken as part of a programme of activities to ensure the safety of the system as a whole, as described in this volume and EN 50129 [F6].

EN 50128 does not provide guidance on all forms of software – it assumes a procedural programming language, for example – and its treatment of software integrity is not underpinned by an agreed theoretical basis.

EN 50128 promotes a qualitative approach to software integrity, but the issue of whether software failure can be modelled probabilistically is an issue of contention.

The guidance in this section has been written to supplement the standard by pointing out some problems that people building railway systems face and how they may be overcome.

### 11.3.7 Planning Human Factors work

You should plan all Human Factors work.

At the beginning of a project you should develop a high-level strategy for the integration of Human Factors into the safety process. This will describe the general approach that will be taken throughout the project.

Once project safety requirements are known, you should plan any Human Factors work that is required. You may produce a separate Human Factors plan or treat Human Factors in a more general plan. Either way, your plan should be integrated with other project planning documents and should describe in detail the techniques to be used, the skills needed and the points at which different activities will be carried out with details of their implementation.

You should also ensure that consideration of Human Factors is integrated into the overall design process.

RSSB publish guidance on Human Factors in a rail context in [F.13].

### 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 fulfill 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.
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;
- Corruption of data;
  - Duplicate or spurious entries,
  - Erroneous/corrupt data that is structurally correct,
  - Structural faults,
  - Type or range faults,
  - Value errors where the value is plausible but wrong,
  - Referential integrity failure between data,
  - Volume, too much/little data,
  - Incorrect ordering of data.

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.

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

Project Managers are responsible for keeping adequate records of ESM activity (safety records), to provide evidence that these activities have been carried out and to record the results of these activities.

A log of all safety records and documentation, and all identified hazards and potential accidents should be maintained; this log is termed the Hazard Log.

This chapter describes the Hazard Log and other safety records that should be produced and kept. It also describes how they may be managed and controlled, so that the most up-to-date versions are available.

12.3.1 Roles and responsibilities

The Project Manager is responsible for the configuration management of all items relating to the project. The Project Manager should write a configuration management plan detailing how this will be achieved, and should ensure that it is followed. These responsibilities may be delegated but the Project Manager normally retains overall accountability.

The Project Manager will normally be responsible for setting configuration management policy and defining processes for configuration control.

The Project Manager is responsible for the creation and maintenance of the Hazard Log and other safety records until the transfer of overall safety responsibility to another party.
The Project Manager may delegate this role to a Project Safety Manager but should retain overall responsibility. Guidance on transferring safety responsibility is provided in Chapter 5.

12.3.2 Identification of configuration items

The identification of configuration items should be started during the early stages of project definition. There may be a number of hierarchical levels of items under configuration control, reflecting the system structure (though it may not be necessary to control all system items). The relationship between configuration items should be documented to provide traceability information. For example, there may be composite items consisting of smaller items; items may be derived from other items (such as design items derived from the requirements).

You should place all items which will provide evidence for safety under configuration management. You should consider placing the following items under configuration management:

- safety-related items;
- items interfacing to other systems;
- items identified as deliverables;
- documentation of enduring value, such as:
  - specifications,
  - designs,
  - drawings,
  - test specifications,
  - user and maintenance manuals,
  - other technical manuals,
- items particularly susceptible to change (for example, software); and
- items supplied by other suppliers.

The following information should be maintained for each item:

- unique identifier;
- item name and description;
- version number; and
- modification status.

All items placed under configuration management control should be indexed, and the index itself should be placed under configuration management.

Section 12.2.2 details considerations specific to software items.

12.3.3 Configuration management plan

Configuration management on a project should be planned and documented in a configuration management plan or a configuration management section of the project plan. This plan should define:

a) a list of the types of configuration items;
b) responsibilities for configuration management within the project, including the person responsible for approving updates to configuration items;

c) the baselines that will be produced;

d) the version control arrangements;

e) the change control process;

f) software configuration management arrangements (if required); and

g) any configuration management tools used.

Items c) to g) inclusive are expanded on below.

12.3.3.1 Baselines

A baseline is a consistent and complete set of configuration item versions. It should specify:

- an issue of the requirements specification;
- all of the configuration items that are derived from these requirements; and
- all the component items and their versions that the configuration items are built from.

Baselines are established at major points in the System Lifecycle as a departure point for the control of future changes.

12.3.3.2 Version control

Different versions of the same item may be needed as the system develops, to allow for different applications, both during the project (such as testing and debugging) and while in operation (such as different processors, or increased functionality).

Versions may be controlled by assigning a unique reference number, a meaningful name and a status to each version, and by monitoring changes to the versions.

Changes made to different versions should be tracked to provide and maintain a change history. In addition, superseded versions of documentation and software should be archived to allow for reference.

It should be possible to readily establish the status of a version, to tell if it has been approved for use or not. Items known to be faulty should be clearly marked as such, so that they are not used by mistake.

12.3.3.3 Change control process

Any changes to a baselined item should be assessed to identify the safety implications of the change (such as the introduction of a new hazard). Changes should be documented and should follow a process for requesting change, assessing the change and the effect that it may have on other configuration items, and reviewing the change.

12.3.4 Safety records

The extent of the safety records maintained by a project will depend on the complexity and level of risk presented by the project. The activities carried out and the records kept should be sufficient to provide a basis for controlling the risk and evidence that the risk has been controlled. Simple and low-risk projects will carry out only a small number of safety-related activities, and the records required of these will be small. High-risk and complex projects will produce more safety records.
Safety records are valuable and difficult to replace. Appropriate security and back-up safeguards should be employed to ensure their integrity.

The Hazard Log is a key safety record. Its functions include:

- detailing hazards and potential accidents;
- maintaining a list of safety records and a chronological journal of entries;
- providing traceability to all other safety records; and
- collating evidence for safety, and supporting the Safety Case, if there is one.

Figure 12-2 illustrates the relationship between the Hazard Log and other safety records.

![Figure 12-2 Pyramid of safety management documentation](image)

Note: there is variation in terminology in the industry and the phrases ‘Safety Case’ and ‘Hazard Log’ are sometimes used to include the evidence below them in Figure 12-2.

12.3.5 Management and control of the Hazard Log

The Hazard Log evolves and should be updated whenever:

- a relevant hazard or potential accident is identified;
- a relevant incident occurs;
- further information relating to existing hazards, incidents or accidents comes to attention; or
- safety documentation is created or re-issued.

The Hazard Log should be stored with the project file so that referenced material is easily accessible. Each section of the Hazard Log may be a separate document, as long as the individual documents are stored together.

The Project Manager should identify a process for updating the Hazard Log, to include project staff with authority to make entries. Each entry in the Hazard Log should be approved by the Project Manager, or delegate.

The Hazard Log should be available for inspection by the Safety Auditor, the Safety Assessor and representatives of the relevant Safety Approvers.
The Project Manager should ensure that adequate provision is made for security and back-up of the Hazard Log and other safety records.

It is not necessary to repeat information documented elsewhere, and so the Hazard Log should make reference to other project safety documentation such as analyses and reports. It is recommended that the Hazard Log be implemented electronically. Special purpose tools are available to enable this, but it is also possible to store the Hazard Log in a database, keeping Hazard Data, Accident Data, Incident Data and the Directory in separate tables. An outline Hazard Log is provided in appendix B.

12.3.6 Managing Human Factors

Your configuration management procedures should cover any Human Factors related documents and data that relate to safety. Configuration management arrangements should also cover these. Configuration management of Human Factors data and documents should be integrated with the configuration management arrangements for other project documents and data. Where changes to non-project documents, such as the Rule Book, are required to implement the project, they should be tracked.

Safety records should cover Human Factors activities, at least as far as they relate to safety. You may find it useful to maintain a database of Human Factors issues, which records the issues and the actions taken to resolve them.

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

![Diagram of typical examples of maintenance records]

**Figure 12-3 Typical examples of maintenance 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>Your maintenance organisation</td>
<td>You should keep records about the way you have set up your organisation, particularly the scope and allocation of safety responsibilities, your organisational goals, your safety culture and your competence. You should also keep records about your suppliers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The risks you have to control</th>
<th>You should keep up-to-date records of all the hazards that your maintenance work is designed to mitigate.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>We recommend that you keep details of these hazards and the arrangements to control them in a Hazard Log. You may find the guidance on structuring and managing Hazard Logs in the project section of this chapter and in appendix B; a useful starting point, but you should be prepared to adapt the guidance to your needs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> some people use the term <em>Risk Register</em> 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.</td>
</tr>
<tr>
<td>Record</td>
<td>Guidance</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.

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

We divide independent professional review into two activities:

1. Safety Audits focus on the ESM processes being used and check that they are adequate and are being followed.

2. Safety Assessments focus on the product of the project and check that the risk associated with the system being developed is (or will be) controlled to an adequate level.

In practice there is overlap between the two.

There is variation in terminology and practice in this area. Some practitioners divide up the topic of independent professional review differently and use the phrases ‘Safety Audit’ and ‘Safety Assessment’ with different meanings. For example, a distinction is sometimes drawn between technical assessment of engineering design and process assessment of safety management activities. You may need to refer to the guidance under both the audit and assessment headings, even if the activity that you are asked to commission or perform is described as one or the other type of review.

This chapter describes these two types of review and the documentation that is required by them. It also discusses how to go about commissioning a review, what the reviews should be checking for, and how the results should be used. Outlines and checklists are provided in appendices B and C respectively, and there is an example, Safety Assessment Remit, in appendix D.

The guidance in this chapter is applicable to all phases in the System Lifecycle.
This chapter is written for Project Managers who will need to commission reviews and interpret the results, and the auditors and assessors who will be performing them.

13.3.1 Safety Audits and Assessments

13.3.1.1 Safety Audits

Safety Audits are intended to check that the ESM of a project is adequate and has been carried out in conformance with the Safety Plan. If there is no Safety Plan, one should be written before a Safety Audit is carried out.

The primary output of an audit is a Safety Audit Report. This report should include:

- a judgement on the extent of the project’s compliance with the Safety Plan;
- a judgement on the adequacy of the Safety Plan; and
- recommendations for action to comply with the Plan or to improve it.

A Safety Audit should consider:

- work since the previous audit (all work so far, if first audit);
- plans for the next stage; and
- recommendations of the previous audit.

13.3.1.2 Safety Assessments

Safety Assessment is the process of forming a judgement as to whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level.

The safety requirements for the system are central to a Safety Assessment. The assessor should review the Safety Requirements Specification to assess whether it is sufficient to control risk, and review the system to assess whether or not it meets or will meet the Safety Requirements Specification.

Safety Assessment involves the use of design analysis, auditing techniques and practical assessment by competent and experienced persons.

The assessor should also review the processes and organisation employed on the project. This aspect of the assessment is easier if the results of a recent Safety Audit are available. If a Safety Audit has not been carried out on the project recently enough that its conclusions are still valid, then one should be commissioned before a Safety Assessment, to ensure that the documentation to be assessed has been produced under a correctly applied Safety Plan. If the audit results are unsatisfactory, then the assessment may be postponed until corrective action has been taken.

The result of a Safety Assessment is a Safety Assessment Report. This report should include an assessment on whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level, and recommendations for corrective action, if necessary.

If the risk is not assessed as acceptable, then the system may need to be re-assessed after corrective action is taken.
13.3.2 Commissioning a Safety Audit or Assessment

In general, the frequency and depth of each type of review and the level of independence of the reviewer (the Safety Auditor or Safety Assessor) will depend on the complexity and level of risk presented by the project. Often it may be preferable to set up arrangements for ongoing interaction between the reviewer and the project throughout the project’s duration, but it remains the case that the effort expended should be proportionate to the complexity and level of risk presented by the project.

Typically, Safety Audits and Assessments of the simplest and lowest risk projects should not take more than about a day of effort from a single auditor or assessor. Safety Audits of the most complex and highest risk projects may involve much more effort from an independent organisation.

Audits and assessments should be commissioned at the points defined in the Safety Plan (see Chapter 11). The Project Manager or Head of Safety may commission additional audits or assessments.

Whoever commissions an audit or assessment should write a Safety Audit/Assessment remit. This should record the requirements of the Audit or Assessment and all the relevant details, including:

1. the project title and reference;
2. the name of the Safety Auditor/Assessor, their qualifications and experience, and their level of independence;
3. references to previous audits and assessments;
4. audit or assessment requirements defining:
   a) the scope of the audit/assessment which may be limited in extent (for instance, to a part of the system) or in time (for instance, to changes since the last release);
   b) the purpose of the audit/assessment (for instance, to support a submission for Safety Approval);
   c) the basis of the audit/assessment. For an audit this will define the documents that the project will be audited against (normally the Safety Plan and the documents that it references). For an assessment this should specify the legal framework (for instance, the ALARP Principle is applicable to some decisions about safety in the UK) and the ESM framework (for instance, the Yellow Book) within which the project is being run; and
   d) any previous assessments or audits whose results may be assumed in the performance of the current audit/assessment.

The remit should be agreed and signed by the Project Manager and the Safety Auditor/Assessor. An outline for a Safety Audit/Assessment remit is provided in appendix B and an example generic Safety Assessment Remit is provided in appendix D.

13.3.2.1 Independence

The Safety Auditor/Assessor should be independent of the project. Whoever commissions an audit or assessment should decide the level of independence. The following paragraphs provide guidance only.

The level of independence should be dependent primarily on the level of risk presented by the project.
For some systems, principally electronic systems, this is indicated by the Safety Integrity Level (SIL) of the system or equipment being developed. (SILs are discussed in Chapter 17.)

The following tables provide guidance on the level of independence.

Table 13-1 provides guidance (derived from IEC 61508 [F.5]) on the level of independence appropriate at each SIL. This table can only be used if a SIL has been assigned to the system.

For systems for which a SIL is either not applicable, or applicable but not yet known, for example when safety requirements have not yet been set, the level of independence should depend on the likely consequence of an accident caused by the system or equipment. Table 13-2 provides guidance on the level of independence appropriate at each classification of consequence defined in Chapter 15. The nomenclature is as for Table 13-1.

Note that ‘HR’ indicates Highly Recommended, ‘NR’ indicates Not Recommended, and ‘-’ indicates no recommendation for or against; however, a lower level of independence may be chosen by agreement with the Safety Approver. For the highest risk projects the Safety Auditor or Assessor should work for an independent organisation. For the lowest risk projects they may be organisationally close to the project, but should not be working on the project.

<table>
<thead>
<tr>
<th>MINIMUM LEVEL OF SAFETY INTEGRITY LEVEL</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent Person</td>
<td>HR</td>
<td>HR</td>
<td>NR</td>
<td>NR</td>
</tr>
<tr>
<td>Independent Department</td>
<td>-</td>
<td>HR</td>
<td>HR</td>
<td>NR</td>
</tr>
<tr>
<td>Independent Organisation</td>
<td>-</td>
<td>-</td>
<td>HR</td>
<td>HR</td>
</tr>
</tbody>
</table>

**Table 13-1 Levels of independence at each SIL**

<table>
<thead>
<tr>
<th>MINIMUM LEVEL OF CONSEQUENCE</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent Person</td>
<td>HR</td>
<td>HR</td>
<td>NR</td>
<td>NR</td>
</tr>
<tr>
<td>Independent Department</td>
<td></td>
<td>HR</td>
<td>HR</td>
<td>-</td>
</tr>
<tr>
<td>Independent Organisation</td>
<td></td>
<td></td>
<td>HR</td>
<td>HR</td>
</tr>
</tbody>
</table>

**Table 13-2 Levels of independence at each consequence category**

Where the tables indicate a choice of independence (for example, Table 13-1 indicates that both Independent Person and Independent Department are Highly Recommended for a SIL 2 system), the following factors should be considered in deciding an appropriate level of independence:

- the degree of previous experience with a similar design;
- the degree of complexity;
- the degree of novelty of the design, or technology; and
- the degree of standardisation of design features.
These factors may also guide the determination of the duration of a particular Safety Audit or Assessment. For example, a system development utilising a novel technology is likely to require a more extensive Safety Audit/Assessment than a development using proven technology.

13.3.2.2 Qualifications

The Safety Auditor should have the following qualifications:

- prior experience as a Safety Auditor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- experience of process assurance (for instance, quality or Safety Audits);
- familiarity with external safety standards and procedures;
- familiarity with the legal and safety regulatory framework within which UK railways operate; and
- training in ESM.

The Safety Assessor should have the following qualifications:

- Chartered Engineer status in an engineering or scientific discipline relevant to the system or equipment;
- prior experience as a Safety Assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- demonstrable application domain experience;
- experience of process assurance (for instance quality or Safety Audits);
- familiarity with external safety standards and procedures;
- familiarity with the legal and safety regulatory framework within which UK railways operate; and
- training in ESM.

The following factors should be taken into account in establishing the relevance of experience:

- purpose of the project;
- technology and methods used; and
- integrity required of the system and accident potential.

Where a Safety Assessment is carried out by a team, the team as a whole should exhibit the necessary domain and process assurance experience, and the lead assessor as an individual should possess the other qualifications.

It is a good idea to retain the same Safety Auditor and Assessor throughout the project.

13.3.2.3 Depth of review

Engineering judgement should be applied to determine the degree to which the guidance above needs to be applied on a particular project. For the simplest and lowest risk projects, for example:
• The requirements for Safety Auditor or Assessor qualifications may be relaxed.

• Audit or Assessment activities listed in section 13.3.3 may be limited to interviewing personnel and reviewing documentation.

• The detail of the audit checklist or assessment checklist may be reduced.

• The Safety Audit or Assessment Report described in appendix B should concentrate on the findings and recommendations of the Safety Audit; the requirements and audit details sections should be brief.

The Safety Audit or Assessment Report should record and justify significant changes to the processes defined in section 13.3.3.

The Safety Assessment Report should concentrate on the findings and recommendations of the Safety Assessment; the requirements and assessment details sections should be brief.

13.3.2.4 Roles and responsibilities

The Project Manager is responsible for:

• initiating Safety Audits or Assessments when scheduled in the Safety Plan;

• preparing the Safety Audit/Assessment requirements;

• appointing an auditor or assessor acceptable to the Safety Approver;

• ensuring the auditor/assessor has appropriate access to personnel, the Hazard Log and other documents;

• commenting on the Safety Audit or Assessment Report;

• formulating any necessary improvement actions in response to the report’s recommendations;

• passing on any parts of the report which materially affect the Safety Assessment process to the Safety Approver; and

• implementing the improvement actions.

The Safety Auditor is responsible for:

• planning the Safety Audit;

• carrying out the Safety Audit; and

• preparing a Safety Audit Report.

The Safety Assessor is responsible for:

• planning the Safety Assessment;

• carrying out the Safety Assessment; and

• preparing a Safety Assessment Report.

13.3.3 The Safety Audit and Assessment processes

13.3.3.1 Performing a Safety Audit

The Safety Audit process consists of three activities:

1 planning the Safety Audit and producing an audit schedule;
executing the audit schedule;
preparing the Safety Audit Report.

The audit schedule should be produced by the Safety Auditor and endorsed by the Project Manager. Planned activities may be modified to reflect any required change of emphasis based on information gathered during the audit, although it is not always necessary for the audit schedule to be re-issued.

The schedule should be brief and should include:
- a statement of the audit requirements, according to the Audit remit, but taking into account any agreed amendments;
- identification of audit activities to be undertaken;
- identification of individuals to be interviewed;
- identification of documentation to be examined;
- audit time-scales; and
- Safety Audit Report distribution and the expected date of issue.

During audit planning the Safety Auditor should become familiar with:
- the Safety Plan;
- the findings and recommendations of any previous Safety Audits;
- details of progress since the last Safety Audit (if any);
- details of the next stage of work; and
- details of project staffing.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The audit activities should include:
- interviews with project personnel;
- examination of project documents;
- observation of normal working practices, project activities and conditions; and
- demonstrations arranged at the auditor’s request.

The evidence for compliance or non-compliance with the Safety Plan that arises from these activities should be noted for inclusion in the Safety Audit Report.

13.3.3.2 What to look for in a Safety Audit

The Safety Audit is a check for adequacy of the Safety Plan and compliance against the Safety Plan. The audit should check, therefore, that the planned project activities are being or have been carried out and in the manner and to the standards prescribed in the Safety Plan.

The Safety Auditor should derive an audit checklist for the investigation, to guide the enquiries and to record results and evidence. An outline for the checklist and an example are included in appendix D. The format of the checklist should mirror that of the Safety Plan and associated ESM activities such that each aspect of these is directly addressed by a question in the checklist. It should be in the form of a checklist with questions that may be answered ‘Yes’ or ‘No’.
The checklist should be drawn up to meet the audit requirements, using the documents referenced in the remit. The auditor should note anything that they find that is objectively wrong, whether or not it relates to a checklist item. *Note that the checklist is an aid for the Safety Auditor – it should not be completed by the project personnel.*

The audit should check that any standards or procedures called up by the Safety Plan have been correctly applied. It should also check that there is traceability from the Safety Plan to project activities that implement it.

The audit should look for documentary evidence that every safety activity has been carried out. The answer to each question on the audit checklist should be supported by documentary evidence.

