

Engineering Safety Management

Issue 3

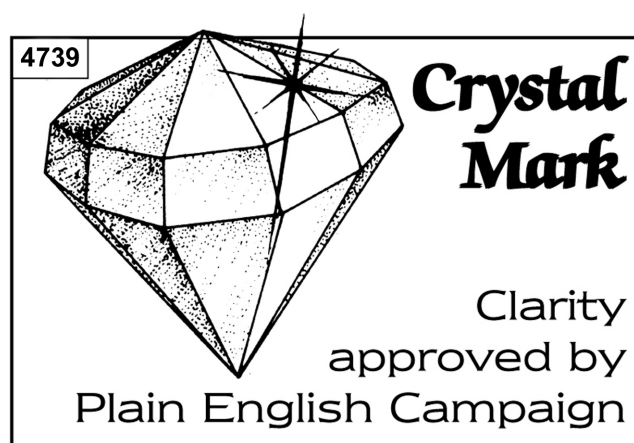
Yellow Book 3

Volume 1

Fundamentals

Disclaimer

Railtrack has taken trouble to make sure that this document is accurate and useful, but it is only a guide. The company does not give any form of guarantee that following the recommendations in this document will be enough to ensure safety. Railtrack will not be liable to pay compensation to anyone who uses this guide.



The Crystal Mark applies to volume 1 only.

Published by Railtrack on behalf of the UK rail industry

Published in January 2000 by:
Railtrack PLC
Railtrack House
Euston Square
London NW1 2EE.
Phone: 020 7557 8000
www.railtrack.co.uk

Distributed by:
Praxis Critical Systems Limited
20 Manvers Street
Bath BA1 1PX.
Phone: 01225 466991
www.praxis-cs.co.uk

Copyright © Railtrack PLC 2000

You can order further copies from the ESM administrator at Praxis Critical Systems.

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 and supported our customers and suppliers by giving details of some of our internal procedures for Engineering Safety Management.

We published Issue 2 of the Yellow Book in 1997 in four volumes. This issue added more basic safety information, written specifically for those managing safety engineering.

After publishing issue 2, we set up a steering group to direct further development of the Yellow Book. We also set up a user group, bringing together people with responsibility for safety from the railway and other industries, to support the steering group.

We wrote issue 3 of the Yellow Book, under the direction of the steering group, with input from users, through the user group and other channels. We now publish material that is specific to Railtrack separately, and the Yellow Book has been aligned with relevant international standards. The guidance in the Yellow Book is no longer specific to Railtrack and may be useful in connection with other railways.

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.

Roger Aylward

Alan Cooksey

Robert A Davis

Bruce Elliott

Eddie Goddard

Ali G Hessami

Roderick I Muttram

Chris Thompson

Brian Clementson

John D Corrie

Andy Doherty

Terry George

Colin Hall

Jim Irwin

Dee Razdan

The members were drawn from the following organisations:

DaimlerChrysler Rail Systems (UK) Limited

HSBC Rail (UK) Limited

Mott MacDonald Limited

Railtrack PLC

Westinghouse Signals Limited

Her Majesty's Railway Inspectorate

London Underground Limited

Praxis Critical Systems Limited

Virgin Trains

WS Atkins Rail Limited

We are also grateful to Plain English Campaign for their help in writing this document.

Volume structure

Volume 1 Engineering Safety Management Fundamentals

- 1 Introduction
- 2 Obligations and liabilities
- 3 Engineering safety management fundamentals
- 4 Putting the fundamentals into practice

Volume 2 Engineering Safety Management Guidance

Part 1: Introductory material

- 1 Introduction

Part 2: Organisational fundamentals

- 2 Safety responsibilities
- 3 Safety culture
- 4 Competence and training
- 5 Working with suppliers
- 6 Communicating and co-ordinating

Part 3: Change fundamentals

- 7 Defining changes
- 8 Identifying hazards and assessing and reducing risk
- 9 Safety requirements
- 10 Safety evidence and authorising change

Part 4: Project fundamentals

- 11 ESM from start to finish
- 12 Safety planning and good practice
- 13 Configuration management, documentation and records
- 14 Independent professional review

Appendices

- A Glossary
- B Document outlines
- C Checklists
- D Examples
- E Techniques
- F Referenced documents

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
2 OBLIGATIONS AND LIABILITIES	4
2.1 UK law	4
2.2 Railways (Safety Case) Regulations	5
2.3 'Reasonable practicability'	5
2.4 Good practice	6
3 ENGINEERING SAFETY MANAGEMENT FUNDAMENTALS	8
3.1 Organisations	9
3.2 Changes	11
3.3 Projects	14
4 PUTTING THE FUNDAMENTALS INTO PRACTICE	16
5 OTHER REFERENCES	16

1 INTRODUCTION

1.1 Purpose

Safety has always been the first concern for the railway. It is due to the professionalism and vigilance of its workers that railway transport is so safe, compared to other forms of transport.

