

*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

Published in 2005 by:
Rail Safety and Standards Board
Evergreen House
160 Euston Road
London NW1 2DX.
Phone: +44 (0)20 7904 7777
www.rssb.co.uk

Copyright © Rail Safety and Standards Board 2005

You can order further copies from RSSB.

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	Eddie Goddard
Roger Aylward	Philip de Graaf
Neil Barnatt	Nick Holmes-Mackie
Richard Barrow	Roger Kemp
Paul Cheeseman	Alan Lawton
John Corrie	Robert Mole
Robert A Davis	Richard Tavendale
Bruce Elliott	Keith Watson
Terry George	

The members were drawn from the following organisations:

AEA Technology Rail	Mott MacDonald Limited
Atkins Rail	Network Rail
Praxis High Integrity Systems	Lancaster University
ProRail	Lloyd's Register Rail Limited
Rail Safety and Standards Board	London Underground Limited
Union Railways (North)	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

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

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.

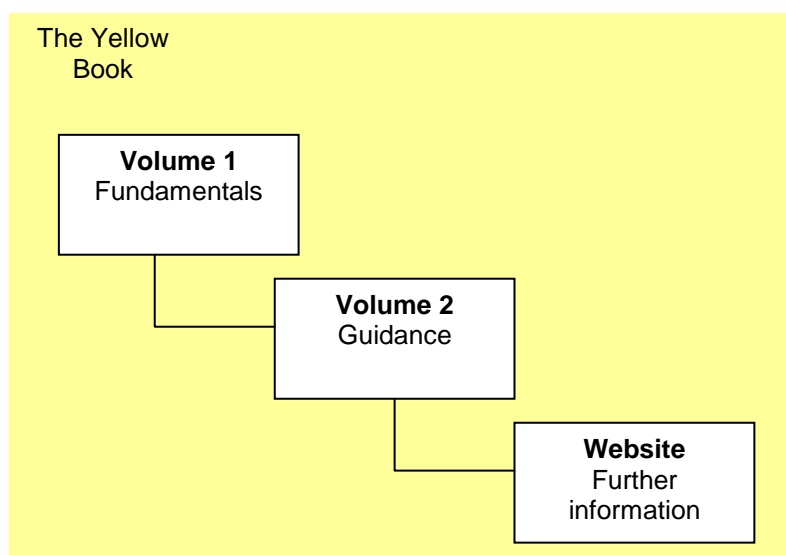


Figure 1 – Overall structure of the Yellow Book

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.

CENELEC standards EN 50126:1999, *Railway Applications –The Specification and Demonstration of Reliability, Availability, Maintainability and Safety* and EN 50129:2003, *Railway Applications – Safety Related Electronic Systems for Signalling* contain guidance on engineering safety cases for some sorts of railway projects and products.

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:

- 1 Anthony Hidden QC, *Investigation into the Clapham Junction Railway Accident*, HMSO, ISBN 0 10 108202 9
(Analysis of weaknesses in management at the root of one of the worst recent British railway accidents.)
- 2 Rt Hon Lord Cullen PC, *The Ladbroke Grove Rail Inquiry Reports*, HSE Books, Part 1: ISBN 0 7176 2056 5; Part 2: ISBN 0 7176 2107 3
(Analysis of causes of one of the worst recent British railway accidents.)
- 3 James Reason, *Managing the Risks of Organisational Accidents*, ISBN 1 84014 105 0
(An in-depth discussion of the organisational factors which contribute to accidents.)
- 4 Construction Industry Advisory Committee, *A Guide to Managing Health and Safety in Construction*, 1995, ISBN 0 7176 0755 0
(Thorough guidance on the duties imposed by the Construction (Design and Maintenance) Regulations 1994.)
- 5 Stanley Hall, *Beyond Hidden Dangers: Railway Safety into the 21st Century*, 2003, Ian Allan Publishing Ltd, ISBN 0711029156
(A readable and thoughtful survey of accidents on the UK railway since the beginning of the railway era.)
- 6 HSE, Discussion document *Safety on the Railway – Shaping the Future*, October 2003
(Presentation of options for reforming UK railway safety law.)
- 7 PAS 55-1: 2003, *Asset Management; Specification for the Optimised Management of Physical Infrastructure Assets*, BSI
(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.

- 1 The Engineering Council, *Guidelines on Risk Issues*, February 1993, ISBN 0-9516611-7-5
- 2 HSE, *Policy Statement on Relationship Between Technical Specifications for Interoperability, the Health and Safety at Work Act, Railway Group Standards & Railway Safety Principles and Guidance*, published on www.hse.gov.uk, 3 September 2003
- 3 HMRI, *Railway Safety Principles and Guidance ('Blue Book')*, ISBN 0 7176 0712 7
- 4 Hazards Forum, *Safety-related Systems – Guidance for Engineers*, March 1995, ISBN 0 9525103 0 8
- 5 BS EN 61508 : 2002, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- 6 HSE, *Reducing Risks, Protecting People*, 2001, ISBN 0 7176 2151 0
- 7 BS EN 50129 : 2003, *Railway Applications – Safety Related Electronic Systems for Signalling*
- 8 BS EN 50126 : 1999, *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety*
- 9 Rail Safety and Standards Board, *How Safe is Safe Enough*, Edition 1a, February 2005

Your suggestions	
Your name and address:	Your phone number:
Your suggestions for changing the Yellow Book:	
Please photocopy this sheet and send or fax your comments to:	
ESM Administrator Rail Safety and Standards Board Evergreen House 160 Euston Road London NW1 2DX	Phone: +44 (0)20 7904 7777 Fax: +44 (0)20 7557 9072 Or you may email your comments to info@yellowbook-rail.org.uk
For our use	
Suggestion number:	
Status (open or closed):	
Reply sent:	