All instances where there is no evidence of compliance should be documented in the Safety Audit Report along with a recommendation for remedial action. Each non-compliance should be identified in terms of the specific requirements of the Safety Plan. The auditor should classify each finding. A suggested classification is shown in section 13.3.4.

Audit findings should be documented on the checklist. Where evidence of compliance is lacking, further in-depth examination should be carried out.

Information gathered through interviews should, where possible, be verified by acquiring the same information from other independent sources.

### 13.3.3.3 Performing a Safety Assessment

The Safety Assessor should become familiar with:

- the Hazard Log;
- the Safety Plan;
- the Safety Requirements Specification;
- the findings and recommendations of any previous Safety Assessments or Safety Audits;
- details of progress since the last Safety Assessment; and
- details of the next stage of work.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The Safety Assessor should prepare an assessment plan. The plan should be brief and should include:

- a statement of the assessment requirements, according to the assessment remit, but taking into account any agreed amendments;
- identification of any dependencies on the project or others, such as access to project personnel or documents;
- identification of the assessor or assessment team, including qualifications, experience and level of independence;
- identification of individuals to be interviewed;
- management arrangements for reporting findings and reviewing, endorsing and distributing the Safety Assessment Report; and
• assessment timescales, including the expected date of issue of the Safety Assessment Report.

The assessment activities should include:
• interviews with project personnel;
• examination of project documents;
• observation of normal working practices, project activities and conditions;
• re-work of parts of the safety analysis work to check accuracy, concentrating on particularly critical areas or where the assessor has reason to suspect a problem; and
• demonstrations arranged at the assessor's request.

13.3.3.4 What to look for in a Safety Assessment

The primary objective in planning and carrying out a Safety Assessment is to make sure that you collect enough information to support a judgement on the acceptability of the risk. The following guidance may help in planning the assessment but you should also employ your professional judgement and experience to tailor the guidance to the application in hand.

The assessment should examine the development or application process, review the design decisions taken by the project staff which have safety implications and verify that risk has been controlled to an acceptable level in accordance with the safety requirements.

The Safety Assessor should derive an assessment checklist to guide the enquiries and to record results and evidence. Example checklists are presented in appendix D. The checklist should be drawn up to meet the assessment requirements, using the documents referenced in the remit. The assessor should note anything that they find that is objectively wrong, whether or not it relates to a checklist item. Note that these checklists are an aid for the Safety Assessor – they should not be completed by the project personnel.

The assessment should not just focus on documents but should look at the processes and organisation behind them. The assessor should look for any shortcomings in the approach to safety and make recommendations.

The assessment should pay particular attention to the Hazard Log, which should provide traceability from the safety requirements to documentation supporting engineering activities on the project.

The assessment should check that there is documentary evidence for every safety activity carried out. The answer to each question on the assessment checklist should be supported by documentary evidence.

If operational data is available, the assessor should analyse it for evidence of:
• hazards not previously identified;
• risks incorrectly classified;
• safety requirements not met; and
• changes in the pattern of operational use.

The Safety Assessor may call for the repetition of any formal tests and the Project Manager should arrange for these to be run under the Safety Assessor’s supervision.
If a previous assessment has been carried out and has not been invalidated by changes to the design or new knowledge, then the assessor need not repeat the analyses carried out and should concentrate instead on analysing new and changed material.

If the assessment detects a flaw in the ESM programme, then the assessor should review the ESM documentation to establish the most likely root cause. The assessor should consider whether this throws doubt on any other aspects of the ESM, and the assessment recommendations should include measures to restore confidence in the affected areas, as well as addressing the defects detected.

Information gathered through interviews should, where possible, be verified by checking the same information from other independent sources.

13.3.3.5 Findings

Findings should be communicated to the Project Manager and project team as soon as possible. You should not wait until the Safety Audit/Assessment Report is prepared and distributed.

This may conveniently be done with a simple three-part form:

- Part 1: Finding
- Part 2: Project response
- Part 3: Assessor's/auditor's comments on project response.

13.3.4 Audit/assessment findings

All auditor's and assessor's findings should be uniquely numbered and classified. The following classification scheme is widely used and is recommended. Categories 1 to 3 should be used when the audit/assessment is supporting a request for Safety Approval.

Category 1 - Issue is sufficiently important to require (substantial) resolution, prior to recommending that the change may become operational. (Alternatively a specific control measure may be implemented to control the risk in the short-term.)

Category 2 - Issue is sufficiently important to require resolution within 3-6 months, but the change may become operational in the interim (possibly with a protective control measure).

Category 3 - Issue is highlighted for incorporation into the Safety Case at the next periodic review, but no action is required separately.

Where there are a large number of lower category issues, the auditor/assessor should consider whether, in totality, they represent sufficient residual risk that they in effect equate to one or more higher category issues (that is, that they would warrant the imposition of any additional mitigating control measures). In these circumstances, it should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document that has been reviewed.

The Project Manager should review and endorse the Safety Audit/Assessment Report, and formulate improvement actions in response to the Safety Auditor's/Assessor's findings. It may be appropriate to record any faults discovered in the system itself in the Data Reporting, Analysis and Corrective Actions System (see Chapter 11). The Project Manager should implement these improvement actions.
The Safety Assessment Report may include recommendations for action by the relevant Safety Approvers, for example reviewing the approval of systems or equipment in service. If the report contains any such recommendations, the Project Manager should pass that part of the report to the relevant Safety Approvers, who should then consider any such recommendations and implement, promptly, any necessary actions.

13.3.5 Managing Human Factors

The Safety Assessor for the project should have sufficient knowledge of Human Factors, both the manner in which it affects safety and the techniques used, to assess whether the Human Factors work has been satisfactorily performed.

If Human Factors work has been integrated with the other parts of the project, it will be desirable for its assessment to be integrated with the assessment of the other parts.

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
This page has been left blank intentionally
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.

Figure 14-1 The system boundary in safety analysis

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

14.3.1 Product development

A product manufacturer may not know all the environments in which their product may be considered for application. In general, they proceed by making informed assumptions (from their own knowledge and by talking to likely customers) about the environment that their product will experience (see Figure 14-4). These assumptions should be made explicit and written down. When it comes to preparing a Safety Case for a specific application, a large part of the work required will be to check that these assumptions hold in the application in question.

![Figure 14-4 Product development](image)

14.3.2 Managing Human Factors

You should identify and describe the people who are likely to influence safety at all stages of a project. Below is a list of people that may be involved:

- the end users;
- the people the end users of the system deal with, including their customers and suppliers;
- maintainers;
- regulators;
- management.

You should assess both the required and existing competency of end users. You should assess the requirements of those who will be involved in all stages of the lifecycle of the systems affected. This will include operators, maintainers, installers, and those responsible for decommissioning.
You should assess abnormal or degraded modes of operation and mode transitions. Users are often more likely to make mistakes in these modes because they are unfamiliar and the tasks that they have to perform may be more difficult. Such modes include the transition of the system during the implementation of the change and between modes of operation. It is important that the change should be well-managed, and Human Factors will influence your ability to achieve this.

Be aware that small changes may have a significant effect when combined. It is important that small changes are assessed to ensure that either the combined effect is not significant, or that it is properly assessed in the context of the other changes taking place.

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.
Chapter 15

Identifying hazards; Assessing risk

Fundamental from volume 1: Identifying hazards

Your organisation must make a systematic and vigorous attempt to identify all possible hazards related to its activities and responsibilities.

Fundamental from volume 1: Assessing risk

Your organisation must assess the effect of its activities and responsibilities on overall risk on the railway.

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>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:
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’.
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

15.3.1 The seven-stage process

The seven-stage process that was introduced in Chapter 3 and depicted below in Figure 15-3 will form the basis of the guidance in this section.

![Seven-stage process diagram]

Figure 15-3 The seven-stage process

This seven-stage process is the approach recommended by this volume. There are alternative, effective techniques.

The steps of the seven-stage process are described in detail in Section 15.3.3.

15.3.1.1 Division of work

The seven-stage process provides an overall framework for controlling risk and demonstrating compliance with legal obligations. In practical application it is often the case that different parts of the process are performed by different organisations.

Any change to the railway can be regarded as introducing a new system or changing an existing one.

Performing the entire process requires expertise on both:

- the system, its function and design; and
- the railway environment in which the system will run.
Typically, the former expertise is provided by the **system supplier** and the latter expertise is provided by the **Transport Operator**, that is the Infrastructure Manager, or the organisation which operates the trains. Table 15-2 shows the typical division of responsibilities across the steps.

As a result of the analysis performed, the Transport Operator will typically define **tolerable hazard rates** for common applications of common systems, that is maximum acceptable rates for the occurrence of these hazards which are consistent with their legal and regulatory constraints and corporate safety objectives.

<table>
<thead>
<tr>
<th>Step</th>
<th>Transport Operator activities</th>
<th>System supplier activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard Identification</td>
<td>Provides initial hazard list</td>
<td>Confirms and extends hazard list</td>
</tr>
<tr>
<td>Causal Analysis</td>
<td>Reviews analysis</td>
<td>Performs analysis</td>
</tr>
<tr>
<td>Consequence Analysis</td>
<td>Performs analysis</td>
<td>Reviews analysis</td>
</tr>
<tr>
<td>Loss Analysis</td>
<td>Performs analysis</td>
<td></td>
</tr>
<tr>
<td>Options Analysis</td>
<td>Reviews analysis</td>
<td>Performs analysis</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Provides initial modelling data</td>
<td>Performs analysis</td>
</tr>
<tr>
<td>Demonstration of Acceptability</td>
<td>Derives acceptable/tolerable hazard rates</td>
<td>Demonstrates achievement of acceptable/tolerable hazard rates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Demonstrates risk meets any other legal criteria for acceptable risk</td>
</tr>
</tbody>
</table>

**Table 15-2 Division of work**

All parties work within agreed overall safety targets and criteria.

15.3.1.2 Iteration and preliminary hazard analysis

Safety analysis is iterative: as the design progresses, the analysis should be repeated to take account of change and extended to cover the extra detail. The design can then be modified to avoid hazards or reduce risks as soon as they are identified. The process should start as soon as a high-level description of the system is available.

A **preliminary hazard analysis** should be carried out in the early phases of the project to determine a measure of the scope and extent of the risk presented by the change.

Preliminary hazard analysis is a first-pass hazard identification and risk assessment intended to determine:
• the scope and extent of risk presented by a change, so that ESM may be applied to an appropriate depth; and

• a list of potential hazards that may be eliminated or controlled during initial design activity.

At the start of a project, design detail will almost always be limited, so the results of preliminary hazard analysis (in particular the depth of application of ESM) should be backed up and reassessed by carrying out a full analysis and risk assessment later.

Preliminary hazard analysis should be carried out before any significant design activity begins. It requires a full high-level description of the system’s function and construction and its interfaces to people and other systems.

The risk assessment activity carried out during preliminary hazard analysis should consist of annotating identified hazards with an initial appraisal of their severity and likelihood. Ideally, the preliminary hazard analysis should support the process of initial safety requirements setting and, therefore, should provide targets for the likelihood of each of the identified hazards.

The results of the preliminary hazard analysis should be used to decide where further quantified analysis is required.

The findings of preliminary hazard analysis and the decisions that result should be documented in a report.

15.3.2 Managing Human Factors in the seven-stage process

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

Identifying, assessing and reducing the risk associated with human error should be a core part of any safety process. Within this process you should address the human contribution to risk, and its mitigation (people can recover from problems as well as cause them), with the aim of controlling the system-wide risk to an acceptable level.
15.3.3 The seven-stage process – stage by stage

15.3.3.1 Stage 1: Hazard Identification

Introduction

Before conducting hazard identification, you need to understand the boundary of the system concerned and its interactions with its environment. This is discussed in Chapter 14. When performing hazard identification, you should always look out for interactions that have not been identified and which have the potential to be implicated in hazards.

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

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

Systematic identification of hazards may be performed empirically or creatively.

Empirical hazard identification

Empirical hazard identification relies largely upon knowledge and experience of the past to identify potential hazards. Whilst it is sometimes sufficient for routine undertakings, novel or modified undertakings will generally also require a more creative form of hazard identification.

Empirical hazard identification methods include:

- checklists (see appendix C); and
- structured walkthroughs.

The following more rigorous empirical methods may also be used:

- Failure Mode and Effects Analysis (FMEA) for equipment and systems (see appendix E); and
- Task Analysis for man-machine interfaces (see ‘Human-Computer Interaction’ [F.24]).

These latter techniques identify particular component failures or human errors, which may lead to hazardous circumstances. They do, however, require a detailed knowledge of the failure modes of components and sub-systems, including human actions and likely errors.

Creative hazard identification

Creative hazard identification methods provide systematic techniques to encourage lateral and imaginative creative thought. Ideally they should employ a team-based approach to exploit the diverse and complementary backgrounds of a range of individuals. They include:

- Brainstorming; and
- Hazard and Operability Studies (HAZOP) (see appendix E).
Empirical and creative hazard identification complement one another, increasing confidence that all significant hazards have been identified.

**Human Factors**

In order to identify sources of human error, you should first understand the tasks that are being carried out.

If you do not fully understand the tasks that people will perform, and the manner in which they are to be carried out, you cannot comprehensively identify where risks may originate.

There are a variety of task analysis techniques, all of which seek to decompose a task into its parts, and formally express the connections between them, such as task order, repetition, parallelism, and conditional execution of tasks.

The possible sources of error can be identified using methods that use the results of the task analysis. Generally, a form of HAZOP (Hazard and Operability Study) is used, with extensions to the normal HAZOP process (failure conditions and keywords) for dealing with the classes of errors that arise in human action. Alternatively, a variant of Failure Mode and Effects Analysis (FMEA) or Failure Mode, Effects and Criticality Analysis (FMECA) can be used.

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

Identification of error requires a multidisciplinary team who understand both the domain and the techniques.

**General remarks**

Once identified, the hazards should be listed. The record of hazards is usually maintained in a Hazard Log (see Chapter 12).

Each hazard is usually associated with several causes. If you have identified a large number of hazards, you should check to see that you have not separately identified multiple causes of a single hazard.

To focus risk assessment effort upon the most significant hazards, the hazards should be ranked. The subsequent stages of risk assessment, as detailed in this document, should be applied on a prioritised basis, beginning with the highest ranking hazards. The relative rank of each hazard should be used to guide the breadth and depth of its further analysis. A simple matrix should be employed. A sample ranking matrix is presented in appendix D.
15.3.3.2 Stage 2: Causal Analysis

Introduction

Once you have identified and ranked the hazards, you should determine those factors contributing to the occurrence of each hazard, in order to:

- enable accurate assessment of the likelihood of occurrence of each hazard; and
- help identify measures to reduce the likelihood of its occurrence.

Causal Analysis requires domain knowledge of the system or equipment. Causal Analysis generally assumes that the design material is organised as a functional hierarchy which shows how the overall system is broken down into ever smaller components.

Before the Causal Analysis can be completed, the analyst should have seen a complete set of design material, normally including but not limited to:

- physical drawings of the system;
- component lists; and
- operating and maintenance instructions.

The key factors to consider in the analysis process are:

- identification and modelling of common cause failures;
- interdependency of some errors and failures; and
- the correct logical relationships.

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

Causal Analysis may be done qualitatively or quantitatively.

Qualitative analysis

Qualitative Causal Analysis should be done to a depth sufficient to enable a realistic subjective estimate to be made of the likelihood of the hazard. It may not be necessary to go to the level of detail of failures in basic system elements in order to do this.

Quantitative analysis

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

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

Key issues are:

- obtaining reliable and accurate data;
• appropriate treatment of uncertainty in the data;
• sensitivity analysis; and
• ensuring that different Causal Factors are combined appropriately to yield consistent results (for example ensuring that two frequencies are not multiplied to yield units in terms of per time squared).

The depth of treatment of uncertainty in data sources should vary according to the nature of the hazard being assessed. For example, consider a hazard with potentially significant consequences. Suppose that a Causal Factor is identified whose occurrence leads to a high likelihood of realisation of the hazard. Significant uncertainty in estimates of the frequency of the Causal Factor are likely to result in significant uncertainty in the frequency determined for the associated hazard (and may, in turn, lead to significant underestimates of potential losses). In such cases, further analysis of the likely frequency of the Causal Factor is warranted.

Quantitative analysis should aim to minimise the significance of uncertainties. The nature and implications of all uncertainties should be carefully documented.

Where the frequencies of Causal Factors are specified with confidence intervals, accurate estimation of the likely mean and distribution of the frequency of occurrence of a hazard requires use of statistical simulation techniques.

Quantitative Causal Analysis techniques are generally based upon formal mathematical foundations and are supported by computer-based tools. However, they cannot generally handle variation in the frequencies of Causal Factors over time.

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

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

**General remarks**

Fault Tree Analysis and FMEA are techniques which may be used to perform Causal Analysis, see appendix E. EN 50129:2003 [F.6] provides guidance on identifying the failure modes of hardware items which may support these or other techniques.
15.3.3.3 Stage 3: Consequence Analysis

Introduction

In contrast to Causal Analysis, which is aimed at determining the factors which lead to the occurrence of a hazard, Consequence Analysis involves determining the possible effects of each hazard. The results of Consequence Analysis should provide an estimate of the likelihood of occurrence of each incident following realisation of the hazard in order to:

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

Like Causal Analysis, Consequence Analysis is mainly empirical, requiring domain knowledge of the system’s environment. It is generally applied to each hazard in a bottom-up manner until all potential consequences (incidents and accidents) have been determined. This leads to identification of several other intermediate states and consequences.

Key issues are:

- developing a clear understanding of the hazard; and
- determining existing physical, procedural and circumstantial Barriers to the escalation of the hazard.

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

Consequence Analysis may be done qualitatively or quantitatively.

Qualitative analysis

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

*Note: identifying all Barriers to escalation of a hazard may sometimes be used to provide only an understanding of how each incident can arise. It may not be necessary to quantify the probability of success of each individual Barrier in order to estimate the likelihood of occurrence of each incident. Rather, it may be possible to make a simple conservative estimate of the likelihood of each incident based upon the understanding gained by consequence modelling.*

Quantitative analysis

Consequence Analysis techniques typically present the results of analysis in the form of a logic tree structure. Such trees lend themselves to quantification in order to obtain an assessment of the likely frequency of predicted incidents and accidents. Event Tree Analysis and Cause Consequence Diagramming are such techniques. The latter is described in appendix E.
Quantification of consequence trees requires an objective assessment of the probability of success of each Barrier to escalation of a hazard (that is an assessment of the Barrier ‘strength’). Such assessment may be based upon historical data, the results of specific causal analysis or, where no objective data can be obtained, on the basis of expert opinion.

Key issues are:

- obtaining reliable and objective data sources for the assessment of Barrier strengths;
- appropriate treatment of uncertainty in the data sources; and
- sensitivity analysis of Barrier strengths.

The depth of treatment of uncertainty in data sources should vary according to the nature of the hazard being assessed. For example, consider a high frequency hazard with potentially significant consequences (major incidents or accidents). Uncertainty in the estimate of the strength of a Barrier may lead to uncertainty in the likelihood of occurrence of a major incident. In such cases, further analysis of the Barrier strength is warranted.

Sensitivity analysis performed upon the Barriers to escalation of a hazard can be used to determine those Barriers with the greatest effect upon the likelihood of occurrence of incidents. The uncertainty associated with estimates of the strength of such Barriers should be reduced where possible. The nature and implications of any uncertainties should be carefully documented.

Where Barrier strengths are specified with confidence intervals, accurate estimation of the likely mean and distribution of the frequency of occurrence of adverse incidents requires use of statistical simulation techniques.

In order to meet the above requirements, quantitative Consequence Analysis techniques are generally based upon formal mathematical foundations and are supported by a suite of computer-based tools.

The typical disadvantages of such techniques should be noted:

- they are generally incapable of addressing temporal variations in data, applying only if Barrier strengths remain constant over time; and
- they are generally incapable of addressing interdependencies between Barriers.

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

General remarks

It is important in Consequence Analysis to consider the full range of consequences. Do not assume that because a failure is termed a ‘Right-side Failure’ that it cannot contribute to an accident. Typically, even Right-side Failures lead to alternative, temporary methods of working, which increase risks.
15.3.3.4 Stage 4: Loss Analysis

Introduction

Loss Analysis comprises a systematic investigation of the safety losses associated with all incidents and accidents identified through Consequence Analysis.

Loss Analysis involves assessment of the losses associated with the hazards of an undertaking before considering risk reduction measures, leaving the consideration of the effect of these measures to later stages.

The losses associated with a system should be aggregated for all hazards of the system. The safety losses experienced by different groups of people (for instance passenger and trackside workers) should be aggregated separately for each group.

Loss Analysis may be carried out qualitatively or quantitatively.

Qualitative analysis

Safety losses should be estimated in terms of Potential Equivalent Fatalities per annum. In other words, all safety losses should be converted into an equivalent annual fatality figure. The current convention is as follows:

- 1 fatality = 10 major injuries
- 1 major injury = 20 minor injuries.