Railtrack has written *Engineering Safety Management* (or the *Yellow Book* as it is more commonly known) to help people who are involved in *changes* to the railway (such as new trains and signalling) make sure that these changes contribute to improved safety. Please do not be misled by the title. The Yellow Book is not just for engineers and you can use it for changes that involve more than just engineering. We considered other titles but felt that it was least confusing to keep the title people were familiar with.

We originally published the Yellow Book for our own purposes. However, in our Network Management Statement and our Railway Safety Case, we have committed ourselves to taking a central role in Britain's railways. We have therefore sponsored issue 3 on behalf of the whole industry, under the direction of a steering group with members from across the industry.

We have improved the Yellow Book over time. This issue is in two volumes. This volume gives the basic legal background to Engineering Safety Management and the fundamentals of carrying it out. It is relevant to anyone working in the railway industry involved in, or accountable for, changing the railway. Volume 2 gives more specialised guidance as described on the next page.

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

System – any collection of equipment, people and procedures which work together to achieve a common goal. We can treat any change to the railway as introducing a new system or changing an existing one.

Engineering Safety Management (ESM) – managing the safety of changes which may affect railway safety. This involves considering the safety of the railway throughout the life of the change but is mostly done before the change is made. We cannot separate engineering from the other factors that affect safety, particularly human factors. ESM involves considering all relevant factors.

Engineering safety case – this presents the justification for the safety of a change to the railway. (Like ESM, an engineering safety case covers more than just engineering.) This is different from a **railway safety case** which is a document that describes an organisation's arrangements for safety management. Where we use **safety case** on its own, we mean an engineering safety case.

1.3 The structure of the Yellow Book

Issue 3 of the Yellow Book is in two volumes:

- 1 Engineering Safety Management Fundamentals
- 2 Engineering Safety Management Guidance

Volume 1 describes some of the safety obligations on people involved in changing 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 advice on ways that have proved effective.

Volume 2 is in three main parts, corresponding to the three groups of fundamentals we describe in this volume. We give guidance on each fundamental in a separate section. There is also a CD-ROM which provides information that supports volume 2.

Volumes 1 and 2 are relevant to you if you are involved in railway ESM, whether or not you are looking to gain our safety acceptance. If you are looking to gain our safety acceptance, you should also read our industry guidance on our acceptance procedures. This describes how we grant safety acceptance and gives guidance on how to get it.

Other organisations, such as Her Majesty's Railway Inspectorate (HMRI) and London Underground Limited, also publish guidance on their safety acceptance procedures. However, these publications are not directly associated with the Yellow Book.

Figure 1 shows the overall structure of this Yellow Book, and figure 2 gives a guide to the content and intended readers of each part.