For example, if 1 major injury is estimated as arising from a hazard (over a year), this equates to 0.1 Potential Equivalent Fatalities.

Quantitative analysis

In order to convert safety losses into monetary values, an indication of what level of expenditure is considered to be necessary, if it would reduce risk by one fatality is required. Such a figure is often referred to as a Value of Preventing a Fatality (VPF). The VPF is a parameter intended only for supporting decisions on whether risk has been controlled to an acceptable level. It is not an estimation of the commercial loss that might follow from such a fatality and so cannot be used for purposes such as arranging insurance cover.

The total Potential Equivalent Fatalities per annum is multiplied by the VPF to yield a monetary loss per annum, for decision making purposes.

VPFs are generally set by Transport Operators. RSSB, in the ‘Railway Strategic Safety Plan 2006’ [F.25], advised its members to use a VPF of £1.5M to support decision-making during 2006.

Be aware that all benchmarks are only rough reflections of the values held by society at large. If there is significant public concern about a hazard, then you should take this into account in your decision making and it may justify precautions that would not be justified otherwise.

Human Factors

The representation of human error should be integrated with other aspects of safety analysis.

Many hazards will have both human and technical causes. In order to model the causes of hazards, it is necessary to consider both classes, and the manner in which they interact.
Standard notations for representing cause and effect, such as event and fault trees can be used to describe the sequences of events that lead to, and from, a hazard. Human error events can be integrated into these descriptions.

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

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

You should understand dependencies between human actions.

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

See 'Incorporating Human Dependent Failures in Risk Assessments to Improve Estimates of Actual Risk' [F.22] for more information on dependencies between human actions.

15.3.3.5 Stage 5: Options Analysis

Options Analysis determines options to reduce the associated losses determined during Loss Analysis. These options can typically be divided into:

- those aimed at reducing the rate of occurrence of a hazard; and
- those aimed at limiting the consequences of a hazard once it has occurred.

For each option, the costs associated with its implementation should be assessed and recorded. Only costs associated directly with implementation of the option should be estimated. The impact of potential benefits realised by the option should not be included (this will be determined in the next stage).

Demonstration of compliance with some legal criteria for acceptable risk, such as the ALARP Principle, requires that all significant potential risk reduction measures are identified and considered. Unless a comprehensive Options Analysis has been undertaken, therefore, it is not possible to demonstrate that the risk has been controlled to an acceptable level.

Options Analysis is therefore best conducted:

- using empirical and creative processes (for example checklists and brainstorming respectively) in a manner similar to that used in Hazard Identification; it should be noted that a thorough Hazard Identification process may also have identified some potential options; and
- through analysis of the results of Causal and Consequence Analysis to guide identification of potential options.
Human Factors

You should seek to design systems to help the user avoid or recover from hazards. As has been previously stated, human error is often a significant cause of hazards. However, people are also the most adaptable part of a system. A simple change to a procedure may be more effective (and faster and cheaper) in reducing system risk than a complex technical solution. However, you should demonstrate that the balance of risks does favour a procedural change; such an approach should not be used as a general excuse to not implement technical changes.

Broadly speaking there are three complementary strategies for reducing the probability of human error:

- Improve the design of the task and the equipment to avoid provoking the operator into error.
- Improve the working environment, for example, by improving procedures, removing distractions, attending to factors which might cause fatigue.
- Improve the performance of the individual, for example, by paying attention to training and competence, fitness, motivation, and safety culture.

As well as reducing people’s contribution to risk, you can improve their contribution to the mitigation of their own and other errors.

When human error is considered within the context of other system failures, it is possible to use standard methods of sensitivity analysis, such as fault tree cut sets to identify those events that have the most impact on the likelihood of a hazard, identifying how the risk can be reduced most effectively.

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

When the factors that influence the likelihood of human error have been identified, it is possible to identify measures that will help to reduce those errors. Options analysis can be used to weigh the possible error reduction methods, taking into account the cost of the measure and the effect that it will have on error rates.


When considering methods of risk reduction you should involve the system users.

A good safety process involves the system users throughout the project, investigating with them how the system may be improved, either to help them avoid error, or to mitigate other system errors.

15.3.3.6 Stage 6: Impact Analysis

Impact Analysis determines the likely effects of each option identified in Options Analysis upon the losses.
Impact Analysis revisits the previous stages, this time allowing for the effects of the option. For each option identified, the following process should be adopted:

1. Determine the impact of the option upon occurrence or escalation of a hazard.
2. On the basis of the revised Causal or Consequence Analysis, revisit the Loss Analysis of the associated hazard to determine the losses to be realised, assuming implementation of the option.
3. Calculate the difference between safety losses with and without the implementation of the option. This is the Safety Value of the change.

In some cases, an option may have the potential to mitigate hazards in other railway systems. In that case, you may increase the Safety Value of the change by the reduction in losses associated with the other system as a result of this option.

Safety Values should be determined individually for each affected population, in the same way as for Loss Analysis.

Where more than one risk reduction option has been identified, care should be taken to ensure that the dependencies between these options are properly addressed.

If the previous stages were originally done qualitatively, then they should be revisited qualitatively. If they were originally done quantitatively, then they should be revisited quantitatively.

Where quantitative analysis is employed, sensitivity parameters may be derived for each of the options through appropriate analysis of the corresponding causal or consequence models. This helps determine the most effective measures for loss reduction.

15.3.3.7 Stage 7: Demonstration of Acceptability

The guidance in this section assumes that you are working to the ALARP Principle. This principle 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.

You might have to adapt the guidance if you are working to other legal criteria for acceptable risk.

As explained in section 15.2.2.6, demonstrating compliance with the ALARP Principle involves demonstrating two separate facts:

1. that the overall risk is in the Tolerability Region, that is, below the Upper Limit of Tolerability; and
2. that risk has been reduced ALARP.

This stage can be divided into two steps, each demonstrating one of these facts.

Demonstration of compliance with Upper Limit of Tolerability

The Upper Limit of Tolerability will be defined for any given railway by some body authorised to do so. Typically, it is defined in terms of the Individual Risk experienced by a member of an affected group of people.

Upper Limits of Tolerability may be set for more than one group of people. For instance, a higher limit may be set for some employees who have entered a line of work that they know is hazardous, than is set for passengers.
Note that completing this step is not enough to show that you have reduced risk to ALARP; to do this you still need to perform the next step – Demonstration of ALARP.

Demonstration of compliance (qualitative)

A qualitative argument for compliance with the Upper Limit of Tolerability may be made on the basis of order of magnitude calculations, by showing that the changed railway presents significantly less risk than before, provided that:

- the risk was below the Upper Limit of Tolerability before the change was made;
- the Upper Limit of Tolerability has not since been reduced by a larger factor than the improvement in safety; and
- there has been no significant adjustment of safety targets between railway systems.

Justification should be made that all the above provisos are met.

In general, a qualitative argument of this form can be made by the system supplier alone, using published information on safety performance and policy for the railway. Alternatively, if a likelihood-severity matrix has been constructed for this application, a qualitative argument for compliance with the Upper Limit of Tolerability may be made by showing that:

- the risk of each hazard falls into a Tolerable or Broadly Acceptable category;
- the guidelines associated with the matrix have been followed; and
- the assumptions associated with the matrix hold for the application in question.

Demonstration of compliance (quantitative)

The quantitative approach to demonstrating compliance with the Upper Limit of Tolerability requires three steps:

1. to apportion the Upper Limit of Tolerability between railway systems;
2. to derive tolerable hazard rates for the system in question; and
3. to show that the actual system hazard rates are below the derived upper limits.

The third step is performed by direct comparison with the results of quantitative Causal Analysis.

If there are already published, authoritative tolerable hazard rates for the system (see section 15.3.1.1), the first two steps can be omitted. Otherwise they may be performed as follows.

To apportion the limit, you will normally employ an existing model of the contribution of safety risk from different railway systems. Typically, you will estimate an initial apportionment in line with historical data as follows:

- estimate what fraction of total annual risk of safety loss is attributable to the system; and
- multiply the Upper Limit of Tolerability by this fraction.

If Upper Limits of Tolerability are set for multiple groups, then this calculation will be carried out for each group.
The initial apportionment may be adjusted to meet strategic objectives for safety improvement.

Tolerable hazard rates for the system are then set so that the exposed members of each group experience an Individual Risk from the system below this limit. To confirm that this is the case, you will need to do the following for each group:

- add up the statistical average number of fatalities (F) that would occur for this group if all hazards occurred at their tolerable hazard rates;
- estimate the number of people (n) within this group exposed to the risk; and
- estimate the Individual Risk (F/n) experienced by an average person who is exposed to the risk and show that this is below the apportioned Upper Limit of Tolerability.

**Demonstration of ALARP**

To show that risk has been reduced ALARP, you have to show that no reasonably practicable options exist which have not been implemented.

A qualitative demonstration may be made relying on informed consensus from a group of experts reviewing the results of Options Analysis that all rejected options are not reasonably practicable. The reasons for this judgement should be articulated and documented.

If a quantitative approach is being followed, Impact Analysis will have calculated, using published, authoritative VPFs, a Safety Value, that is a monetary value for the improvement in safety arising from each option. Options Analysis will have estimated the net cost of implementing the option. An option may be rejected as not reasonably practicable if the Safety Value is significantly less than the cost.

*Note: this conclusion can only be made robustly if the difference between the two values is more than the total uncertainty in both of them.*
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.
This page has been left blank intentionally
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.
This page has been left blank intentionally
Part 5

Risk Control Fundamentals
This page has been left blank intentionally
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

A project carrying out safety-related work should identify the hazards and accidents that may result from the work, assess the risk associated with these, control the risk to an acceptable level and set safety requirements to ensure this level of risk is met. There is a legal requirement to assess the risks involved in safety-related work. Safety requirements should also be consistent with any targets accepted by the operator.

Safety requirements may be quantitative or qualitative. In some areas, such as software, where Systematic Failure is a particular issue, good engineering practice for meeting integrity requirements is to use Safety Integrity Levels (SILs). SILs are described in section 17.3.3 below.

The activity of establishing safety requirements follows and builds on the work described in Chapter 15. If you have not already done so, you should read the Background section of Chapter 15 as it also provides important background for this chapter.

The Safety Requirements Specification consolidates information provided by these activities into specific requirements, which form the basis against which the safety of the system is tested and assessed.
The activity of establishing requirements in general, and safety requirements in particular, is iterative.

The guidance in this chapter is applicable to all phases of the System Lifecycle from the Requirements Definition onward.

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

17.3.1 Setting safety targets

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

a) derive numerical accident targets which conform to legal criteria for acceptable risk;

b) derive hazard occurrence rate and/or unavailability targets which are consistent with (a);

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

The requirements may be apportioned further to sub-systems of the hierarchy and aligned with the system design. In general, targets for Systematic Failure should not be set below sub-system function level. Refer to IEC 61508 [F.5] or EN 50129:2003 [F.6] for further guidance on this decomposition.

Any functional requirements on the system or equipment that are necessary to reduce risk to an acceptable level should be incorporated as qualitative safety requirements.

The analyst may set other qualitative safety requirements, such as conformance to external standards and should do so whenever:

- such conformance is assumed in the calculation of safety targets; or
- such conformance is otherwise required to control risks to an acceptable level.

If the seven-stage process described in Chapter 15 is being used, then some requirements will arise from the fifth step, Options Analysis. However, requirements may also arise from relevant regulations, standards and codes of practice.

17.3.2 Apportionment of Random Failure targets

It is not generally necessary to descend the fault tree fully, that is, to set targets for base events. The analyst should set targets at a level coincident with the hierarchical breakdown of the system being developed.

17.3.3 Assignment of Safety Integrity Levels

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

However, as the complexity of designs increases, Systematic Failures contribute a larger proportion of the risk. For software, all failures are systematic. In software and some other areas where designs may be particularly complex, such as electronic design, current best practice is to make use of Safety Integrity Levels (SILs) to control Systematic Failures.
SILs are described in a number of widely-used standards, including EN 50129:2003 [F.6] and IEC 61508 [F.5] and we recommend defining SILs for systems or parts of systems for which the guidance on SILs in such standards is applicable. Otherwise, we recommend that you should use other means, such as rigorous checking, to control the risk arising from Systematic Failure.

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

SILs represent different levels of rigour in the development process and are related to approximate probability targets. Five levels are defined. There are four safety-related SILs, ranging from SIL 4, the most stringent, to SIL 1, the least stringent. Functions which are not relied upon at all to control risk may be described as having SIL 0. Each level is populated with increasingly stringent processes and techniques.

Each integrity level is associated with a target probability of failure. One widely accepted association is shown in Table 17-1, which is derived from IEC 61508 [F.5]. In most cases, you should use the Continuous/High Demand column.

The Low Demand column should only be used if demands are expected to occur:

- no more than once per year; and
- no more than twice as often as the function is tested to check that it works.

<table>
<thead>
<tr>
<th>Low Demand Mode of Operation (probability of failure on demand)</th>
<th>Continuous / High Demand mode of operation (Dangerous failure rate per hour)</th>
<th>Safety Integrity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥10⁻⁵ to 10⁻⁴</td>
<td>≥10⁻⁹ to 10⁻⁸</td>
<td>4</td>
</tr>
<tr>
<td>≥10⁻⁴ to 10⁻³</td>
<td>≥10⁻⁸ to 10⁻⁷</td>
<td>3</td>
</tr>
<tr>
<td>≥10⁻³ to 10⁻²</td>
<td>≥10⁻⁷ to 10⁻⁶</td>
<td>2</td>
</tr>
<tr>
<td>≥10⁻² to 10⁻¹</td>
<td>≥10⁻⁵ to 10⁻⁵</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 17-1 Safety Integrity Levels

Note: no target probabilities are set for SIL 0.

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

Each sub-system within the overall system will generally take the maximum SIL of all the functions that it implements. The components within that sub-system may then be allocated SILs according to the guidance given in section 17.3.4.

However, if it can be clearly demonstrated that a sub-system's functions are wholly independent of each other (that is, the immediate effects of a function's failure are restricted to that function), then these functions (or groups of functions) may be considered as sub-systems in themselves and assigned SILs accordingly. In this way, the apportionment of SILs need not be confined to physically separate units.

It is very difficult to prove functional independence within a sub-system and so it is important to take care in assigning functions to sub-systems. If possible, functions with differing SILs should be segregated either physically or logically.
Practitioners have successfully justified designs with software functions of different SIL on the same processor, although EN 50128 [F26] does not provide any support for this practice. To be able to use software functions of varying SIL on the same processor, you must be able to produce a safety argument that demonstrates that the lower SIL functions cannot influence the behaviour of those with higher SILs. This may be through mechanisms that prevent interference such as memory protection, or shown by analysis of the code, for example by demonstrating that no part of the code will write to memory outside of its designated area.

However, this can be difficult to do, and the effort required may be excessive compared with other solutions to the same problem.

Once the SIL for a sub-system has been established, then appropriate techniques to develop the sub-system to that level can be established by reference to tables in standards, including EN 50129:2003 [F.6] and IEC 61508 [F.5].

17.3.4 Apportionment of Safety Integrity Level

Having set a SIL for a function to achieve the necessary probability target, the analyst may need to apportion this between lower-level functions. By default the lower-level functions will inherit the highest SIL of the top-level functions that they support.

However, it is possible to use a redundant architecture to build high SIL systems from sub-systems of lower SIL by building in back-up or protection functions.

If the architecture ensures that a top-level function can only fail if both a main and back-up function fail and the two functions are independent, then the SIL of the top function may sometimes be higher than that of the main or back-up function.

In some cases, there may also be a combinator function (for instance, a voting scheme), which combines the results of the main and back-up functions.

Table 17-2 shows some combinations which are generally regarded as valid, provided that:

- the lower level functions are physically separated and built using different design principles, and
- the combinator suppresses any hazard for any failure of one lower level function.

Note that the combinator always inherits the top level SIL.

The table should not be repeatedly applied to allow a SIL 4 system, say, to be made of many SIL 1 systems.
### 17.3.5 Software safety requirements

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

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

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

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

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

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

Guidance on the development of software for safety-related railway applications can be found in EN 50128 [F.26] which also describes techniques appropriate to each SIL.

Evidence of validation of the software against its requirements should be produced. If EN 50128 is used, then this is documented in a software assessment report and a software validation report. This evidence will form an important part of the overall system Safety Case.
EN 50128 requires a Software Safety Requirements Specification and a Software Requirements Specification for safety-related software. It is possible to combine these into one document, but the safety-related requirements should be clearly identified.

The Software Safety Requirements Specification will play a pivotal role in the Safety Case for the system. As we noted above, you will need to show that:

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

To support this, the Software Safety Requirements Specification must be complete, precise, and intelligible to both those developing the software and those applying it. Of course, it is also desirable for the Software Requirements Specification to have all these attributes, or indeed any other Requirements Specification.

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

EN 50128 provides no method for estimating the probability of software failure. The practice of using the worst-case probability associated with the SIL of the software is not supported by the standard. We are aware that this practice has been followed on some railway systems, nonetheless. We do not endorse it, although we do not consider it to be a completely unreasonable approach as the requirements of the standard would be open to challenge if they routinely resulted in software that failed more often than this limit.

Without estimating the probability of software failure it is not possible to estimate the probability of failure of a system containing software. It is possible, however, to estimate the probability of system failure from non-software causes and to present this figure, carefully explained, together with the SILs of the system function in the Safety Case. If you are using fault trees, the probability of system failure from non-software causes can be calculated by setting the probabilities of software failure to zero, although it must be understood that this is a device for excluding software failure from the calculation, not an assumption that software does not fail.4

17.3.6 Maintenance

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

17.3.7 Managing Human Factors

You should set requirements for Human Factors. Human Factors requirements will come from several sources, including:

- client requirements;
- risk assessment;
- legislation;

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

Some of these sources will be specific to the railways.

Safety-related Human Factors requirements should be integrated with the general safety requirements.

Many aspects of Human Factors have safety connotations; however, not all Human Factors issues are safety-related. Therefore, some but not all Human Factors requirements will be safety-related. Similarly, not all safety issues have a Human Factors component.

17.3.8 The Safety Requirements Specification

The following structure is recommended for a Safety Requirements Specification:

• Introduction.
• Background. A summary of the system and project, including configuration information, where appropriate.
• Statement of safety requirements. A list of all safety requirements.
• Justification of safety requirements. The assumptions and calculations supporting the statement of safety requirements, including a record of the techniques employed, and the manner in which they were applied.
• Reference to safety documentation. References to all documents used together with version numbers.

Other effective formats are in common use. The Safety Requirements Specification does not need to be a separate document and is sometimes combined with other documents. A Safety Requirements Specification will, however, normally include at least as much information as provided in the structure above.

The Safety Requirements Specification should be submitted to the Safety Approver for endorsement.

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

The Safety Approvers for a project will grant Safety Approval on the basis of inspecting evidence for safety. The Project Manager is responsible for ensuring that this evidence for safety is prepared, maintained, and submitted to the Safety Approvers. The Project Manager may delegate the preparation to a Project Safety Manager but should retain overall responsibility.

The evidence should show that it is practical to maintain the system in a safe state and to do so safely. This may involve showing that the maintenance resources which are needed, such as procedures, test equipment, training and spares, are in place.

#### 18.3.1 Background

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

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

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

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

*Note: the phrase ‘Safety Approval’ is used by some people to describe a process during which someone accepts liability for the railway change. The phrase ‘safety acceptance’ is used to describe an endorsement without acceptance of liability. In this volume ‘Safety Approval’ is used to describe any process by which a Safety Approver grants its approval for a proposed change to the railway to proceed, regardless of the implications for legal liability.*

#### 18.3.2 Application

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

Any Safety Case should be submitted to the relevant Safety Approvers for endorsement. A complete version should be submitted and endorsed before any change is introduced to the railway. If the project is making staged changes, then several versions may need to be submitted and endorsed, each covering one or more stages, building the overall safety argument in manageable stages.

Interim versions of the Safety Case may be submitted as the project proceeds and this is generally a good idea as it makes it less likely that the Safety Approvers will raise unexpected objections at the end of the project.

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

The Safety Case should be handed over to whoever is responsible for maintaining the system so that it can inform their ESM activities.

18.3.4 Guidance on content of Safety Case

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

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

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

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

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

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

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

Goal Structuring Notation (GSN) has been found a useful technique for structuring and illustrating Safety Cases. See appendix E for further details.

18.3.5 CENELEC standard EN 50129:2003

EN 50129:2003 [F.6] defines the conditions which should be met to accept a safety-related electronic railway signalling system.

The principal normative contents of EN 50129 are:

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

Note though, that EN 50129 is not intended to provide comprehensive guidance on writing a Safety Case. It provides a structured framework for demonstrating safety but requires interpretation to deliver a convincing demonstration of safety for a railway change or product.

This volume in general, and this chapter in particular, have been written to allow the reader to comply with EN 50129 while following the guidance provided, and to help with interpreting this standard effectively.

18.3.6 Types of Safety Case

Three different types of Safety Case can be considered, see EN 50129:2003 [F.6]

1 A **generic product Safety Case** provides evidence that a generic product is safe in a variety of applications.

2 A **generic application Safety Case** provides evidence that a generic product is safe in a specific class of applications.