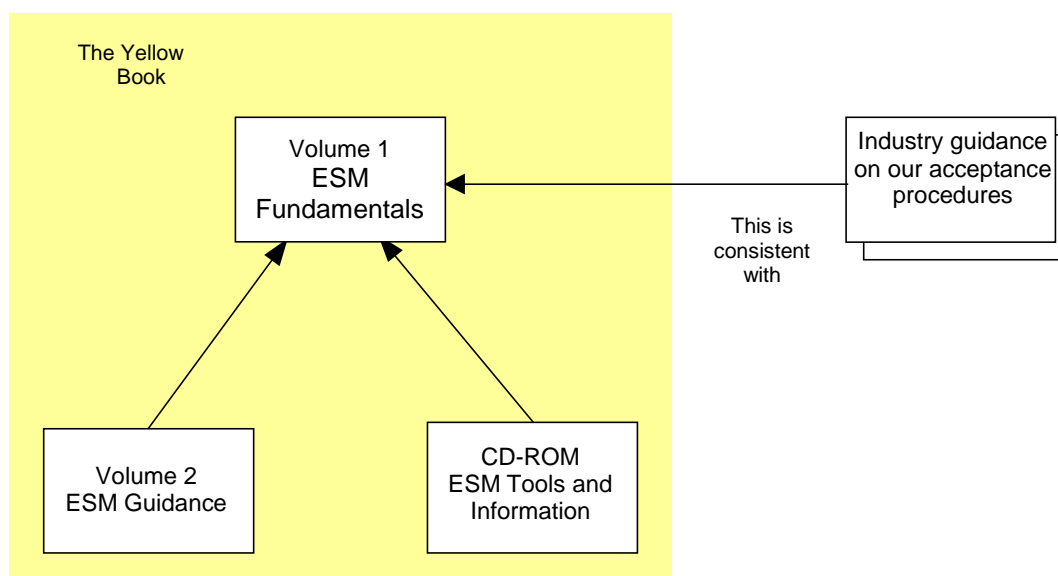


Figure 1 – Overall structure of the Yellow Book

Part	Content	Intended readers
Volume 1 – Engineering Safety Management Fundamentals	<ul style="list-style-type: none"> • The essential features of an effective approach to ESM 	<ul style="list-style-type: none"> • Senior executives in the railway industry • Anyone whose work contributes to railway change
Volume 2 – Engineering Safety Management Guidance	<ul style="list-style-type: none"> • Guidance on one proven way of putting the fundamentals into practice 	<ul style="list-style-type: none"> • Anyone whose work contributes to railway change • Anyone assessing or auditing this kind of work
CD ROM – Engineering Safety Management Tools and Information	<ul style="list-style-type: none"> • Practical support to assess risk 	<ul style="list-style-type: none"> • Anyone carrying out a risk assessment
Industry guidance on our acceptance procedures	<ul style="list-style-type: none"> • Railtrack policy and guidance on gaining Railtrack safety acceptance 	<ul style="list-style-type: none"> • Anyone seeking our safety acceptance • Anyone assessing or auditing projects for which Railtrack safety acceptance is requested

Figure 2 – Content and intended readers of the Yellow Book, and associated publications

2 OBLIGATIONS AND LIABILITIES

The main purpose of the Yellow Book is to help you set up a process that protects you and others from mistakes and gives documented evidence (the engineering safety case) that risk is at an acceptable level. The Yellow Book also helps you to keep within the law and relevant standards.

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 UK law, but the discussion is no substitute for detailed legal advice.

2.1 UK law

The Government reviewed the arrangements for regulating railway safety before privatising the British main line railway. It followed recommendations in the report '*Ensuring Safety on Britain's Railways*' and confirmed that the Health and Safety Executive (HSE) would be the safety regulator for the whole railway network. In fact HMRI, which is part of HSE, does the regulating.

More generally, the '*Health and Safety at Work etc Act 1974*' places duties on employers and employees. Employers must ensure, 'so far as is reasonably practicable', the health, safety and welfare of their employees and of other people they affect. In the case of railways, this includes passengers and other members of the public. Section 2.3 discusses the phrase, 'so far as is reasonably practicable'.

The act applies to those who supply products, such as trains and signalling systems, as well as those who run and maintain the railways. These responsibilities can be shared under a contract but cannot be completely transferred.

The act contains powers to make regulations. Regulations made under the act have the force of law. HSE publishes guidance notes on regulations, which you should read if they are relevant to you.

The '*Management of Health and Safety at Work Regulations 1992*' says employers must assess the risk to employees and others affected by their work. Employers who share a workplace must also co-operate to achieve safety and share safety information.

The '*Construction (Design and Management) Regulations 1994*' place duties on those involved in some construction projects. They must plan, co-operate, share information and keep certain records. This will control the risk to the health and safety of people affected by the project. The people involved must be able to show HSE that they have done this.

The '*Railways (Safety Critical Work) Regulations 1994*' place a duty on those who employ people doing defined 'safety-critical' work on the railway to assess that they are competent and fit to do the work. The assessment must be recorded.

The '*Railways (Safety Case) Regulations 1994*' say that train and station operators and railway infrastructure controllers must prepare a railway safety case. The railway safety case must be accepted before they start operations and they must follow it. We discuss railway safety cases in the next section.

As well as the railway's own acceptance processes, statutory approval is needed for new and changed railways. The '*Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations 1994*', made under the '*Transport and Works Act 1992*', confirm the powers given to HMRI by earlier laws. They also extend them, in particular, to include the general power to approve trains.