3 A **specific application Safety Case** is relevant to one specific application.

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

NB. EN 50129:2003 [F.6] requires that a specific application Safety Case be split into two Safety Cases: application design and physical implementation. This publication, however, does not recommend splitting the Safety Case in that way for all applications.

18.3.7 Managing Human Factors

To demonstrate that risk associated with a change has been reduced to an acceptable level, you must provide a safety argument. Because Human Factors affect the risk, the safety argument should consider Human Factors. Making Human Factors an integral part of the safety argument for a project will improve the argument.

You should have evidence to support the Human Factors parts of the safety argument.

18.3.8 Safety evidence for software

18.3.8.1 Software not developed to EN 50128

Following the process described in EN 50128, including the provisions for record keeping, will deliver evidence that a program meets its Software Safety Requirements Specification (including the specified SIL).
Sometimes it may not be practicable to follow this process. One reason may be that the designer wishes to use software that has already been developed. COTS (Commercial Off The Shelf [F.27]) and SOUP (Software Of Unknown Pedigree [F.28]), which may include software developed within your organisation (for which there is no surviving design process documentation) are classes of such software, but there are others. For brevity, we will talk about COTS in the remainder of this section, but the advice given is applicable to other classes of previously developed software.

Paragraph 9.4.5 of EN 50128 includes requirements relating to the use of COTS but following these may not be the most practicable approach in every case.

You will need to show that the COTS meets its safety requirements, including its Safety Integrity requirements. It is possible to make a convincing argument for this in many cases. However, it may be difficult for higher SILs and it is not guaranteed to be possible in every case. You should work out, at least in outline, how you will make the argument before committing yourself to using COTS.

The safety argument for COTS may be complicated by the fact that COTS often includes functions that are not required and not used. You will need to show that the presence of these functions has no hazardous side-effects. It may also be impossible for the user to find out exactly how COTS software was developed.

Activities that may deliver evidence to support your argument, include reliance on other standards, process assessment, design analysis and analysis of service record. It is usual to use a mixture of several of these.

18.3.8.2 Other standards

If you have followed another well-recognised standard for safety-related software, then you may be able to base your argument for its Safety Integrity on that. Some possible standards include:

- Mű 8004 [F.29];
- DEF-STAN 00-55 [F.19];
- IEC 61508 [F.5];
- RIA 23 [F.30].

18.3.8.3 Process assessment

Where you have not done something that EN 50128 recommends, you may still be able to claim that you have achieved the desired Safety Integrity if you have used alternative measures or techniques and you can justify a claim that they are suitable and at least as effective. Alternatively, if the process used has largely followed EN 50128 but has fallen short of its requirements in isolated areas, then it may be possible to carry out the omitted activities or generate the omitted outputs after the event. Carrying out these activities later than the standard prescribes may in some cases reduce the SIL that can be claimed, and may also lead to extra work, time and cost with little material benefit.

When developing software you should be aware that much of the data produced during software development lifecycle is easily lost but expensive to replace. Even if you have no specific plans to base a safety argument on the development process used, it may still be a good investment to keep records of the process in case you need them later.
18.3.8.4 Design analysis

Software is generally too complex, and has too many states, to prove by analysis that it behaves exactly as it should.

It may, however, be possible to show that some simple properties hold and this may be enough to show that a software safety requirement is met, or to form part of such a demonstration.

For example, it may be possible by careful analysis of the input/output statements in a program, and its control flow, to show that two output instructions will always occur in a particular order.

It may also be possible, by careful inspection of the data path for an item of data, to show that it cannot be corrupted on the way. It is generally much harder to show that it will always be delivered.

Tools exist that allow you to perform static analysis of program code, in order to prove certain properties of a system, such as the absence of run-time exceptions, or the adherence to certain coding standards.

You should bear in mind the SIL you are trying to achieve when considering whether this approach is workable and if so what tools and techniques to use.

Conclusions from analysis typically depend upon assumptions such as ‘code cannot be overwritten’ and ‘return addresses on the stack cannot be corrupted’, which you should identify and confirm. If you analyse the source code rather than the object code, there will always be an assumption about the integrity of the compiler which you will have to confirm (see Chapter 15 for more information about managing assumptions).

If the possible safety arguments are considered during the architectural design of the system it may be possible to design the system to make the safety arguments easier.

18.3.8.5 Service record

If your software is already in service, you may be able to collect some evidence for its Safety Integrity from its service record.

It may be possible to make a direct claim for the frequency of hazardous software failures without recourse to SILs from records of its operation in service, provided that you can show all of the following:

- The records of failures are thorough and accurate.
- The software is under change control and the version for which the claim is made is substantially the same as the versions for which records were kept.
- The software will be subject to a similar pattern of use to that for which records were kept.
- The total time in operation of the software is known.

The data used, needs to be either complete or a statistically valid subset. Any bias in the collection of data will invalidate conclusions drawn from it. The data needs to include information about the environment that the system was operating in, and the manner in which it was being used. If you are basing part of a safety argument upon such data, you should be able to demonstrate that the data used is of a high enough quality. This may require that the party providing the data also provides details of the collection method, sampling techniques and storage regime used.
See BS 5760 part 8 [F.31] and EN 50128 [F.26] for further specific advice on the use of previous experience.

It may also be possible to make a direct claim for the frequency of hazardous software failures, without recourse to SILs, from records of testing, provided that:

- the test inputs were random; and
- the software will be subject to a similar pattern of use to that for which it was tested.

However, it is not generally statistically valid to claim that the mean time between a hazardous failure is more than one third of the total duration of use or testing for which records were kept, and then only if no hazardous failures occurred. In practice it is difficult to make claims for a Safety Integrity better than SIL 2 using a service record or testing data.

18.3.8.6 EN 50128 and IEC 61508

EN 50128 [F.26] and IEC 61508 [F.5] both place requirements on the production of safety-related software, although the scope of IEC 61508 is wider than EN 50128 and covers topics treated by EN 50129 as well. EN 50128 is customised for railway applications and embodies good practice for both signalling and trainborne systems. In the context of the railways, EN 50128 is the primary standard that should be followed. On the whole, EN 50128 is derived from IEC 61508-3. However, there are two significant differences:

- As described in section 2.3 above, EN 50129 and IEC 61508 associate SILs with different ranges of probability of failure. In this case the requirements of IEC 61508 are more onerous.
- IEC 61508 does not define the term ‘SIL 0’. If it is used to mean non-safety-related, then designating software as SIL 0 excludes it from the scope of IEC 61508. EN 50128 does define SIL 0 and sets requirements for it, essentially setting requirements on all software in railway control and protection.

Yellow Book guidance follows IEC 61508 when associating SILs with different ranges of probability of failure and acknowledges the use of the term ‘SIL 0’ to refer to functions which are not relied upon at all to control risk.

Some aspects of the guidance in IEC 61508 and EN 50128 are difficult to interpret for software where the instructions are not executed in sequence (see appendix A).

18.3.9 Content of the Safety Case

The headings described in Table 18-1, which include all the parts required by EN 50129:2003 [F.6], are recommended for a Safety Case.

Alternative headings may be appropriate in some cases but they should cover the same topics as this structure.
1. Executive Summary
2. Introduction
3. Definition of System
4. Quality Management Report
5. Safety Management Report
   - Introduction
   - Roles and Responsibilities
   - Safety Lifecycle
   - Safety Analysis
   - Safety Requirements
   - Safety Standards
   - Safety Audit and Assessment
   - Supplier Management
   - Safety Controls
   - Configuration Management
   - Project Safety Training
6. Technical Safety Report
   - Introduction
   - Assurance of Correct Functional Operation
   - Effects of Faults
   - Operation with External Influences
   - Safety-related Application Conditions
   - Safety Qualification Tests
   - Other Outstanding Safety Issues
7. Related Safety Cases
8. Conclusion

Table 18-1 Recommended Safety Case Structure

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

18.3.10 Safety Case: Executive Summary

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

- a brief description of the change, its purpose, functionality and location;
- a summary of the safety design and development process undertaken;
- a summary of the assessment and audit processes undertaken;
- a summary of the test and operational experience; and
- a summary of the current safety status in terms of evidence obtained and unresolved hazards.
18.3.11 Safety Case: Introduction
This section should describe the aim, purpose, scope and structure of the Safety Case.

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

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

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

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

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

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

The following ESM issues should be addressed:
- Roles and Responsibilities;
- Safety Lifecycle;
- Safety Analysis;
- Safety Requirements;
- Safety Standards;
- Safety Audit and Assessment;
- Supplier Management;
• Safety Controls;
• Configuration Management; and
• Project Safety Training.

Each issue is treated in a separate section, below.

18.3.14.2 Roles and Responsibilities

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

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

18.3.14.3 Safety Lifecycle

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

18.3.14.4 Safety Analysis

This section should present a detailed discussion of the safety analysis process used on project. It should provide assurance that all foreseeable hazards have been identified, that Intolerable Risks have been eliminated and that other risks have been controlled to an acceptable level.

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

The following should be provided:

• a list of the analysis methods used and their application on the project;
• identification of the design documents referenced during the analysis work, clearly indicating the configuration and status of the design for each analysis; and
• evidence that the safety analysis process is capable of addressing the safety of future system changes.

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

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

This section should discuss the approach used to demonstrate that risk has been controlled to an acceptable level and demonstrate that the approach follows good practice.
This section should record any elements of safety policy which are relevant to the analysis. These may include agreed safety targets and latitude allowed to their contractors and suppliers to change aspects of the railway environment in which the system or equipment will run.

18.3.14.5 Safety Requirements

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

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

Any assumptions made should be stated and justified.

Evidence for compliance with the safety requirements is addressed in section 18.3.15.3 below.

18.3.14.6 Safety Standards

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

18.3.14.7 Safety Audits and Safety Assessments

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

• a description and justification of timing of the audits and assessments should be described;

• a justification that the auditors and assessors had sufficient competence and independence; and

• a justification of any decision not to take action in response to a finding or recommendation.

18.3.14.8 Supplier Management

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

18.3.14.9 Safety Controls

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

18.3.14.10 Configuration Management

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

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

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

18.3.15 Safety Case: Technical Safety Report

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

1. Introduction;
2. Assurance of Correct Functional Operation;
3. Effects of Faults;
4. Operation with External Influences;
5. Safety-related Application Conditions;
6. Safety Qualification Tests;
7. Other Outstanding Safety Issues.

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

18.3.15.1 Assurance of Correct Functional Operation, Effects of Faults, Operation with External Influences

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

These activities should be provided under three headings:

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

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

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

The Hazard Log should be used as the primary source of evidence.
These sections should show that the approach adopted controlled risk to an acceptable level.

These sections should present evidence that each Safety Requirement has been met and will remain met, or adequately justify any that have not been met or may not remain met. Such a justification should include an assessment of the residual risk presented by the non-compliance. They should include the following, where relevant:

a) evidence that the safety requirements were defined according to good practice (see Chapter 17);

b) identification and justification of major changes made to the safety requirements throughout the project;

c) a summary and reference to all analyses carried out during requirements definition;

d) evidence that high-level allocation of safety requirements to sub-systems has been carried out;

e) an explanation and justification of all use of sub-systems, prefabricated sections, dependencies on other systems and so on, which have been produced outside the direct control of the project;

f) safety evidence acquired from verification and validation of the system summarised, including the strategy and method employed and the results and evidence obtained;

g) evidence that further work or improvements identified as a result of validation and verification activities have been carried out;

h) evidence that the system has been integrated with existing systems and procedures in a safe and controlled manner;

i) evidence that commissioning activities have been examined for commissioning-specific hazards;

j) evidence that, for systems with extensive or complex hardware, software or human factors considerations, a formal hazard identification and analysis activity has been carried out;

k) practical experience of operating the system, including testing, integration, commissioning and any in-service experience summarised;

l) evidence that the hazards associated with system operation will be adequately controlled under both normal and abnormal conditions and for all modes of operation;

m) evidence that all aspects affecting safe operation and maintenance, including staffing levels, training requirements, operational management and interfaces to other systems, have been addressed;

n) evidence that response time requirements and other analogue issues, such as non-overlapping tolerances have been considered.

18.3.15.2 Safety-related Application Conditions

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

Safety qualification tests are conducted under operational conditions and may be called ‘field trials’ or ‘pilot operation’. The purpose of these tests is to gain increased confidence that the system has met its safety requirements. These tests can never be sufficient alone to demonstrate safety but can corroborate the analytical evidence presented in previous sections by showing that the results predicted by the analysis are actually achieved. They will typically check actual performance against predictions derived from this analysis.

The tests require the system to be put into operational service before final Safety Approval, therefore appropriate precautions and monitoring must be in place to ensure that safety is maintained during the testing period, including any necessary precautions against risk introduced by the monitoring. Provisional Safety Approval will normally be required before the tests can start. Safety qualification testing should never be used as a means for bringing a system into unrestricted operational service before its Safety Case is complete.

This section should record when and how the system was put into service; what precautions were in place, whether it operated with or without passengers, and what Safety Approval was obtained at each stage. Full descriptions of the tests, together with their results, should be referred to.

This section should review the fault history and status of the system or equipment as recorded in the Data Reporting, Analysis and Corrective Action System (DRACAS) and demonstrate that the test results are consistent with the conclusion in section 18.3.17 that the safety requirements have been met and that risk has been controlled to an acceptable level.

18.3.15.4 Other Outstanding Safety Issues

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

18.3.16 Safety Case: Related Safety Cases

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

18.3.17 Safety Case: Conclusion

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

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

5 The acronym FRACAS is sometimes used instead
The conclusions section should document any caveats on which the conclusion is based, including assumptions and limitations and restrictions on use. The Safety Approver may carry these forward as conditions of Safety Approval.

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.
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>Description</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. |
| **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. |
| **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>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Mode, Effects and Criticality Analysis (FMECA)</td>
<td>An extension to FMEA in which the criticality of the effects is also assessed.</td>
</tr>
<tr>
<td></td>
<td>See appendix E.</td>
</tr>
<tr>
<td>Failure Reporting, Analysis and Corrective Action System (FRACAS)</td>
<td>Another name for Data Reporting, Analysis and Corrective Action System</td>
</tr>
<tr>
<td>fault</td>
<td>A fault is a defect in a system, product or other change which may cause a failure.</td>
</tr>
<tr>
<td>Fault Tree Analysis (FTA)</td>
<td>A method for representing the logical combinations of various states which lead to a particular outcome (top event).</td>
</tr>
<tr>
<td></td>
<td>See appendix E.</td>
</tr>
<tr>
<td>Goal Structuring Notation (GSN)</td>
<td>A method for representing safety arguments in diagrammatic form.</td>
</tr>
<tr>
<td></td>
<td>See appendix E.</td>
</tr>
<tr>
<td>handover</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Note: this process is referred to as ‘Handback’ within the main line railway.</td>
</tr>
<tr>
<td>hazard</td>
<td>A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product.</td>
</tr>
<tr>
<td></td>
<td>Note: this broadly corresponds to a ‘precursor (cause)’ in the RSSB Safety Risk Model.</td>
</tr>
<tr>
<td>Hazard and Operability Study (HAZOP)</td>
<td>A study carried out by application of guide words to identify all deviations from the design intent with undesired effects for safety or operability.</td>
</tr>
<tr>
<td></td>
<td>See appendix E.</td>
</tr>
<tr>
<td>Hazard Log</td>
<td>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.</td>
</tr>
<tr>
<td>Head of Safety</td>
<td>A person responsible for dealing with general safety issues throughout an organisation.</td>
</tr>
<tr>
<td>Human Factors</td>
<td>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.</td>
</tr>
<tr>
<td>incident</td>
<td>Unplanned, uncontrolled event, which under different circumstances could have resulted in an accident.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Individual Risk</td>
<td>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.</td>
</tr>
<tr>
<td>Infrastructure Manager</td>
<td>An organisation responsible for managing railway infrastructure.</td>
</tr>
<tr>
<td>Intolerable Risk</td>
<td>A risk which cannot be accepted and must be reduced.</td>
</tr>
<tr>
<td>loss</td>
<td>A measure of harm.</td>
</tr>
<tr>
<td>maintenance</td>
<td>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.</td>
</tr>
<tr>
<td>Potential Equivalent Fatality (PEF)</td>
<td>A convention for aggregating harm to people by regarding major and minor injuries as being equivalent to a certain fraction of a fatality.</td>
</tr>
<tr>
<td>Project Manager</td>
<td>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).</td>
</tr>
<tr>
<td>Project Safety Manager</td>
<td>The person responsible for safety on a project and for producing all safety-related documentation.</td>
</tr>
<tr>
<td>Random Failure</td>
<td>A failure resulting from random causes such as variations in materials, manufacturing processes or environmental stresses.</td>
</tr>
<tr>
<td>reliability</td>
<td>The probability that an item can perform a required function under given conditions for a given time interval.</td>
</tr>
<tr>
<td>remit</td>
<td>Terms of reference, in particular for a Safety Audit or Safety Assessment.</td>
</tr>
<tr>
<td>Right-side Failure</td>
<td>A failure which does not result in the protection provided by a signalling system being reduced.</td>
</tr>
<tr>
<td>risk</td>
<td>Combination of the likelihood of occurrence of harm and the severity of that harm.</td>
</tr>
<tr>
<td>risk assessment</td>
<td>Making an assessment of the risk arising from one or more hazards.</td>
</tr>
<tr>
<td>Risk Assessment Report</td>
<td>A document containing an analysis of the risk arising from one or more hazards.</td>
</tr>
<tr>
<td>safety</td>
<td>Freedom from unacceptable risk.</td>
</tr>
</tbody>
</table>

*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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Case</td>
<td>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. Early issues may present analysis and assessment information, plans and requirements.</td>
</tr>
<tr>
<td>Safety Certificate</td>
<td>A certificate authorising system, product or other change for use.</td>
</tr>
<tr>
<td>Safety Control</td>
<td>A quality control with the potential to reveal hazardous faults.</td>
</tr>
<tr>
<td>Safety Engineering</td>
<td>The application of technical methods to ensure achievement of the safety requirements.</td>
</tr>
<tr>
<td>Safety Integrity</td>
<td>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.</td>
</tr>
<tr>
<td>Safety Integrity Level (SIL)</td>
<td>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.</td>
</tr>
<tr>
<td>Safety Lifecycle</td>
<td>The additional series of ESM activities carried out in conjunction with the System Lifecycle for safety-related systems.</td>
</tr>
<tr>
<td>Safety Management System</td>
<td>A systematic and documented approach to managing safety.</td>
</tr>
<tr>
<td>Safety Plan</td>
<td>A document detailing the activities to be carried out, and responsibilities of people to ensure the safety of work being carried out.</td>
</tr>
<tr>
<td>safety planning</td>
<td>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.</td>
</tr>
<tr>
<td>Safety Records Log</td>
<td>A reference to every safety document produced and used by a project.</td>
</tr>
<tr>
<td>Safety Requirements Specification</td>
<td>Specification of the requirements that a product, system or change to the railway must satisfy in order to be judged safe.</td>
</tr>
<tr>
<td>safety standard</td>
<td>A document which establishes criteria or requirements by which the safety of products or processes may be assessed objectively.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Safety Value</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>See accident severity.</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 provides suggested document outlines for the following ESM documents:

1. Safety Plan (see Chapter 11)
2. Hazard Log (see Chapter 12)
3. Safety Assessment and Audit remits (see Chapter 13)
4. Safety Assessment and Audit Reports (see Chapter 13)

The outlines do not show administrative document sections such as change history, terminology and referenced documents sections, which should be added according to your own document standards.
B.1 Outline Safety Plan

The scope and coverage of this outline is designed to be consistent with the CENELEC standard EN 50126 [F.11]. This is one of a group of European standards for safety within the rail industry. EN 50126 defines a process for the management of Reliability, Availability, Maintainability, and Safety (RAMS). The letters in square brackets refer to the CENELEC requirement detailed in clause 6.2.3.4 of EN 50126.

The recommended structure for the Safety Plan is as follows:

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Aims and objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(describe the aims and objectives of this Safety Plan for readers unfamiliar with ESM or this project)</td>
</tr>
<tr>
<td>Scope [b]</td>
<td>(include the lifecycle phases this Safety Plan addresses)</td>
</tr>
<tr>
<td>Structure</td>
<td>(describe the structure of the plan)</td>
</tr>
</tbody>
</table>

**Background and Requirements**

<table>
<thead>
<tr>
<th>Summary of system [c, m]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(include, or refer to, a description of the extent and context of the system, including interfaces to other related programmes)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outline of project [a]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a brief description of the aims and conduct of the project and the ESM approach taken, including a statement of compliance with the organisation's safety policy, or a justification of an alternative approach, the risk assessment criteria that will be used and a description of or reference to the process for assigning safety functions to system elements)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safety requirements [f]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a summary of the safety requirements or a reference to them and a description of the process by which the safety requirements were established and maintained; where none are available the Safety Plan should indicate how and when the safety requirements are to be determined)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk assessment criteria [f]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a brief description of the criteria used to derive risk tolerability targets for the system)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assumptions and constraints [n]</th>
</tr>
</thead>
<tbody>
<tr>
<td>(list any assumptions or constraints on the system or the project)</td>
</tr>
</tbody>
</table>
Safety Roles and responsibilities [d, f]
(indicate and justify Competence and independence of appointments)

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

Safety Lifecycle [e]
(describe and relate the project and Safety Lifecycles)

Safety Analysis [f]
(describe and justify the approach, see Chapter 15)

Safety Deliverables [g]
(justify exclusion of key deliverables)

Safety Standards
(justify use of Safety Standards on project)

Safety Assessments [f, p]
(justify frequency of assessments)

Safety Audits [f, p]
(justify frequency of audits)

Safety Case and Certification [h, i]
(describe certification requirements additional to those of ESM)

Contractor Management [o]
(refer to contractor-produced plans and other documentation, where appropriate)

Configuration Management
(refer to technical and quality planning documentation, where appropriate)

Safety Training
(including contractors, where appropriate)

System Operation, Modification and Maintenance [j, k]
(briefly describe, or refer to, process and approval mechanisms for analysing operation, system modification, and performing system maintenance)

Decommissioning and Disposal
(describe arrangements for decommissioning the system at the end of its lifecycle and disposing of it)
Safety Controls [p] (define controls, for instance formal review, approvers and standards for safety deliverables), including:

- Hazard Log;
- Hazard Analysis;
- Risk Assessment;
- Safety Req Spec; and
- Safety Case.

Safety Documentation [f, l] (describe production, approval and maintenance of each document; justify any not produced), including:

- Preliminary Hazard Analysis;
- Risk Assessment Report;
- Hazard Log;
- Safety Requirements Specification;
- Safety Audit and Safety Assessment Reports;
- Safety Case;
- Design and Test Specifications;
- Review reports;
- Testing and Acceptance records; and
- Training records.

Safety Engineering [f] (indicate activities to meet and validate safety requirements for each phase of the lifecycle, including DRACAS arrangements)

Validation and Verification of External Items [f] (specify an approval procedure for the use of external items and justify a decision to not validate and verify any external items)
B.2 Outline Hazard Log

The scope and coverage of this outline is designed to be consistent with the CENELEC standard EN 50126 [F.11]. The Hazard Log contains the following sections:

The recommended structure for the Hazard Log is as follows:

**Introduction**

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

The following should be included:

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

**Journal**

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

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

If the Hazard Log is stored in a database, then it may be possible to use the intrinsic change recording facilities to maintain a Journal semi-automatically.
The **Directory**, sometimes known as the Safety Records Log, should give an up-to-date reference to every safety document produced and used by the Project. The documents referred to should include (but not be limited to) the following, where they exist:

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

For each document the Directory should include the following:

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

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

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

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

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

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

Accident Data

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

- a unique reference;
- a brief description of the potential accident;
- a reference to a report giving a full description and analysis of the accident sequence;
- a categorisation of the accident severity and the highest tolerable probability of the accident (the accident probability target); and
- a list of the hazards and associated accident sequences that could cause the accident.
### B.3 Outline Safety Audit and Assessment remits

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

<table>
<thead>
<tr>
<th>Safety Auditor/Assessor</th>
<th>The name of the auditor/assessor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independence</td>
<td>Requirements for auditor/assessor independence.</td>
</tr>
<tr>
<td>Qualifications and Experience</td>
<td>Requirements for auditor/assessor qualifications and experience.</td>
</tr>
<tr>
<td>Requirements</td>
<td>Requirements for the audit/assessment itself, including:</td>
</tr>
<tr>
<td></td>
<td>• the scope of the audit/assessment;</td>
</tr>
<tr>
<td></td>
<td>• the purpose of the audit/assessment;</td>
</tr>
<tr>
<td></td>
<td>• the documents that the project will be audited against, and the prevailing legal framework for accepting risk; and</td>
</tr>
<tr>
<td></td>
<td>• any previous assessments or audits which should be taken into account.</td>
</tr>
<tr>
<td>Other Information</td>
<td>As required.</td>
</tr>
<tr>
<td>Report to be issued by</td>
<td>Target date.</td>
</tr>
<tr>
<td>Commissioned by:</td>
<td>Name of person commissioning the audit/assessment.</td>
</tr>
</tbody>
</table>
B.4 Outline Safety Audit and Assessment reports

B.4.1 Outline Safety Audit Report

The following structure is recommended for an audit report:

**Summary**
Management summary of the rest of the document.

**Requirements**
This section should state the audit requirements and identify any areas where the audit deviated from it.

**Audit Details**
This section should provide details of the conduct of the Safety Audit, such as who was interviewed and what was examined.

**Findings**
This section should list each finding and should discuss its impact. Evidence to support each finding should be given.

Chapter 13 contains a suggested classification for findings.

**Conclusions and Recommendations**
This section should include a judgement on the extent of the Project’s compliance with the Safety Plan and a statement about the adequacy of the safety requirements. The degree of compliance may be graded as:

- unqualified compliance with the Safety Plan;
- compliance qualified by the need for implementation of minor recommendations that are based on each non-compliance of minor impact;
- non-compliance requiring implementation of major recommendations that are based on each non-compliance of major impact, followed by a subsequent Safety Audit.

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

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

The audit report should provide evidence to justify the Safety Auditor’s findings and conclusions. The report should be dated and signed by the Safety Auditor.
B.4.2 Outline Safety Assessment Report

The following structure is recommended for an assessment report:

**Summary**
Management summary of the rest of the document.

**Requirements**
This section should state the assessment requirements and identify any areas where the assessment deviated from it.

**Assessment Details**
This section should provide details of the conduct of the Safety Assessment, such as who was interviewed and what was examined.

**Findings**
This section should list each finding and should discuss its impact. Evidence to support each finding should be given.

Chapter 13 contains a suggested classification for findings.

**Conclusions and Recommendations**
This section should state the Safety Assessor’s opinion as to the degree of compliance of the system or equipment with its safety requirements, in one of the following four forms:

a) The Safety Assessor concludes that the system meets its safety requirements.

b) The Safety Assessor concludes that the system will meet its safety requirements provided that specified recommendations are carried out and without a further assessment.

c) The Safety Assessor cannot be sure that the system will meet its safety requirements.

d) The Safety Assessor concludes that the system does not meet its safety requirements.

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

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

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

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

The assessment should identify any non-compliances with respect to the relevant standards and legal requirements.
This page has been left blank intentionally
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.
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?
d) Have these incidents involved changes to the information on which the Safety Case was based (thereby requiring a reworking of the Safety Case)?

e) Have all changes to the Safety Case been approved by the Safety Approver?

f) Has all operational support documentation with safety connotations been reviewed during this phase?

g) Have these reviews caused changes to the information on which the Safety Case was based (thereby requiring a reworking of the Safety Case)?

h) Has all safety-related documentation necessary for the use of the operational support team been handed over?

i) Has all training documentation in safety aspects been reviewed and approved?

j) Have all Procedures, Work Instructions and method statements required been defined and approved, including any variations to existing standards?

k) Have all required as-built diagrams, drawings, photographs and other documentation been supplied?

l) Has all required training for the operational team been carried out?

m) Has a formal channel of communication been established between the operational support team and the development team to ensure that data about operational safety is fed back into the future developments?

C.2 Safety planning

These checklists have been produced to assist the creation and evaluation of the ESM Activities section of the Safety Plan. They provide guidance on safety planning for safety activities throughout the System Lifecycle.

The Safety Plan should define responsibilities and timescales for each ESM activity scheduled.

C.2.1 General considerations

The safety-related activities listed below should be considered throughout the lifecycle:

a) Maintain Hazard Log;

b) Revisit Safety Plan and update and re-issue where appropriate;

c) Revisit safety analysis work and re-issue all affected documentation, as appropriate;

d) Establish criteria for risk tolerability;


C.2.2 Concept and feasibility

a) Preliminary Hazard Analysis scheduled;

b) Analysis of safety implications of each proposed technical approach scheduled;

c) Production of report on this analysis scheduled;

d) Guidance provided on safety analysis (Chapter 15) considered.
C.2.3 Requirements definition
   a) Guidance provided on establishing safety requirements (Chapter 17) considered;
   b) Production of acceptance test plan scheduled.

C.2.4 Design
   a) Design techniques and procedures specified;
   b) Standards for the production of design documentation specified;
   c) Allocation of safety requirements to top-level sub-systems scheduled;
   d) Allocation of random and systematic elements of the hazard probability targets to high-level sub-systems scheduled;
   e) Diagrammatic method of allocation referred to in item d) above described;
   f) Guidance provided on Risk Assessment (Chapter 15) considered;
   g) Re-use of sub-systems and/or components clearly identified and justified;
   h) Plans for the review and testing of built components and documentation scheduled;
   i) System integration plan production scheduled;
   j) Occupational Health and Safety issues, related to operation and maintenance, considered;
   k) Production of validation and verification plan scheduled;
   l) Independent formal reviews of design and its associated design documentation against safety requirements scheduled.

C.2.5 Implementation
   a) Implementation techniques specified;
   b) Procedures, standards and working practices specified;
   c) Automatic testing tools and integrated development tools specified;
   d) Occupational Health and Safety issues, related to operation and maintenance, considered;
   e) Review of validation and verification plan scheduled;
   f) Implementation of reviewed verification plan scheduled.

C.2.6 Installation and handover
   a) Strategy for installation and handover defined;
   b) States for start-up, steady-state (normal operation), shut-down, maintenance and abnormal operation addressed;
   c) Required approvals of acceptance plan specified (should include client);
   d) Requirement for client attendance at acceptance testing specified;
   e) Independence of acceptance testing team defined;
   f) Requirements for acceptance testing documentation defined;
g) Means of safe and controlled integration of the system with existing systems and procedures defined;

h) Start-up of the system addressed;

i) Parallel operation of the replacement system and the existing system addressed;

j) Sub-system versus full system switch-overs addressed;

k) Cross-validation of results between existing and replacement systems addressed;

l) Fallback to the existing system if the replacement system fails addressed;

m) Safety training required for operators, users, maintainers and managers of the system identified;

n) Means of ensuring system integrity following installation defined;

o) Inspections and Safety Assessments scheduled, where appropriate;

p) Guidance provided on transfer of safety responsibility (Chapter 5) considered;

q) All documentation or manuals that provide operational or maintenance support to ensure safe operation of the system identified;

r) Occupational Health and Safety issues, related to operation and maintenance, considered;

s) Approval authorities for support material identified;

t) Reviews of support material scheduled.

C.2.7 Operations and maintenance

a) Maintenance plan included or referred to;

b) Plan agreed by Project Manager and Operations Manager;

c) Testing and auditing of the system scheduled;

d) Routine actions which need to be carried out to maintain the ‘as designed’ functional safety of the system or equipment identified;

e) Actions and constraints required during start-up, normal operation, foreseeable disturbances, faults or failures, and shutdown to ensure safety identified;

f) Records which need to be maintained, showing results of maintenance, audits, tests and inspections identified;

g) Records which need to be maintained on hazardous incidents (or incidents with the potential to create hazards), system failure and availability rates identified;

h) Actions to be taken in the event of hazards, incidents or accidents occurring identified;

i) Comparisons of system performance with design assumptions scheduled;

j) Procedure for assessing deviations for safety implications and for proposing modifications defined;

k) Procedures for modifying the system in-service defined;

l) System performance below tolerable risk addressed;

m) Identification of systematic faults addressed;
n) New or amended safety legislation identified and taken into account;

o) Modifications to the safety requirements addressed;

p) Need for analysis of the effect of a proposed modification on system safety addressed;

q) Approval of modification implementation plan defined;

r) Need for maintenance of documentation effected by modifications highlighted;

s) Inspection, testing and/or analysis of modifications addressed;

t) Occupational Health and Safety issues, related to operation and maintenance, considered;

u) Criteria for withdrawal of the system from service identified.

C.2.8 Decommissioning and disposal

a) Safety-related considerations for decommissioning the system or equipment identified;

b) How the system or equipment is to be removed, including the safe disposal of any hazardous material addressed;

c) The phasing in of any replacement system or equipment addressed;

d) Any gaps in the level of service provided by removing the system or equipment addressed.

C.3 Updating the Hazard Log

These checklists have been produced to assist the use and evaluation of the Hazard Log.

C.3.1 How to enter new hazard data

In the Hazard Data section:

a) New reference created;

b) Hazard briefly described;

c) Reference to full description and analysis provided;

d) Assumptions recorded;

e) Severity category of related accident recorded;

f) Likelihood of hazard and related accident recorded;

 g) Random probability of hazard recorded;

h) Target likelihood recorded;

i) ‘Open’ hazard status recorded;

j) Name of person or company responsible recorded;

k) Actions for risk reduction recorded.

In the Journal section:

a) Date recorded;
b) New journal entry number created;
c) Name of person entered;
d) Journal entry described as ‘New hazard identified’;
e) New hazard referenced.

C.3.2 How to modify existing hazard data
In the Hazard Data section:
a) Hazard reference identified;
b) New hazard data recorded;
c) Latest hazard status recorded;
d) Any actions for further risk reduction recorded.
In the Journal section:
a) Date recorded;
b) New journal entry number created;
c) Name of person entered;
d) Journal entry described as ‘Modification to hazard data’;
e) Affected sections referenced.

C.3.3 How to enter new incident/accident data
In the Incident/Accident Data section:
a) New reference created;
b) Incident/accident briefly described;
c) Reference to full description and analysis provided;
d) Incident/accident severity category recorded;
e) Incident/accident probability target recorded;
f) Causes of incident/accident recorded.
In the Journal section:
a) Date recorded;
b) New journal entry number created;
c) Name of person entered;
d) Journal entry described as ‘New Incident’ or ‘New Accident’;
e) New hazard referenced.

C.3.4 How to modify existing incident/accident data
In the Incident/Accident Data section:
a) Incident/accident reference identified;
b) New incident/accident data recorded.
In the Journal section:
   a) Date recorded;
   b) New journal entry number created;
   c) Name of person entered;
   d) Journal entry described as ‘Modification to accident/incident data’;
   e) Modified accident/incident referenced.

C.3.5 How to enter directory data

In the Directory
   a) New reference created;
   b) Document title recorded;
   c) Current version number and issue date recorded;
   d) Physical location of document recorded.

In the Journal section
   a) Date recorded;
   b) New journal entry number created;
   c) Name of person entered;
   d) Journal entry described as ‘New document’;
   e) New document referenced.

C.3.6 How to modify existing directory data

In the relevant section
   a) Document reference identified;
   b) New document data recorded.

In the Journal section
   a) Date recorded;
   b) New journal entry number created;
   c) Name of person entered;
   d) Journal entry described as ‘Modification to document entry’;
   e) Modified document entry referenced.

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 provides examples of the following:

1. Hazard ranking matrix (see Chapter 15)
2. Risk assessment (see Chapter 15)
3. Safety Assessment Remit (see Chapter 13)
4. Safety Audit checklist (see Chapter 13)
5. Safety Assessment checklist (see Chapter 13)
D.1 Example hazard ranking matrix

The following are examples of matrices that may be used in the initial ranking of hazards. The higher the rating, the more priority should be assigned to the hazard.

Matrix A is commonly used and has been successfully applied, but Matrix B is preferred by some practitioners as it assigns the same rank to risks which are associated with a similar number of equivalent fatalities per year. Matrix C assigns similar ranks to risks, which are associated with a similar number of equivalent fatalities per year, but is biased to assign higher ranks to risks with more severe consequences.

Other practitioners prefer to use matrices which divide the hazards into a small number of broad categories, such as those described in Chapter 15.

<table>
<thead>
<tr>
<th>Severity of Potential Harm/Loss</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5= Daily to monthly</td>
<td>25</td>
<td>20</td>
<td>15</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>4= Monthly to yearly</td>
<td>20</td>
<td>16</td>
<td>12</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>3=1 to 10 yearly</td>
<td>15</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>2=10 to 100 yearly</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>1= Less than 100 yearly</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table D-1 Example hazard ranking matrix (A)

<table>
<thead>
<tr>
<th>Severity of Potential Harm/Loss</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5= Daily to monthly</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>4= Monthly to yearly</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>3=1 to 10 yearly</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>2=10 to 100 yearly</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>1= Less than 100 yearly</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Table D-2 Example hazard ranking matrix (B)
### D.2 Risk assessment

#### D.2.1 Introduction

The example presented in this appendix is provided to illustrate application of the risk assessment framework detailed in this document. The example does not necessarily relate to actual operational circumstances and the data used within the example is provided for the purposes of illustration only. In order to simplify the example, some crude assumptions have been made that are unlikely to apply in practice. This example assumes that the ALARP Principle applies.

#### D.2.2 Background to example

The undertaking subject to analysis is the operation of an Automatic Half Barrier level crossing in a particular location. There is scope for making improvements to the operation and use of this system. The aim of this risk assessment is therefore to determine whether changes are required, in order to reduce the risk presented by the particular Automatic Half Barrier to a level that is compliant with the principle of ALARP.

It should be noted that the Automatic Half Barrier concerned has, to date, been in operation for a period of 20 years. There is, therefore, some considerable operational experience of its use.

#### D.2.3 Hazard Identification

The operation of an Automatic Half Barrier level crossing is not a novel process. Hence the hazards associated with this undertaking were predominantly identified from a checklist.

The likely frequency and severity of each hazard has been estimated using the categorisation detailed in tables D-1 and D-2.

For each hazard, its estimated frequency and severity have been multiplied to obtain the hazard’s ‘rank’. Table D-3 presents the results of hazard identification and ranking.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>5 – Daily to monthly</th>
<th>4 – Monthly to yearly</th>
<th>3 – 1 to 10 yearly</th>
<th>2 – 10 to 100 yearly</th>
<th>1 – Less than 100 yearly</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Multiple</td>
<td>25</td>
<td>24</td>
<td>22</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td>fatalities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single fatalty</td>
<td>23</td>
<td>21</td>
<td>18</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Multiple major</td>
<td>20</td>
<td>17</td>
<td>13</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>injuries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major injury</td>
<td>16</td>
<td>12</td>
<td>8</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Minor injury</td>
<td>11</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table D-3 Example hazard ranking matrix (C)**
### Table D-1 Categorisation for estimated hazard frequency

<table>
<thead>
<tr>
<th>Frequency category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Less than 100 yearly</td>
</tr>
<tr>
<td>2</td>
<td>10 to 100 years</td>
</tr>
<tr>
<td>3</td>
<td>1 to 10 yearly</td>
</tr>
<tr>
<td>4</td>
<td>Monthly to yearly</td>
</tr>
<tr>
<td>5</td>
<td>Daily to monthly</td>
</tr>
</tbody>
</table>

### Table D-2 Categorisation for estimated hazard severity

<table>
<thead>
<tr>
<th>Severity category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minor injury</td>
</tr>
<tr>
<td>2</td>
<td>Major injury</td>
</tr>
<tr>
<td>3</td>
<td>Multiple major injuries</td>
</tr>
<tr>
<td>4</td>
<td>Single fatality</td>
</tr>
<tr>
<td>5</td>
<td>Multiple fatalities</td>
</tr>
<tr>
<td>Hazard Ref.</td>
<td>Hazard Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Works Crossing is Used When Not Authorised</td>
</tr>
<tr>
<td>2</td>
<td>Failure of Level Crossing to Protect Public From Train</td>
</tr>
<tr>
<td>3</td>
<td>Barrier Operates Without Being Caused By Train</td>
</tr>
<tr>
<td>4</td>
<td>Misuse of Level Crossing By Road User</td>
</tr>
<tr>
<td>5</td>
<td>Use of Crossing Exceeds Original Design Limits</td>
</tr>
<tr>
<td>6</td>
<td>Signal Passed at Danger (SPAD) at Signal Protecting Level Crossing</td>
</tr>
<tr>
<td>7</td>
<td>Poor Sighting of Level Crossing</td>
</tr>
</tbody>
</table>

Table D-3 Results of hazard identification
D.2.4 Causal Analysis

Causal Analysis has been conducted to estimate the annual frequency of occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard.

For the purposes of this illustrative example, only the results of Causal Analysis of Hazard 2 are presented – ‘Failure of Level Crossing to Protect Public from Train’. The simple fault tree constructed to evaluate the frequency of occurrence of the hazard is presented in Figure D-1.

The fault tree has been quantified on the basis of the following analysis:

- From examination of the timetable it has been determined that an average of four trains traverse the crossing per hour. Protection is required for the crossing of each train for a period of approximately 90 seconds. At any time, therefore, the probability of the event ‘Train at or near level crossing’ is as follows:

\[
\text{Probability} = \frac{90 \times 4}{3600} = 0.1
\]
• There is some considerable operational experience of use of the level crossing controller employed at this crossing, both within the UK mainline network and overseas. On the basis of the records of this experience, it has been determined that the frequency of the event ‘Controller indicates route clear when occupied’ is $5.0 \times 10^{-3}$ per annum per controller.