HMRI publishes guidance on how the regulations apply and how to get approval. The approval process is similar to the railway's own acceptance process. In many cases, the work done to get railway acceptance will help to get HMRI approval as well.

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

2.2 Railways (Safety Case) Regulations

Any train or station operator must write a railway safety case and have it accepted before starting operations. The operator must then follow their safety case.

HSE accepts railway safety cases from the infrastructure controller, who owns and runs the infrastructure. The infrastructure controller may accept railway safety cases from train and station operators.

The Railway Group is made up of us and those organisations whose railway safety cases we accept.

Among other things, the railway safety case must describe:

- the operator's safety policy and arrangements for safety management;
- the operator's 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.

A railway safety case must also show a systematic approach to managing technical change in general. An engineering safety case shows a systematic approach to managing the safety of one change to the railway. The two are different but related and an engineering safety case can support a railway safety case.

2.3 'Reasonable practicability'

We have seen that 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. We have taken account of the HSE discussion document, '*Reducing Risks, Protecting People*'.

If you are working on a change to the railway, you should first identify the hazards associated with the change. 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, government guidance and standards. If the risk is low and completely covered by good practice, published by a recognised authority, showing that you have followed this good practice 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.

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 the part of the railway being changed. 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 always 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 reduce the risk.

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

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 the risk as low as reasonably practicable.

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

To decide whether a step that would reduce risk is reasonably practicable, you must balance the reduction in risk against other factors. These include cost and any increase in complexity.

In *'Reducing Risks, Protecting People'*, HSE suggest that you can use a figure of slightly under £1 million (at 1998 prices) as a 'benchmark' – an indication of what it is reasonably practicable to spend to reduce risk by one fatality. However, you should use a higher figure for risks for which there is high public concern. As risks of major railway accidents fall into this category, the benchmarks used in railway decision making are often higher.

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.

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.

2.4 Good practice

The main reason for using good practice is to reduce 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. This could help your defence against a charge of negligence and reduce other legal liabilities.

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

Our Safety and Standards Directorate maintains a series of *'Railway Group Standards'*, which cover aspects of the UK main line railway and members of the Railway Group must meet these.

HMRI's '*Railway Safety Principles and Guidance*' (the 'Blue Book') 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 Hazard 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.

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

- 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 have published European standards for railway applications and are working on others.

The Yellow Book is generally in line with these standards and following the Yellow Book guidance will help you meet these other standards. However the Yellow Book takes a wide view of good practice and does not say that you have to follow any one standard.

3 ENGINEERING SAFETY MANAGEMENT FUNDAMENTALS

To make sure that a change to the railway is safe and to show this, you must follow a systematic approach to Engineering Safety Management.

You do not need to carry out a full programme of ESM activities if you can show that the change involves only a 'broadly acceptable' level of risk, or no risk. However, you must monitor the risk to check that it stays low.

If the risk comes completely within accepted standards that define agreed ways of controlling it, showing that you have met these standards 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 you need to carry out an ESM programme, it must have some fundamental features. We can look at these under three headings. These are:

- the **organisation**, including the people who work within it, that will carry out the work;
- the proposed **change** to the railway; and
- the **project**, in other words the collection of activities which will make the change happen.

We use 'organisation' to mean a company, government agency or other corporate group.

Any change to the railway should be managed as a project.

The fundamentals do not just apply to the railway. When we refer to a 'change', this could be a change to any complicated system. In our case, this system will always be the railway, including not just physical parts like the track and trains, but people and procedures as well.

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

3.1 Organisations

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.

You need a structured organisation with good communications to carry out successful ESM. Everyone should have clear responsibilities and understand them.

In particular, anyone whose work creates a risk should be responsible for managing it. They should have the knowledge they need to understand the implications of that risk and to put controls in place.

Your organisation should identify who is accountable for the safety of work. They will stay accountable even if they pass on responsibility, for parts of the work, to others.

The organisation that takes the lead in introducing a change should make sure that the other organisations are clear on their safety responsibilities. If you hand over infrastructure changes to an infrastructure controller or hand over rolling stock to a train operator, you may also transfer some safety responsibility.

3.1.2 Safety culture

Your organisation must have safety as a primary goal.