• Similarly, there is considerable experience of use of the particular type of track circuit employed in this undertaking to indicate the presence of an approaching train to the level crossing controller. Records maintained suggest that, for the rolling stock type used on the line concerned, the frequency of the event ‘Track circuit failure’ is $2.5 \times 10^{-3}$ per annum.

• An independent contractor has previously been employed to determine the likelihood of failure of communications to the level crossing controller. Analysis conducted by this contractor suggests that the frequency of the event ‘Communication System Failure’ is $1.5 \times 10^{-3}$ per annum.

• The event ‘Timing Sequence Failure’ covers the situation when there is a pedestrian or vehicle on the crossing when the barriers fall. Operational experience gained from use of the level crossing suggests that slow-moving pedestrians and traffic cause protection to be removed from this crossing twice per year on average. Hence the frequency of the event ‘Timing Sequence Failure’ is $2.0$ per annum.

Using the above values of each of the fault tree base events, the frequency of Hazard 2 has been determined as follows:

$$\text{Frequency} \approx \left(2.5 \times 10^{-3} + 1.5 \times 10^{-3} + 5.0 \times 10^{-3} + 2.0\right) \times 0.1 = 0.20$$

*Note that the frequency of the hazard is dominated by the frequency of the event ‘Timing Sequence Failure’.*

D.2.5 Consequence Analysis

Consequence Analysis has been conducted to determine those incidents, which may arise from occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard, in a similar manner to that for Causal Analysis.

For the purposes of this illustrative example, only the results of Consequence Analysis of Hazard 2 are presented – ‘Failure of Level Crossing to Protect Public from Train’. The particular method of consequence analysis used to analyse this hazard is the ‘Cause Consequence’ modelling technique. This is an inductive method of analysis where the hazard under consideration is displayed at the bottom of a decision-tree structure. Possible protective Barriers affecting event escalation are then identified, classified and assessed. The potential outcomes (consequences) as a result of success or failure of the Barriers are presented at the top of the page. The consequences can range from benign, essentially safe conditions to major or catastrophic accidents.

The simple cause-consequence models constructed to investigate the consequences of Hazard 2 are presented in Figure D-2. The consequences to pedestrians and other road users are modelled separately.
For the purposes of this analysis it has been estimated that, on average, 500 pedestrians use the crossing per day, taking 9 seconds each to traverse the crossing. Since trains run for 15 hours per day on this line, this leads to the following probability of a pedestrian being present at the crossing at any given time whilst trains are running:

\[
\text{Probability} = \frac{500 \times 9}{3600 \times 15} = 8.3 \times 10^{-2}
\]

Similarly, to estimate the probability of a road user being present at the crossing it has been estimated that, on average, 1000 vehicles use the crossing per day, taking 5 seconds to traverse the crossing.

It can be seen from the analysis that most occurrences of the hazard do not lead to an accident, due to mitigating factors such as the vigilance of pedestrians and other road users and other circumstantial factors, such as there being no traffic at the crossing when the hazard occurs.

*Note: the estimates of the probability with which a vehicle or pedestrian takes successful emergency action have to take account of the fact that, in most cases where the hazard occurs, it is as a result of a slow-moving vehicle or pedestrian in the first place.*
Figure D-2 Cause-consequence models for Hazard 2
D.2.6 Loss Analysis

Loss Analysis has been conducted to determine the magnitude of potential safety losses associated with each hazard.

For the purposes of this illustrative example, only the results of Loss Analysis of Hazard 2 are provided – ‘Failure of Level Crossing to Protect Public from Train’. Table D-4 presents details of the loss modelling conducted. The incidents (consequences) have been taken from the cause consequence diagram presented earlier. The following incidents were identified:

- Safe Condition;
- Near Miss;
- Train Hits Pedestrian;
- Road User Strikes Train;
- Road User Strikes Crossing.

It has been assumed that no losses arise from a Safe Condition. A Near Miss is judged not to result in safety losses, although it can result in significant train delays. The remaining consequences all result in both safety and commercial losses.

Following analysis of accident statistics, for circumstances similar to the level crossing under study, it has been assumed that:

- the incident ‘Train Hits Pedestrian’ results in no injuries to passengers, but 1 fatality to a member of the public;
- the incident ‘Road User Strikes Train’ results in 2 minor injuries to passengers and a single major injury to a member of the public;
- the incident ‘Road User Strikes Crossing’ results in 1 minor injury to passengers and 1 major injury to a member of the public.

The injuries associated with each incident have been converted to a corresponding Potential Equivalent Fatality (PEF) figure using the following convention:

- 1 fatality = 10 major injuries;
- 1 major injury = 20 minor injuries.
### Table D-4 Results of Loss Analysis for hazard 2

<table>
<thead>
<tr>
<th>Incident</th>
<th>Frequency (per annum)</th>
<th>Safety loss per incident (PEF)</th>
<th>Safety loss per annum (PEF)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Passenger</td>
<td>Public</td>
</tr>
<tr>
<td>Train Hits Pedestrian</td>
<td>$8.4 \times 10^{-4}$</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Near Miss (1)</td>
<td>$8.4 \times 10^{-4}$</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Near Miss (2)</td>
<td>$1.5 \times 10^{-3}$</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Road User Strikes Train</td>
<td>$1.1 \times 10^{-4}$</td>
<td>$10^{-2}$</td>
<td>0.1</td>
</tr>
<tr>
<td>Road User Strikes Crossing</td>
<td>$2.6 \times 10^{-4}$</td>
<td>$5 \times 10^{-3}$</td>
<td>0.1</td>
</tr>
<tr>
<td>Total per annum</td>
<td></td>
<td>$2.4 \times 10^{-6}$</td>
<td>$8.8 \times 10^{-4}$</td>
</tr>
</tbody>
</table>

It should be noted that, in order to demonstrate compliance with the ALARP criteria, in a subsequent stage of risk assessment, safety losses have been determined individually for the following groups exposed to the risk of railway operations: passengers and the public. The hazard has not been determined to lead to any losses to employees (trackside workers).

The annual frequency of each incident has been determined by multiplying the estimated frequency of the hazard (derived during Causal Analysis) by the estimated probability of the hazard leading to the incident, once the hazard has occurred (derived during Consequence Analysis).

Commercial losses have been estimated by means of expert judgement and from knowledge of previous incidents.

### D.2.7 Options Analysis

Both structured brainstorming and a suitable checklist have been used to identify potential risk mitigation options for each hazard. The checklist that has been used records known mitigation measures employed elsewhere throughout the UK mainline network. Use of brainstorming and the checklist together provide a high degree of confidence that all significant options for risk mitigation have been identified.

Table D-5 summarises those risk mitigation options that have been identified.
Option costs have been derived from knowledge of previous application of protective measures at similar level crossings and, for measures such as provision of Automatic Train Protection, through use of expert judgement.

**D.2.8 Impact Analysis**

Each of the potential risk mitigation options identified in the previous stage of risk assessment have been analysed further to determine their effects upon the losses associated with operation and use of the level crossing.

Estimates of the reductions in losses achieved through use of each option have been calculated by modifying the Causal or Consequence models associated with the option (developed in the previous stages of risk assessment).

<table>
<thead>
<tr>
<th>Hazard Ref.</th>
<th>Hazard Description</th>
<th>Hazard Rank</th>
<th>Option</th>
<th>Option Cost (£ pa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Failure of Level Crossing to Protect the Public From Passing Trains (Wrong-side Failure of Level Crossing)</td>
<td>8</td>
<td>1. Modify crossing to have more reliable controller</td>
<td>750</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Modify crossing sequence to provide greater crossing time</td>
<td>750</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Rewire cables to controller to replace degraded cabling</td>
<td>1000</td>
</tr>
<tr>
<td>3</td>
<td>Barrier Operates Without Being Caused By Train</td>
<td>12</td>
<td>4. Provide Closed Circuit Television to protect crossing from vandalism/abuse</td>
<td>2500</td>
</tr>
<tr>
<td>4</td>
<td>Misuse of Level Crossing By Road User</td>
<td>8</td>
<td>5. Provide warning signs at approach to level crossing</td>
<td>300</td>
</tr>
<tr>
<td>6</td>
<td>SPAD at Signal Protecting Level Crossing</td>
<td>4</td>
<td>6. Provide Automatic Train Protection</td>
<td>20000</td>
</tr>
<tr>
<td>7</td>
<td>Poor Sighting of Level Crossing</td>
<td>20</td>
<td>7. Provide warning signs to indicate to road user the state of route ahead</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8. Re-routing of approaching road</td>
<td>50000</td>
</tr>
</tbody>
</table>

**Table D-5 Results of Options Analysis**

For the purposes of this illustrative example, only the results of the analysis of one of the options are presented – modify crossing sequence to provide greater crossing time. To further analyse this option it has been estimated that by increasing the crossing time, the probability of the event ‘Timing Sequence Failure’ can be reduced by an order of magnitude.
Applying this revised failure probability within the previous causal analysis of the hazard leads to a reduced annual probability of occurrence of the hazard of $2.1 \times 10^{-2}$. The loss analysis conducted previously has therefore been revised and the results of this revised analysis are presented in Table D-6.

<table>
<thead>
<tr>
<th>Incident</th>
<th>Frequency (per annum)</th>
<th>Safety loss per incident (PEF)</th>
<th>Safety loss per annum (PEF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train Hits Pedestrian</td>
<td>$8.8 \times 10^{-5}$</td>
<td>-</td>
<td>$8.8 \times 10^{-5}$</td>
</tr>
<tr>
<td>Near Miss (1)</td>
<td>$8.8 \times 10^{-5}$</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Near Miss (2)</td>
<td>$1.6 \times 10^{-4}$</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Road User Strikes Train</td>
<td>$1.2 \times 10^{-5}$</td>
<td>$10^{-2}$</td>
<td>$1.2 \times 10^{-7}$</td>
</tr>
<tr>
<td>Road User Strikes Crossing</td>
<td>$2.7 \times 10^{-5}$</td>
<td>$5 \times 10^{-3}$</td>
<td>$1.4 \times 10^{-7}$</td>
</tr>
</tbody>
</table>

Table D-6 Revised Loss Analysis assuming modified crossing sequence time

D.2.9 Demonstration of Acceptability

We consider three Groups exposed to the risks of their operations: employees (trackside staff), passengers and the public.

Table D-7 details the ALARP criteria used in this example, which are consistent with guidance in [F.17]. Each of the values represents an average risk of fatality per annum for an individual in the respective Group.

<table>
<thead>
<tr>
<th>Group</th>
<th>Upper Limit of Tolerability</th>
<th>Broadly Acceptable Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>$10^{-3}$</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>Passenger</td>
<td>$10^{-4}$</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>Public</td>
<td>$10^{-4}$</td>
<td>$10^{-6}$</td>
</tr>
</tbody>
</table>

Table D-7 ALARP criteria

Previous investigations and analysis suggest that Automatic Half Barrier level crossings contribute 10%, 20% and 50% of the total risk of all operations, to Employees, Passengers and the Public respectively.
There are known to be 300 such crossings in the network. Whilst some crossings are known to pose slightly increased risk compared to others, analysis suggests that the majority of crossings are associated with similar risk levels.

Hence, it can be assumed that the fraction of the total safety risk which is associated with a single Automatic Half Barrier level crossing is as follows:

\[
\text{Fraction of total safety risk to Employees associated with a single crossing} = \frac{1 \times 0.1}{300} = 3.3 \times 10^{-4}
\]

\[
\text{Fraction of total safety risk to Passengers associated with a single crossing} = \frac{1 \times 0.2}{300} = 6.7 \times 10^{-4}
\]

\[
\text{Fraction of total safety risk to Public associated with a single crossing} = \frac{1 \times 0.5}{300} = 1.7 \times 10^{-3}
\]

The apportioned ALARP criteria which the level crossing under consideration should meet can therefore be determined by multiplying the criteria given in Table D-7 by the above fractions. The resulting apportioned criteria are given in Table D-8.

<table>
<thead>
<tr>
<th>Group</th>
<th>Apportioned Upper Limit of Tolerability</th>
<th>Apportioned Broadly Acceptable Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>$3.3 \times 10^{-7}$</td>
<td>$3.3 \times 10^{-10}$</td>
</tr>
<tr>
<td>Passenger</td>
<td>$6.7 \times 10^{-8}$</td>
<td>$6.7 \times 10^{-10}$</td>
</tr>
<tr>
<td>Public</td>
<td>$1.7 \times 10^{-7}$</td>
<td>$1.7 \times 10^{-9}$</td>
</tr>
</tbody>
</table>

**Figure D-8 Apportioned ALARP criteria for the undertaking concerned**

In order to determine the total safety losses associated with the undertaking, the estimated safety losses associated with each of the hazards, prior to application of mitigation measures, have been summed together. The results of this summation are presented in table D-9 (note that only the estimated safety losses associated with Hazard 2 have previously been presented as part of this illustrative example).

<table>
<thead>
<tr>
<th>Group</th>
<th>Total Safety Losses Associated with the Undertaking per annum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>0</td>
</tr>
<tr>
<td>Passenger</td>
<td>$5.2 \times 10^{-7}$</td>
</tr>
<tr>
<td>Public</td>
<td>$8.0 \times 10^{-4}$</td>
</tr>
</tbody>
</table>

**Figure D-9 Total safety losses associated with undertaking per annum**

It is estimated that, on average, 10000 different individuals are regular daily users of the crossing. The average risk to each of these individuals, associated with the undertaking, is therefore as presented in Table D-10. It should be noted that significantly more than 10000 different individuals use the crossing per year. However, outside of the 10000 regular daily users, other individuals use the crossing very infrequently and are not therefore considered in this risk apportionment.
Table D-10 Average safety losses per individual associated with the undertaking per annum

Comparison of the average Individual Risk with the apportioned ALARP and Benchmark criteria suggests that the risks to employees and passengers fall below the Apportioned Broadly Acceptable Bound. However, the average risk to a member of the public falls within the Tolerability Region (above the Apportioned Broadly Acceptable Bound and below the Apportioned Upper Limit of Tolerability). It is therefore necessary to determine those risk mitigation measures which should be applied, in order to reduce risks to ALARP levels.

For the purposes of this exercise we use a VPF of £1.5M.

Table D-11 presents a summary of each of the risk mitigation options and the annual reductions in safety losses to which they may lead. Note that only the reductions in safety losses associated with modified crossing sequence time have previously been presented as part of this illustrative example. The table employs the VPF value detailed above. Net costs are derived by subtracting any mitigated commercial losses from the direct costs.

<table>
<thead>
<tr>
<th>Risk mitigation option</th>
<th>Direct costs per annum (£)</th>
<th>Net costs per annum (£)</th>
<th>Annual mitigated safety loss (PEF)</th>
<th>Annual monetary value of mitigated loss (£)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>750</td>
<td>710</td>
<td>3.9×10⁻⁵</td>
<td>59</td>
</tr>
<tr>
<td>2</td>
<td>750</td>
<td>690</td>
<td>7.9×10⁻⁴</td>
<td>1200</td>
</tr>
<tr>
<td>3</td>
<td>1000</td>
<td>950</td>
<td>9.1×10⁻⁵</td>
<td>136</td>
</tr>
<tr>
<td>4</td>
<td>2500</td>
<td>2400</td>
<td>6.3×10⁻⁵</td>
<td>94</td>
</tr>
<tr>
<td>5</td>
<td>300</td>
<td>290</td>
<td>2.3×10⁻⁵</td>
<td>34</td>
</tr>
<tr>
<td>6</td>
<td>20000</td>
<td>20000</td>
<td>7.1×10⁻⁵</td>
<td>106</td>
</tr>
<tr>
<td>7</td>
<td>200</td>
<td>1900</td>
<td>5.6×10⁻⁵</td>
<td>84</td>
</tr>
<tr>
<td>8</td>
<td>50000</td>
<td>49000</td>
<td>6.3×10⁻⁵</td>
<td>94</td>
</tr>
</tbody>
</table>

Table D-11 Cost-benefit analysis of potential risk mitigation options

It can be seen that only option 2 is reasonably practicable to implement. Hence, the risks associated with the undertaking are reduced to ALARP levels through implementation of option 2 only and without any further mitigation measures.
The residual risk of the undertaking after implementation of option 2 is as follows:

\[
\text{Residual risk} = 8.0 \times 10^{-4} - 7.9 \times 10^{-4} = 1.0 \times 10^{-5} \text{ per annum}
\]

The average residual risk to the 10000 regular daily users of the crossing is therefore \(1.0 \times 10^{-9}\) per annum. This is less than the apportioned benchmark.

D.3 Safety Assessment Remit

The following generic wording was used and recommended by the Railtrack System Review Panels as a starting point for writing remits for Safety Assessments:

*The assessment shall:*

- State the safety targets which have been used in carrying out the assessment.
- Give a professional recommendation on the suitability and acceptability of the document with regard to its stated purpose.
- The critical and most sensitive arguments of the documents should be clearly and concisely highlighted and a professional opinion shall be given as to the robustness of the argument. Where the argument is contained in whole or part within other documents or is part of existing custom and practice this should be clearly identified.
- A professional opinion should also be given, with regard to the railway system as a whole, as to the practicality of any measures used to mitigate against the hazards raised.
- Identify any non-compliances to Railway Group or Railtrack Line Standards and legal requirements.
- Supply related technical advice as required by the Client, or as perceived necessary by the adviser.

All assessor observations are to be uniquely numbered and classified into one of the following three Classes, categories 1 to 3 should be used where operational use is being sought and categories A to C where other documents are under review (additional subclasses are permitted to aid clarity):

**Documents seeking Operational Authority**

- **Category 1** Issue is sufficiently important to require (substantial) resolution, prior to recommending that the train/equipment may become operational. (Alternatively, a specific control measure may be implemented to control the risk in the short-term.)

- **Category 2** Issue is sufficiently important to require resolution within 3-6 months, but the train/equipment may become operational in the interim (possibly with a protective control measure).

- **Category 3** Issue is highlighted for incorporation into the Safety Case at the next periodic review, but no action is required separately.
Other Documents

Category A Concerns errors, omissions or questions that have a direct bearing on the acceptability of the document, which it is necessary to resolve prior to the consideration of downstream or offspring documents.

Category B Requires satisfactory resolution prior to acceptance of a complete safety submission, or within a defined time period (not normally to exceed 6 months).

Category C Minor errors, for example, syntax, spelling, minor technical matters which have no direct significant safety implications. For clarity, these require to be recorded and corrected if the document is re-issued, but are not in themselves sufficiently significant to warrant re-issue on their own.

For either the numerical or alphabetical categories, where there are a large number of lower category issues, the reviewer is to consider whether in totality they represent sufficient residual risk that they in effect equate to one or more higher category issues (for example, that they would warrant the imposition of any additional mitigating control measures). In these circumstances, it should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document which has been reviewed.
D.4 Safety Audit checklist

D.4.1 Pro forma

This section presents a pro forma for each question in the audit checklist. Each question should be entered and given a unique reference. Following the audit the answer should be ringed, evidence to support the answer entered and the impact of the answer indicated. Conformance should be indicated by ringing OK; or category 1, 2 or 3 (see Chapter 13). Any further comments should also be noted.

<table>
<thead>
<tr>
<th>Question: &lt;Enter question&gt;</th>
<th>Ref: &lt;Enter unique reference&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence: &lt;Enter supporting evidence&gt;</th>
<th>Yes No n/a</th>
<th>&lt;Ring answer&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comments: &lt;Enter any other comments, if any&gt;</th>
<th>OK 1 2 3</th>
<th>&lt;Ring impact&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

D.4.2 Example audit checklist

This section contains typical questions that might be asked during a Safety Audit. It is intended to be an example and is neither exhaustive nor mandatory.

Where a question asks if something is adequate, judgement from the Safety Auditor is required, taking into account explanations provided by the Project Manager. In general something is adequate if:

- it meets specified requirements;
- it is effective and economical;
- it is appropriate to the circumstances; and
- it represents good practice.
D.4.2.1 Safety planning
a) Is there an adequate Safety Plan (see Chapter 11)?
b) Are the responsibilities for safety and the competencies of staff clearly defined?
c) Is the Safety Plan clear, easily obtained and accessible to the project?
d) Have appropriate safety requirements been defined for each deliverable?
e) Have suitable controls been devised to verify the safety requirements?
f) Has an appropriate approach to safety been chosen?

D.4.2.2 Safety documentation
a) Has the safety documentation required for the project been identified?
b) Has the identified documentation been produced?
c) Is the plan for safety documentation adequate?
d) Have the responsibilities for producing safety documentation been identified?
e) Has the documentation been produced by the staff identified for the task?
f) Has an appropriate standard for documentation been specified?
g) Has the standard been consistently applied?

D.4.2.3 Sub-contract management
a) Has an adequate method of evaluating sub-contractor capability been identified?
b) Has this method been rigorously applied to all sub-contractors?
c) Has each sub-contractor been set safety targets or requirements?
d) Has each sub-contractor produced a Safety Plan?
e) Have these plans been reviewed and approved as defined in the project Safety Plan?
f) Is there any evidence of sub-contractor non-compliance?
g) Have all sub-contractor-identified hazards been entered in the Hazard Log?