The most important factor in achieving safety is creating a safety culture. This means running an organisation so that safety is seen as a primary goal and considered appropriately in every activity. Everyone should understand that achieving safety will help to meet business goals. Setting up safety procedures is not enough. All staff should understand why these procedures are necessary and use them.

3.1.3 Competence and training

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

Staff should have the proper training, technical knowledge, skills, experience and qualifications for their job.

3.1.4 Working with suppliers

Whenever your organisation contracts out the performance of ESM activities, 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.

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.

This fundamental is needed to make sure that the other fundamentals do not get lost in contractual relationships. Your organisation will set specific requirements from these fundamentals, which are relevant to the work being done, before passing the requirements on to the supplier. You do not have to pass them on by writing them into the contract, though this is normally a good idea.

3.1.5 Communicating safety-related information

If your organisation has information that someone else needs to reduce risk, your organisation must pass it on.

This information may include problems you find in someone else's work, or assumptions about someone else's work which are important to safety. Your organisation should pass on any relevant information about hazards and safety requirements to its suppliers.

3.1.6 Co-ordination

Whenever your organisation is working with others on one change, they must co-ordinate their ESM activities.

There are specific legal obligations in this area, for instance regulation 9 of the '*Management of Health and Safety at Work Regulations 1992*'.

3.2 Changes

3.2.1 Defining changes

Before starting work on a change, your organisation must define the aims, extent and context of the change.

This is often done in a requirements specification.

If you are in doubt about the aim, extent or context of the change, you will also be in doubt about claims for its safety.

When you define a change you should also find out which authorities will have to approve your safety case.

3.2.2 Identifying hazards

When your organisation considers change, it must make a systematic and vigorous attempt to identify any possible hazards. Your organisation must consider hazards which could contribute to an accident at any time, from introducing the change into the railway to removing it.

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

You should not just consider accidents which might happen during normal operation, but others which might happen at other times, such as installation, track-testing, commissioning, maintenance, emergencies, decommissioning and disposal.

You should consider the people who the change will affect, and design it to help them avoid mistakes.

When identifying hazards, you should consider all the effects of the change 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 grounds for your belief that it is so unlikely to happen.

3.2.3 Assessing risk

Your organisation must assess the effect of any proposed change on overall system risk.

There are legal duties to assess risk.

Risk measures 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 changes are made specifically to make the railway safer, that is to *reduce* risk, at least in the long run. You should still assess them in case they introduce other risks.

3.2.4 Reducing risk

Your organisation must carry out a thorough search for measures which reduce overall system risk, within its area of responsibility. It must decide whether each measure is reasonably practicable and, if so, must take it.

If your organisation finds that risk is still intolerable, it must not accept it.

If the risk is in the broadly acceptable region, you need only consider measures which are clearly reasonably practicable.

There are legal duties to do this.

You should look for:

- ways to get rid of hazards or to reduce their likelihood;
- ways to contain the effects of hazards, if they happen; and
- contingency measures to reduce harm if there is an accident.

You should look for ways of controlling both hazards introduced by the change itself and hazards that are already present in the railway. Even if a change is designed to make the railway safer then you should still see if there are ways that you could make the railway even safer.

3.2.5 Safety requirements

Your organisation must set safety requirements for any change, to reduce the risk associated with the change to an acceptable level.

Safety requirements are requirements that should be met to make sure that the safety risk presented by a change is reduced to an acceptable level. Safety requirements may specify:

- features or functions of the change, including any which help people avoid dangerous mistakes;
- what the change must not do to ensure safety;
- environmental conditions under which the change must operate to stay safe;
- targets for carrying out a function reliably, or reliably avoiding a dangerous state;
- features of the design and build processes; and
- operational procedures and restrictions.

You will set some safety requirements to meet regulations or standards. Others may arise when you identify hazards and assess and reduce risk.

3.2.6 Evidence of safety

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

You should normally put these arguments together in a safety case to show that:

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

If other people must take action before a change is safe, the safety case should describe these actions and show that the other people have accepted responsibility for carrying out these actions.

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

If you are working on signalling systems or equipment, CENELEC standard ENV 50129:1998, '*Railway Applications – Safety Related Electronic Systems for Signalling*' is relevant. It places requirements on safety cases.

3.2.7 Authorising changes

No change can be authorised until all necessary safety approvals have been given.

You must get safety approval from the necessary safety authorities. You will usually need approval from both the railway authority (such as Railtrack and London Underground Limited) and the regulatory authority (HMRI in the UK). Safety approval will normally be based on accepting the safety case.

The approving authority will normally produce a certificate, setting out any restrictions on how the work is used.

The approving authority will usually give safety approval at the end of a project, when the change is about to go into service. Some projects make staged changes to the railway in which case each stage will 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.

3.3 Projects

3.3.1 ESM from start to finish

Your organisation must start ESM activities as soon as possible. It must review the results of these activities, and any assumptions made throughout the project. It must review and extend ESM activities whenever new information makes this necessary. It must monitor information on performance that relates to safety.

You should start early while it is easiest to build safety in. However, you may have little design information early in the project, so you should repeat the hazard analysis and risk assessment activities throughout the project, as the design becomes more detailed.

New information also includes design changes and information on faults.

3.3.2 Safety planning

Your organisation must plan all ESM activities before carrying them out.

You will normally write a safety plan, which should describe how you will put all these ESM fundamentals into practice on your project.

You do not have to write one plan for the whole programme beforehand, but you should plan each ESM activity before you do it.

You should adjust the extent of the safety plan and the ESM activities you carry out according to the extent of the risk.

3.3.3 Systematic processes and good practice

Your organisation must carry out safety-related projects following systematic processes which use good engineering practices. It must write down the processes beforehand.

You should use good systems engineering practice to develop 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.

When choosing methods, you should take account of relevant standards. What is and is not good practice will depend upon the requirements.

3.3.4 Configuration management

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

You should keep track of the items that the project produces and the relationships between them. This is known as configuration management. Your configuration management arrangements should let you:

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

If you are in doubt about any of the above, you cannot be certain that all risk has been controlled.

3.3.5 Records

Your organisation must keep full and auditable records of all project ESM activities.

You should keep records to show that you have followed the safety plan. These records may include the results of design activity, analyses, tests, reviews and meetings. You should keep a hazard log which records all the possible hazards identified and describes the action to be taken to get rid of them, or reduce their likelihood or severity to an acceptable level.

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

You should keep records until you are sure that nobody will need them to make further changes or to investigate an incident. Often you will have to keep records until the change has been removed from the railway.

3.3.6 Independent professional review

ESM activities you carry out must be reviewed by professionals who are not involved in the activities concerned.

These reviews are normally structured as a series of safety audits and safety assessments. They assure that the work has been carried out safely and provide evidence to 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 project. They will depend on the amount of risk and novelty and on how complicated the project is.

4 PUTTING THE FUNDAMENTALS INTO PRACTICE

If your organisation has a systematic approach to ESM, you should check that it puts all the fundamentals into practice. If you do not, or if your approach does not 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 may also find the following further reading helpful:

- 1 HMRI, *Railway Safety Principles and Guidance* ('Blue Book'), ISBN 0 7176 0712 7
(Advice on designing, constructing and altering works, plant and equipment, while maintaining railway safety.)
- 2 *Investigation into the Clapham Junction Railway Accident*, Anthony Hidden QC, HMSO, ISBN 0 10 108202 9
(Analysis of weaknesses in management at the root of one of the worst recent British railway accidents.)
- 3 The Engineering Council, *Guidelines on Risk Issues*, February 1993, ISBN 0-9516611-7-5
(Practical and ethical guidance to engineers and managers on their safety responsibilities.)
- 4 Hazards Forum, *Safety-related Systems – Guidance for Engineers*, March 1995, ISBN 0 9525103 0 8
(An overview of the professional, practical and legal aspects of working on safety-related systems, particularly computer-based systems.)
- 5 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 OTHER REFERENCES

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

- 1 HSE, *Ensuring Safety on Britain's Railways*, published by the Department of Transport, 1993
- 2 HSE discussion document, *Reducing Risks, Protecting People*, 1999
- 3 IEC Standard 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC Publication 61508-1 (First edition - 1998)
- 4 CENELEC Standard ENV 50129:1998, *Railway Applications – Safety Related Electronic Systems for Signalling*

Your Suggestions	
<i>Your name and address:</i>	<i>Your phone number:</i>
<i>Your suggestions for changing the Yellow Book:</i>	
Please photocopy this sheet and send or fax your comments to:	
ESM Administrator Praxis Critical Systems Limited 20 Manvers Street Bath BA1 1PX	Phone: 01225 466991 Fax: 01225 469006
For our use	
Suggestion number:	
Status (open or closed):	
Reply sent:	