D.4.2.4 Testing
a) Has testing called for in the Safety Plan been carried out?
b) Is the test team independent of the development team?
c) Have incidents arising from testing activities been entered in the Hazard Log?
d) Does the testing programme adequately demonstrate the safety of the system?
D.5 Safety Assessment checklist

Where a checklist question relates to a document or a task, the current section providing guidance for that document or task should be consulted. These have not been identified in the checklists to avoid extensive updating when changes are introduced.

Questions marked with an asterisk may require comments to be recorded separately and referenced accordingly.

D.5.1 Commissioning an assessment

Checklist for person writing requirements:

a) Safety Assessor has sufficient independence (see Chapter 13);
b) Safety Assessor has sufficient qualifications and experience (see Chapter 13);
c) Requirements have been discussed with Project Manager;
d) Remit has been signed by originator;
e) Remit has been signed by Safety Assessor;
f) Remit has been copied to Safety Assessor and Project Manager.

D.5.2 The assessment process

Checklist for Safety Assessor:

a) For the system to be assessed, has the following documentation been checked:
   - Safety Plan?
   - Hazard Log?
   - Safety Requirements Specification?
   - Specification?
   - Drawings?
b) Have safety requirements been identified in the documentation listed above?
c) Having read the above documentation do you have any questions or points of doubt over the requirements? *
d) Has the system been identified functionally by means of block diagrams?
e) Do the block diagrams cover levels of the systems from the highest down to line replaceable units?
f) Do the block diagrams adequately represent the system, as specified?
g) Is there design documentation showing reasons for decisions made in the system design process? 
h) Do you have any comments or recommendations regarding the design disclosure document? *
i) Has a hazard list been compiled?
j) Have hazards been removed/mitigated, where appropriate?  
k) Do you have any comments or recommendations concerning the hazard list?  
l) Has a list of potential accidents been compiled?  
m) Do you have any comments or recommendations on the list of potential accidents?  
n) Have any novel or unproved features in the design been noted, so that particular attention can be given to resolving any safety problems?  
o) Do you have any comments or recommendations regarding the novel or unproved features?  
p) Has any information been compiled on the safety of similar systems?  
q) Do you have any comments or recommendations on the information provided on similar systems?  
r) Have accident sequences been analysed for each type of potential accident?  
s) Do you have any comments on the accident sequence analyses?  
t) Have risk assessments been made?  
u) Has the risk been controlled to an acceptable level?  
w) Have tolerable risk levels been agreed?  
x) Have accident rate targets been set?  
y) Have hazard rate targets been set?  
z) Are Safety Integrity Levels applicable to elements of the design and, if so, have they been defined?  
  aa) Has the design been assessed against the targets for the random elements of the design?  
  ab) Has the design been audited against the design rules implied by the Safety Integrity Level?  

D.5.3 Assessment checklist: Requirements definition  
Checklist for Safety Assessor:  
a) For the system to be assessed, have the following documents been checked:  
  • Feasibility Studies Reports?  
  • Statement of Requirements?  
  • Drawings?  
b) Have safety targets or requirements been given in the following documents:  
  • Feasibility Studies Reports?
• Statement of Requirements?

c) Having read the above documents, do you have any questions or areas of doubt in the requirements?

d) Has a Safety Plan been prepared?

e) Do you have any comments or recommendations concerning the Safety Plan?

f) Has a Hazard Log been started?

g) Do you have any comments or recommendations regarding the Hazard Log?

h) Has the system been identified, in schematic or functional drawings?

i) Has Failure Mode and Effect Analysis been done?

j) Do you have any comments or recommendations concerning the Failure Mode and Effect Analysis?

k) Have accident sequences been considered?

l) Do you have any comments on potential accident sequences, hazards, initiating events or contributory incidents?

m) Have the severities or consequences of potential accidents been determined or classified?

n) Do you have any comments on accident severity or consequence classification?

o) Has the design been altered during project definition to reduce hazards?

p) Do you have any comments or recommendations concerning hazard reduction?

q) Have the probabilities or frequencies of initiating events been determined?

r) Do you have any comments or recommendations on the likelihood of initiating events or hazards?

s) Have the Risk Assessment criteria for determining tolerability been drawn up?

t) Does target apportionment take into account the expected number of units in service?

u) Do you have any comments on the determination of the tolerability of risk?

v) Have risks been determined for all aspects of the design?

w) Are there aspects of the design which you would recommend for further risk assessment?

x) Does the specification for design and development contain safety targets and requirements?
y) Do you have any comments on the specified targets or requirements?

z) Have safety targets been allocated to the lower level functions?

aa) Do you have any comments or recommendations on the allocation of safety targets?

D.5.4 **Assessment checklist: Design, build and test**

Checklist for Safety Assessor for use during system design, implementation, and testing:

a) Has a Safety Plan been formally issued?

b) Do you have any comments or recommendations concerning the Safety Plan?

c) Has a Hazard Log been started and maintained?

d) Do you have any comments or recommendations on the contents of the Hazard Log?

e) Is the system design well-defined?

f) Have the safety-related parts of the system been made as simple as possible?

g) Have safety-related sub-systems been identified?

h) Has there been any development of the design to remove undesirable features or improve performance characteristics?

i) Are there any potential accidents associated with the design?

j) Have the potential accident sequences been adequately examined?

k) Have Design Reviews been carried out?

l) Do you have any comments or recommendations on the Hazard Identification and Analysis work?

m) Has Risk Assessment been carried out?

n) Does this table take into account the expected number of units in service?

o) Do you have any comments or recommendations concerning the assessment of risks?

p) Have tolerable levels of risk been established?

q) Is the tolerability of risk consistent with the relevant industry standards?

r) Have targets for numerical accident probability or rate been agreed for each type of potential accident?

s) Have targets for numerical accident probability or rate been agreed for elements of the accident sequence?

t) Have targets (quantitative or qualitative) been allocated down to sub-system functional level?
u) Have quantitative hazard rate targets been apportioned separately to the random and Systematic Failure modes?

v) Has the potential effects of common cause failures been assessed?

w) Have random hazard rate targets been apportioned to the lower level functions of the system?

x) Are Safety Integrity Levels applicable to elements of the design and, if so, have they been defined?

y) Have Safety Integrity Levels been apportioned to lower level functions according to agreed rules (see Chapter 17)?

z) Have the targets and criteria developed from the above been adequately recorded and reported in the Hazard Log?

aa) In carrying out the Safety Assessment, it is necessary to compare the random targets with those predicted for the random elements. Is the comparison satisfactory?

ab) For the Safety Assessment of the systematic elements, it is necessary to audit the design against the tolerable levels of risk, the agreed rules for Safety Integrity Levels and the design techniques. Is the design acceptable?

D.5.5 Assessment checklist: Customer acceptance and validation

Checklist for Safety Assessor:

a) Does the Safety Plan contain an element relating to a test and acceptance programme?

b) Are the safety features of the design identified for acceptance tests?

c) Do you have any comments or recommendations concerning the adequacy of the test programme?

d) Have the results of the safety test and acceptance programme been recorded and reported in the Hazard Log?

e) Are the results satisfactory?

f) Are there any shortcomings or outstanding items?

g) Is the level of test coverage adequate?

D.5.6 Assessment checklist: Site trial/pilot scheme

Checklist for Safety Assessor:

a) Does the Safety Plan contain requirements for the conduct of Site Trial?

b) Does the Safety Plan contain requirements for the conduct of a Pilot Scheme?

c) Are the safety features of the system design identified for Site Trial purposes?
d) Are the safety features of the system design identified for Pilot Scheme purposes?

e) Do you have any comments regarding the adequacy of the Site Trial to demonstrate the safety features?

f) Do you have any comments regarding the adequacy of the Pilot Scheme to demonstrate the safety features?

g) Has an incident or defect reporting system been set up for the Site Trial?

h) Is the trial covered by a Safety Certificate?

i) Is the system being used with the constraints of the Safety Certificate?

j) Are all necessary support arrangements in place?

D.5.7 Assessment checklist: In-service support

Checklist for Safety Assessor:

a) Has support of the system in service been addressed during Requirements Definition?

b) Has support of the system in service been addressed during Design and Development?
This page has been left blank intentionally
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)

FMEA should be carried out in compliance with established standards such as BS 5760 [F.35].

*Note that users of this standard should ensure that they use a common set of units, if they wish their risk ratings to be comparable.*

The analyst should consider components at a detailed level of indenture and record their failure modes along with causes and effects. The failure effects of these sub-components then become failure modes of components at the next higher level of indenture. The process is repeated up the functional hierarchy to yield the individual failure modes of the whole system.

The depth of the analysis should be adjusted according to the preliminary appraisal of the hazards. The components which contribute to more severe hazards should be analysed in greater detail.

Checklists, HAZOP or other techniques may be used to identify basic failure modes.

The analysis is recorded on a worksheet which has at least the following columns:

<table>
<thead>
<tr>
<th>Item Ref</th>
<th>The unique identifier of the sub-component being considered.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of this sub-component.</td>
</tr>
<tr>
<td>Failure Ref</td>
<td>A unique identifier for the failure mode entered.</td>
</tr>
<tr>
<td>Mode</td>
<td>A description of the failure mode.</td>
</tr>
<tr>
<td>Causes</td>
<td>For this failure.</td>
</tr>
<tr>
<td>Effect</td>
<td>Of this failure (local and system-wide).</td>
</tr>
<tr>
<td>Compensating Provisions</td>
<td>Which may cause the effects of this failure not to be promulgated.</td>
</tr>
<tr>
<td>How detected</td>
<td>The means by which the failure may be detected.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Any other notes made by the analyst.</td>
</tr>
</tbody>
</table>

This conforms to the British Standard for FMECA [F.35], except that there is no column for ‘Severity of effects’. Criticality is considered instead during the later stages of Risk Assessment, although note that FMECA may be more appropriate for some applications.

E.2 Hazard and Operability Studies (HAZOP)

Where detailed design information is available and a high-level of assurance is required a Hazard and Operability Study or HAZOP can be carried out.

HAZOP is a systematic, creative examination of a design by a multi-disciplinary team. HAZOP is recommended for systems with potential catastrophic accidents, novel features or for systems that span several engineering disciplines.
HAZOP is an analysis technique developed originally for the chemical industry and described in the Reference Guide [F.36], Hazop and Hazan [F.37] and CAP 760 [F.38]. The technique should be carried out as described in these documents.

The principal difference between the application of HAZOP in the chemical industry and the application in other engineering fields is in the way in which the design documentation is examined. In the chemical industry, examination is guided by traversing the flowchart, a schematic showing the connection of vessels, pipes and valves. In engineering applications an alternative representation of the parts and their interactions, such as a mechanical drawing, circuit schematic or data flow diagram should be used. The same technique can be applied at a number of levels within the design.

If no convenient form of the design exists, then the analyst should construct a Functional Block Diagram. At each level of indenture, this shows the components of the system or a sub-system, as blocks, with lines drawn between each pair of boxes that directly interact.

The team collects the design documentation, including a full functional breakdown of the system. Each component, including the interfaces, of the system is inspected in turn. The team considers the intention of the system and by applying a list of guide words attempts to reveal plausible deviations from the design intention.

The guide words for hardware systems typically are as follows. Alternative guide words are provided in [F.38]:

a) NO or NOT No part of the intention is achieved but nothing else happens
b) MORE Some quantitative increase over what was intended
c) LESS Some quantitative decrease over what was intended
d) AS WELL AS Some qualitative increase over what was intended
e) PART OF Some qualitative decrease over what was intended
f) REVERSE The logical opposite of the intention happens
g) OTHER THAN Something quite different happens

The team should be constituted to cover the areas of expertise required to fully understand the system. For example, the examination of a signalling system may require a safety process expert, a hardware engineer, a software engineer, an expert in signalling principles and potential users and maintainers.

It is quite likely that the team will be unable to establish immediately whether a possible deviation can occur or what its effect can be. In that case an action can be recorded to establish this outside the meeting.

### E.3 Fault Tree Analysis

Fault Tree Analysis (FTA) is a widely known and accepted top-down or deductive system failure analysis technique. The Fault Tree Handbook, NUREG-0492 [F.39], is a comprehensive reference document for FTA, and may be used in conjunction with other FTA standards.

FTA begins with a single undesired top event and provides a method for determining all the possible causes of that event.
A correctly constructed fault tree is a graphical and logical model of the various parallel and sequential combinations of events that will result in the occurrence of the top event.

FTA can be used for both qualitative as well as quantitative analysis. The graphical nature of the technique aids the qualitative identification of potential sources of single-point failures and safety-critical failure combinations.

The precise definition of the top event is critical to the success of the analysis, since an incorrect top event will, in most cases, invalidate the whole analysis.

The system is analysed, from the identified top events, in the context of its environment, and modes of operation, to find all credible causal events.

The fault tree is made up of gates, which serve to permit or inhibit the flow of fault logic up the tree. The gates show the relationship of lower events – the inputs to the gate – needed for the occurrence of a higher event – the output of the gate. The gate symbol denotes the relationship of the input events required for the output event.

The fault tree is used to produce the minimal cut sets - the minimum combination of independent base events which, if they occur or exist at the same time, will cause the top event to occur. The minimal cut sets provide the basis for both the qualitative and quantitative analysis of the system.

Fault trees are relatively simple in concept, but can be very difficult in practice. This is particularly true when quantitative analysis is required. Chapter V of NUREG-0492 [F.39] provides a detailed explanation of the technique. The following key concepts and rules from that document are given here to guide the analyst in the approach required to the construction of the tree.

In determining the causes of an event in a fault tree, the analyst should identify the immediate, necessary and sufficient causes for the occurrence of that event. The temptation to jump directly to the basic causes should be resisted, even if these may appear obvious.

The dependence between base events within a minimal cut set should be identified during FTA. This is achieved by performing Common Cause Failure Analysis on the Minimal Cut Sets to identify potential dependencies.

The following basic rules should be applied when constructing a fault tree:

a) Write the statements that are entered into the event boxes as faults: state precisely what the fault is and when it occurs.

b) If the answer to the question ‘Can this fault consist of a component failure?’ is ‘Yes’, classify the event as a ‘State of Component Fault’. If the answer is ‘No’, classify the event as a ‘State of System Fault’. If an event is classified as a ‘State of Component Fault’, add an OR-gate below the event and look for primary, secondary and command faults that may cause the event. If an event is classified as a ‘State of System Fault’, an AND-gate, OR-gate, INHIBIT-gate, or possibly no gate at all may be required, and the minimum, necessary and sufficient causes should be determined.

c) If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.

d) All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken.
e) Gate inputs are to be properly defined fault events. Gates are not to be connected directly to other gates.

f) Identify fixed probabilities, that is, non-failure conditions, with inhibit gates.

E.4 Cause Consequence Diagramming

Cause Consequence Diagramming (or Cause Consequence Analysis) is a technique that embodies both causal and consequence analysis. However, in the context of the Yellow Book it is useful primarily as a consequence analysis tool.

The technique provides a diagrammatic notation for expressing the potential consequences of an event (normally a hazard) and the factors that influence the outcome.

The basic notation is introduced in the context of the example in Figure E-1. In this diagram the hazard is Ignition. The final outcomes (or ‘significant consequences’) are shown in octagons and vary from no incident to a major fire. The major factors that influence the outcomes are shown in ‘condition vertices’.

The diagram shows that a major fire will only occur as a result of the ignition hazard if both the sprinkler and alarm system fail. If we can estimate the frequency with which the hazard will occur and the probability that the sprinkler and alarm systems will fail on demand (and, importantly, we know to what degree these failures are correlated) then we can estimate the frequency with which the hazard will give rise to this accident. This is an essential step on the way to estimating the risk arising from the hazard.

There are variations in notation. The tool used to draw the examples in appendix D produces output in a slightly different format.

The notation allows further symbols. For a slightly fuller exposition refer to ‘Safeware: System Safety and Computers’ [F.40], pages 332-335.
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).

Figure E-2  The DRACAS process
E.6 Goal Structuring Notation

E.6.1 Introduction

Objective evidence to support a safety argument has typically been presented in documents called Safety Cases but other titles are used. Whatever the name of the document, in some instances the document size, as well as the time, resources and cost of developing such safety arguments has become excessive. This is a concern as it could potentially:

- present a barrier to implementing small or low-cost schemes;
- lead to an incorrect belief that Engineering Safety Management is only undertaken in order to gain regulatory approvals and adds little real value; and
- make it difficult for the Safety Approver to review all of this evidence in a short amount of time.

For the rail industry to continually improve its safety record it must be able to implement large schemes efficiently and small changes cost-effectively. To meet this aim, we recommend that the level of Safety Engineering and analysis undertaken (and thus the size of the safety argument) should be commensurate with the level of risk and complexity of the change proposed. Judgement is therefore required as to the level of risk associated with the project and thus the degree of evidence and application necessary to assess and mitigate the risk. If the volume of evidence is becoming unwieldy, the aim of the argument may be unclear and it may not serve its purpose.

One tool that facilitates the development of well-defined and structured safety arguments is Goal Structuring Notation (GSN).

This section provides authors and reviewers of safety arguments with an introduction to how GSN can be used efficiently and effectively. It aims to provide clear guidance on why GSN can improve the development of safety arguments, as well as when and how it should be applied. Railway application case studies and references to further more detailed GSN guidance are provided.

This section is not enough on its own to teach you how to use GSN well.

It should also be noted however that this section does not give guidance on how to develop the safety argument itself – it only provides guidance on how GSN can be used to pictorially represent the safety argument structure. Guidance on how a safety argument should be developed is provided in Chapter 18.

E.6.2 What is GSN?

GSN is a graphical notation that presents the logical structure of a safety argument. It helps people writing and reviewing safety arguments to focus their time on the evidence which is critical to the argument. For particular applications (see guidance provided in Section 3) GSN can improve the efficiency of Safety Case development and review without compromising safety.
GSN was developed by the University of York, most recently under the guidance of Dr. Tim Kelly. It has been adopted in other industries within which the development and operation of safe systems is a priority. These include both the military and aerospace sectors [F.41].

As the name implies, Goal Structuring Notation requires the clear definition of the safety goal (objective), for instance, that a new train or signalling product is acceptably safe to be operated in service. The building blocks [F.42] of the safety argument are then developed from the top-down as a network of related elements, commonly referred to as a Goal Structure. The symbols used to describe the different facets of the argument are described below.

It is noted that the goal structure itself does not provide a time-based sequence of tasks which need to be undertaken, but should concisely and clearly present what evidence is needed to provide a safety justification.

To illustrate the notation, Figure E-4 shows a small part of a simple safety argument which is based on the application of the Yellow Book fundamentals (note this is for illustrative purposes only).
Goal (represents the claims and sub-claims of the safety argument)

Strategy (the approach used to logically progress from goals to sub-goals)

Solution (the evidence on which the safety argument is based)

Assumption (the assumptions on which the argument are based must be stated)

Justification (clarifies the reasoning behind the approach used)

Context (defines the circumstances in which the claims are valid)

Goal to be developed (requires further development work)

Models (reference detailed accounts of the systems and processes referred to in the argument)

Solved By links (demonstrate which goals, strategies or solutions are being used to support a claim)

In Context Of links (indicate the elements that are providing contextual information for a given claim or strategy)

Requires Instantiation (acts as a place holder if evidence is not yet available)

Figure E-3 Basic GSN Symbols
E.6.3 When to Use GSN

As we say above, the level of ESM work undertaken should be commensurate with the level of risk and the complexity of the project. Judgement is therefore required as to the level of risk associated with the project and thus the level of evidence and application necessary. One of the aims of GSN is to improve the efficiency of Safety Case development (by enabling effort to be focussed where critical, and avoiding the development of detailed evidence where it does not directly support the safety argument). In order to realise the benefits which GSN can bring, it is important for you to understand when its application is appropriate. The guidance below and in the next section will assist you to make this judgement.

Ideally, the goal structure should be developed as early as possible in the project. Developing an initial goal structure during planning will help you to understand what you need to do to control risk and to collect evidence that it has been controlled.

GSN can be applied to railway Engineering Safety Management by a range of users, including the developers of safety arguments and independent reviewers. GSN is particularly suited to the development of safety arguments which are:

- Complex (for instance, many stakeholders/interfaces or the system itself is complex);
- Novel (not standard practice) or not well understood; or
- Involve hazards classified as high risk.
The Yellow Book follows the CENELEC standards in separating application-specific Safety Cases from generic Safety Cases. GSN can be used for both:

- For generic level Safety Cases, the complex interfaces can be clearly documented in the goal structure. As GSN is easily read by non-ESM practitioners, communication is enhanced across stakeholders. Case Study 1 below (E.6.5) provides an example GSN structure for a complex project with numerous stakeholders.

- Application specific Safety Cases. Once a goal structure has been developed for a specific application it is often possible to re-use some of, if not all of, the captured argument for another similar application. The fact that GSN explicitly defines operation, location and assumptions through its use of context and assumptions elements makes the job of transferring arguments simpler. Case Studies 2 (E.6.6) and 3 (E.6.7) below, provide examples of the use of GSN during the development of application-specific Safety Cases.

GSN can also be used to illustrate the different levels of a Safety Case, that is, to explain how particular analyses and mitigations contribute to the overall argument. For example, GSN can be used to bring the diverse branches (hazard mitigation, standard compliance, design integrity etc.) of an existing Safety Case together to present a single coherent safety argument. Alternatively, it may be used to express some particularly complex aspects of a Safety Case such as the mitigation of hazards and the demonstration of ALARP. GSN makes these levels clearly visible and so helps you to avoid duplicated work and ensure that the safety argument remains structured and concise.

Whilst GSN frequently works well when there are many stakeholders or the safety argument being expressed is complex, there are numerous situations when its application may not be appropriate. These include:

- When safety arguments are routine or simple, or just involve compliance with standards. In these cases there may be no point in developing a GSN structure, as the steps required to be undertaken to justify safety may be easily deduced and evident without using GSN;

- When the project or scheme is significantly part-way through the Safety Case process and the reviewer is familiar with the existing Safety Case; and

- When making ‘minor’ revisions to existing text-based Safety Cases or risk assessments.

GSN is a new tool in terms of its application to railway Engineering Safety Management. The Yellow Book Steering Group would therefore appreciate feedback on its application on the railway in order to provide further improved guidance to Engineering Safety Management practitioners.

E.6.4 How to Use GSN

The most robust way to create a goal structure is through a systematic group discussion, not too dissimilar to those suggested by the Yellow Book for undertaking creative hazard identification.

---

6 Judgement is required by the risk assessment developer as to whether GSN is the most appropriate tool to use. Other tools exist as outlined below and we recommend that you select the most appropriate tools based on the level of risk presented by the project or scheme, and thus the level of detail and work required to support the safety argument.

7 Feedback can be provided via the feedback form in the back of this volume.
The fundamental steps involved in developing a GSN goal structure are [F.42] as follows:

1. Define the Goal: Initially this will be the overall objective of the safety argument

   System X is acceptably safe to operate

2. State the Context(s): This is the basis on which the goal (or sub-goal) is claimed. For example, to argue that “System X is acceptably safe...” it is necessary to define exactly what is meant by “acceptably safe”.

   System X is acceptably safe to operate
   “Acceptably Safe” = all risks reduced to ALARP

3. Identify Strategies: These should describe how the claim is substantiated. In certain situations the approach may be obvious, but typically strategies need to be made explicit using a Strategy element. For instance, the two strategies for the demonstration that System X is safe may be by the mitigation of hazards and compliance to relevant standards.

   System X is acceptably safe to operate
   Argument that all hazards controlled
   Argument that all applicable standards met

4. Justify the Strategy(ies) and State any Assumptions: Once a strategy has been made explicit it may be useful to state why the approach was adopted using a Justification element. Similarly, any assumptions made should be defined and contextual information added.

   All hazards identified During HAZOP
   Infrastructure is not TSI Compliant – Standards compliance alone will not demonstrate ALARP

5. Further Develop Strategies into Sub-Goals or Solutions as Necessary: Eventually after a number of iterations a claim will not need further expansion, refinement or explanation. In such situations a Goal can be supported directly by a Solution which refers to a piece of evidence.

   Argument that all hazards controlled
   All Safety Requirements Met

   Hazard Log Ref. XX

Figure E-5 How to develop a GSN structure

GSN is a fast and easy-to-use tool. The pictorial representation of the safety argument can be quickly developed and this enables the reviewer to identify at a very early stage in the project if any supporting evidence is missing.
The GSN goal structure can help you to identify the tasks required to be undertaken to justify the safety argument and so help you to write a Project Safety Plan (including programme) as described in the Yellow Book. You would not normally expect to have a sub-goal associated with each hazard, but you would expect sub-goals associated with a robust hazard identification, analysis and management process, with the associated solutions as to how that can be achieved (see Yellow Book Volume 2). GSN could, however, be used to provide a clear structure for the mitigation of key hazards which have their own complex arguments, for instance, a hazard associated with electromagnetic interference.

In some circumstances, the Safety Case developer may be required to follow a Safety Case structure recommended by a particular standard or guideline, for example EN 50129, which has defined section structure headings for a Safety Case. In these circumstances, GSN may still be an appropriate tool to use. You would still structure the Safety Case, as required, but then have the GSN goal structure point where necessary to the appropriate sections of the report. The GSN methodology facilitates a check that all the parts of the Safety Case link together and are integrated and well-structured to support the top-level argument. GSN would also ensure that evidence is not duplicated.

There are pitfalls with the use of GSN, and the following is provided as guidance on how not to apply it:

- We recommend the consideration of the whole railway system, in order to avoid the risks at system boundaries being missed. GSN should not therefore be used to simply compartmentalise a major project, as this could increase the risk of system integration problems and hazardous events. If the goal structure simply follows the structure of your system or your team, then you may have fallen into this trap, as you should expect some goals to apply across the organisation or to more than one (or even all) parts of a system.

- Risks can arise when changing between normal and failed states. For instance, when a system is repaired it must continue the safety arrangements enforced during the failure, that is, it must remember the moves already in progress and not set up some new conflicting moves. The goal is therefore to keep the railway safe through all its operating, maintenance and credible failure modes, and also all mode transitions. If you just set sub-goals associated with each mode, you may leave the mode-transition matters without consideration. Make sure, therefore, that the goal structure has sub-goals that cover the transitions between normal and failed states and back again.

- Just because you have developed a GSN goal structure it does not automatically follow that your safety argument is good. GSN is not a substitute for clarity of thought (although one of its benefits is that it can expose a lack of clarity). Similarly, following the EN 50129 or Yellow Book Safety Case, document structures do not in themselves guarantee safety. Chapter 18 provides further guidance in this respect.

- GSN should not be thought of as a tool for creating a work breakdown structure. The solutions may help to identify tasks, but they are not tasks, they are evidence of requirements needed to support a particular objective.
E.6.5 Case Study 1: New Railway Scheme

We recommend that the railway should be considered as a system. It is not adequate to consider one product or task in isolation. GSN provides a quick method of identifying at the outset of the project what the interfaces to the other components of the railway system are and ensure that a 'systems view' is taken.

Figure E-6 illustrates a GSN structure for a new railway scheme (for example, CTRL Section 2), and demonstrates the strength of GSN in complex applications where there could be numerous stakeholders. The structure illustrates how the different elements of the scheme fit together and how all the sub-systems are actually closely integrated.

Figure E-6 is the highest level of the safety argument structure, so the areas of the structure requiring further development into sub-objectives, until solutions (sources of evidence) can be identified, are clearly indicated using the diamond symbol (see Figure E-5 above).
### E.6.6 Case Study 2: Assurance of a New Product

GSN is particularly beneficial for complex safety arguments. Figure E-7 provides an example GSN structure for a new rolling stock project. The rolling stock manufacturer and the Safety Case reviewer undertaking the independent safety verification must ensure that the train is acceptably safe. This example assumes that the goal is to reduce the associated risks from introducing the new trains to a level which is As Low As Reasonably Practicable (ALARP), which may not be appropriate in all cases. Common Safety Targets or similar could also be incorporated.
The strategy to demonstrate that the train is acceptably safe is founded on a risk-based safety argument. This safety argument is documented in a Safety Case (Goal 02), and the strategy to deliver this goal is based on an argument that all requirements have been met through a combination of evidence from previous similar applications, test data specific to this application, and the implementation of robust management processes in accordance with the good practice outlined within this volume.

The strength of this GSN model is that the Safety Case can now start to be developed with a measure of confidence that all of the key issues will be addressed and the safety argument will be concisely presented. The solutions at the bottom of the structure will identify what evidence is required to support the safety argument, and thus the Project Manager is able to ensure resources are allocated as appropriate to obtain this evidence. The GSN structure therefore provides a good medium to communicate the aims of the project, whilst providing a planning tool for the Project Manager to identify the work required to be undertaken to support the safety argument, with an assurance that this work is directly supportive of the project aims. Without too much further work, a Safety Strategy document could quickly be developed around this structure, with a clearly defined safety argument and the key areas of evidence identified at the outset of the project, to provide confidence in the overall safety management strategy adopted.
E.6.7 Case Study 3: Cross-Acceptance

Experience in the rail industry (for instance the Sheerness resignalling scheme) to-date has demonstrated that GSN may be beneficial in the cross-acceptance of a system.
For the Sheerness branch resignalling\textsuperscript{8} much of the signalling scheme was traditional, using conventional track circuits and colour light signals. However, the use of axle counters introduced an element of novelty into the scheme, so that an application-specific Safety Case for the scheme was necessary.

Figure E-8 provides an extract of the argument constructed in GSN for the resignalling project. The project was required to meet the ALARP Principle. The argument was based on the premise that an ‘adequate level of safety’ would be achieved as long as:

- hazards associated with the use of the new signalling control system for the project had been identified; and
- precautions had been taken, or were in place, with respect to each hazard, that either reflected good practice (where the risk is low and appropriate best practice exists) or are shown to be sufficient to reduce the level of risk associated with the project to a level that is at least tolerable and ALARP.

Since much of the signalling system had already been previously certified by the relevant approvals body, the two main goals (G1 and G2) used in the goal structure distinguished between inherited hazards (hazards which were considered to be no different to the previous application and with risk reduction measures already in place) and new hazards (hazards which had not been considered before and for which adequate risk reduction measures needed to be identified).

For the inherited hazards, the argument was that all previously identified hazard prevention or mitigation measures were considered and that those measures which were relevant to the current scheme had been implemented correctly. Reference to, and review of, existing evidence reduced the effort needed to produce this aspect of the argument.

For the new hazards, it was necessary to argue that an appropriate process was adopted for the identification of the hazards and that all adequate mitigation measures had been identified and implemented correctly. The techniques adopted here were similar to those that would be adopted for any new development.

The use of GSN in this application facilitated communication of the Safety Case argument to the key stakeholders, including the appointed ISA, and enabled the approvals body (Network Rail) to gain a better and more immediate understanding of the management of safety for the project.

\textsuperscript{8} This example has been published with the kind permission of GE Transportation Systems and ERA Technology Ltd.
Figure E-8 Extract of Sheerness Branch Resignalling Scheme Safety Argument

G0
The Signalling Control System used for the Sheerness Branch Resignalling project provides an adequate level of safety for railway operations.

S
Argument built on similarities with previously approved applications of the Signalling Control Systems and compliance with generic product approval constraints and limitations.

C01
Adequate safety defined in YB3 as 'risks reduced to at least tolerable and as low as reasonably practicable (ALARP)'

C0
Project Specification for Sheerness Branch Resignalling

Adequate additional prevention / mitigation measures have been taken with respect to all new hazards or their causes associated with the application of the Signalling Control System on the Sheerness Branch Resignalling project.

C5
Baseline application and product approval safety case submissions.

C0
System Design Specification for the Sheerness Branch Resignalling.
Figure E-8 (cont.) Extract of Sheerness Branch Resignalling Scheme Safety Argument
E.6.8 Summary of GSN Benefits

In summary, the benefits of using GSN [F.43] for railway projects are that the development of a GSN structure during the planning phase of a project:

- provides a clear and comprehensive safety argument;
- aids easy construction of the safety argument; and
- improves communication through a clear representation.

Includes argument context:

- is easily understood by readers of varying skill levels;
- provides justification for parent to child relationship within the argument; and
- ensures that all effort to develop safety evidence is directly in support of the safety argument and not wasted.

E.6.9 How to Get Started

The aim of this section (see above) was to ‘to provide authors and reviewers of safety and risk assessments with an introduction to how GSN can be used’. If you require more than just an introduction in order to get started, training courses in the application of GSN for Safety Cases in the railway industry have been developed and are available from professional organisations; and commercial tools are available to support the presentation of the GSN structures. In addition, the University of York has set up a GSN User Group [F.44], which shares information across industry sectors on the application of GSN.

A full list of references to further information can be found in the following section. In particular, [F.45] provides details on the use of ‘Modular’ GSN structures. This modular approach enables the Safety Case to be partitioned into separate safety arguments corresponding to the main components of the system architecture. Additional symbols have also been developed to facilitate the development of these ‘modular’ arguments for particularly large or complex projects.

As stated at the beginning of this section, GSN is only one tool which can be used to assist in the structuring of safety arguments. Other examples of similar tools include:

- Toulmin’s Notation [F.20]. Describes a pattern for the structure of a typical argument.
Appendix F

Referenced documents

This appendix provides full references to the documents referred to in the body of this volume.


F.2 RSSB, How Safe is Safe Enough?, Edition 1a: February 2005


F.4 Department for Transport, Railways (Interoperability) Regulations 2006 Guidance


F.8 Railway Group Standard GE/RT8250, Safety Performance Monitoring and Defect Reporting of Rail Vehicles, Plant & Machinery, Issue 1, June 2001


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
<table>
<thead>
<tr>
<th>Referenced documents</th>
<th>Appendix F</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.15 ISO 10007:2003, Quality management systems. Guidelines for configuration management</td>
<td></td>
</tr>
<tr>
<td>F.17 Health and Safety Executive, Reducing Risk, Protecting People, 2001, ISBN 0 7176 2151 0</td>
<td></td>
</tr>
<tr>
<td>F.25 The Railway Strategic Safety Plan 2006, RSSB</td>
<td></td>
</tr>
<tr>
<td>F.26 EN 50128:2001, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems</td>
<td></td>
</tr>
<tr>
<td>F.28 Health and Safety Executive, Methods for assessing the safety integrity of safety-related software of uncertain pedigree (SOUP), 2001</td>
<td></td>
</tr>
<tr>
<td>F.29 German Federal Railways Standard Mü 8004</td>
<td></td>
</tr>
<tr>
<td>F.30 Railway Industry Association, Safety related software for railway signalling (RIA 23), 1991</td>
<td></td>
</tr>
<tr>
<td>F.33 EN 41003:1999, Particular safety requirements for equipment to be connected to telecommunications networks</td>
<td></td>
</tr>
<tr>
<td>F.34 BS 7671:2001, Requirements for electrical installations. IEE Wiring Regulations. Sixteenth edition</td>
<td></td>
</tr>
</tbody>
</table>
F.35 BS 5760: Part 5 1991, Reliability of systems, equipment and components: Part 5 Guide to failure modes, effects and criticality analysis


F.37 Kletz Trevor A., Hazop and Hazan, (The Institution of Chemical Engineers, 2006), ISBN 0852955065

F.38 Civil Aviation Authority Safety Regulation Group, CAP 760, Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases for Aerodrome Operators and Air Traffic Service Providers, 13 January 2006


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
<table>
<thead>
<tr>
<th>Your suggestions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your name and address:</strong></td>
</tr>
<tr>
<td><img src="image.jpg" alt="Image" /></td>
</tr>
</tbody>
</table>

**Your suggestions for changing the Yellow Book:**

**Please photocopy this sheet and send or fax your comments to:**

<table>
<thead>
<tr>
<th>ESM Administrator</th>
<th>Phone: +44 (0)20 7904 7777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail Safety and Standards Board</td>
<td>Fax: +44 (0)20 7557 9072</td>
</tr>
<tr>
<td>Evergreen House</td>
<td>Or you may email your comments to</td>
</tr>
<tr>
<td>160 Euston Road</td>
<td><a href="mailto:info@yellowbook-rail.org.uk">info@yellowbook-rail.org.uk</a></td>
</tr>
<tr>
<td>London NW1 2DX</td>
<td></td>
</tr>
</tbody>
</table>

**For our use**

<table>
<thead>
<tr>
<th>Suggestion number:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status (open or closed):</td>
<td></td>
</tr>
<tr>
<td>Reply sent:</td>
<td></td>
</tr>
</tbody>
</table>
### INDEX

#### A

**Accident**
- Data: 7, 9, 11, 228, 241, 242, 285, 286, 287
- Sequence: 228, 234, 242, 257, 286
- Target: 29, 198
- See Assumptions, Dependencies and Caveats

**ALARP**
- Criteria: 275, 277, 278
- Demonstration: 183, 184
- Principle: 138, 164, 165, 166, 180, 182, 228, 234, 267, 309
- See As Low As Reasonably Practicable

**Assumptions, Dependencies and Caveats**
- 41, 121, 122, 123, 124, 125, 168, 187

#### B

**Barrier**
- 9, 177, 178, 229, 271

**Automatic Half**
- 267, 277, 278

#### C

**Causal Factor**
- 8, 9, 27, 175, 176, 229

**Commercial Off The Shelf**
- 213

**Consequence**
- 96, 139, 163, 177, 178, 182, 186, 206, 228, 229, 269, 271, 273, 274, 286, 295

**COTS**
- See Commercial Off The Shelf

#### D

**Data Reporting, Analysis and Corrective Action System**
- 91, 222, 229, 230

**DRACAS**
- See Data Reporting, Analysis and Corrective Action System

#### E

**Engineering Safety Management**
- 3, 12, 24, 27, 53, 54, 97, 136, 138, 151, 172, 217, 227, 229, 237, 298, 301, 302

**Activities**
- 22, 29, 34, 52, 63, 90, 100, 101, 125, 142, 216, 217, 233, 253

**Application**
- 24, 155, 172, 236

**Documents**
- 91, 145, 235

**Fundamentals**
- 11, 17, 18, 89

**Responsibilities**
- 51, 63, 64

**Error**
- Configuration Data: 118
- Human: 11, 28, 180
- Likelihood of: 181

**ESM**
- See Engineering Safety Management

**Event**
- Hazardous: 107, 304
- Higher: 294
- Input: 294
- Output: 294
- Top: 202, 230, 293, 294

#### F

**Failure**
- Component: 52, 173, 175, 212, 218, 294
- Critical: 41, 64, 294
- Equipment: 250
- Hidden: 204
- Predictive: 90
- Probability: 199, 202, 215
- Right-side: 178, 231
- Software: 108, 201, 202, 214, 215
- System: 120, 181, 185, 202, 255, 293
- Systematic: 7, 8, 28, 29, 161, 197, 198, 199, 234, 287
- Wrong-side: 234, 261

**Failure Mode and Effects Analysis**
- 173, 174, 229, 292

**Failure Mode, Effects and Criticality Analysis**
- 174, 230
<table>
<thead>
<tr>
<th>Index</th>
<th>Engineering Safety Management Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Requirements Specification</td>
<td>28, 100, 137, 147, 196, 197, 201, 202, 203, 211, 219, 233, 238, 239, 240, 284</td>
</tr>
<tr>
<td>Safety Standard</td>
<td>53, 140, 219, 233</td>
</tr>
<tr>
<td>Safety Value</td>
<td>182, 184, 234</td>
</tr>
<tr>
<td>Safety-related</td>
<td>52, 57, 65, 66, 71, 82, 83, 103, 104, 105, 133, 134, 199, 203, 211, 233, 234, 251, 253, 287</td>
</tr>
<tr>
<td>Activities</td>
<td>104, 116, 127, 220, 253</td>
</tr>
<tr>
<td>Information</td>
<td>20, 58, 77, 79, 80, 81, 82, 123, 124, 191</td>
</tr>
<tr>
<td>Projects</td>
<td>25, 70, 97, 117, 219</td>
</tr>
<tr>
<td>Software</td>
<td>102, 201, 202, 213, 215</td>
</tr>
<tr>
<td>System</td>
<td>56, 70, 96, 233</td>
</tr>
<tr>
<td>Tasks</td>
<td>52, 66, 67, 69, 73</td>
</tr>
<tr>
<td>Work</td>
<td>25, 28, 53, 54, 69, 73, 75, 81, 102, 103, 135, 189, 197, 207</td>
</tr>
<tr>
<td>Signal Passed at Danger</td>
<td>269</td>
</tr>
<tr>
<td>SIL</td>
<td>213</td>
</tr>
<tr>
<td>Software Of Unknown Pedigree</td>
<td>213</td>
</tr>
<tr>
<td>SOUP</td>
<td>213</td>
</tr>
<tr>
<td>System Lifecycle</td>
<td>10, 21, 39, 52, 60, 66, 73, 80, 90, 96, 114, 117, 127, 136, 151, 160, 191, 198, 233, 234, 253</td>
</tr>
<tr>
<td>The 'Railways and Other Guided Transport Systems (Safety) Regulations 2006'</td>
<td>135, 209</td>
</tr>
<tr>
<td>Tolerability Region</td>
<td>166, 182, 228, 234, 279</td>
</tr>
<tr>
<td>Transport Operator</td>
<td>53, 56, 80, 86, 101, 108, 154, 162, 171, 179, 234</td>
</tr>
<tr>
<td>Transport Undertaking</td>
<td>154, 234</td>
</tr>
<tr>
<td>UML</td>
<td>See Unified Modeling Language</td>
</tr>
<tr>
<td>Unified Modeling Language</td>
<td>168</td>
</tr>
<tr>
<td>Upper Limit of Tolerability</td>
<td>182, 193, 184, 277, 278, 279</td>
</tr>
<tr>
<td>Value of Preventing a Fatality</td>
<td>179, 234</td>
</tr>
<tr>
<td>VPF</td>
<td>See Value of Preventing a Fatality</td>
</tr>
</tbody>
</table>