

# Appendices

# Appendix A

## Glossary

This glossary defines the specialised terms used in this volume. Volume 1 uses simpler and more restricted terminology which is introduced in the volume itself.

We have tried to minimise inconsistencies between the terminology used in this volume and that used in other principal sources of information for railway ESM. However it is not possible to eliminate inconsistency entirely because there is variation in usage between these other sources.

<b>accident</b>	An unintended event or series of events that results in harm.  <i>Note: this broadly corresponds to a 'hazardous event' in the Railtrack S&amp;SD Safety Risk Model.</i>
<b>accident likelihood</b>	The likelihood of an accident occurring. May be expressed as numeric probability or frequency or as a category.
<b>accident sequence</b>	A potential progression of events that result in an accident.
<b>Accident Sequence Analysis</b>	Derivation of the sequence of events which lead from hazard to accident.
<b>accident severity</b>	A measure of amount of harm. May be expressed as a financial value or as a category.
<b>accident trigger</b>	A condition or event which is required for a hazard to give rise to an accident.  <i>Note: this broadly corresponds to a 'precursor (consequence)' in the Railtrack S&amp;SD Safety Risk Model.</i>
<b>ALARP principle</b>	The principle that no risk in the tolerability region can be accepted unless reduced 'As Low As Reasonably Practicable'.  <i>See chapter 8.</i>
<b>apportioned risk benchmark</b>	A target for the average individual probability of fatality per annum experienced by a group, arising from a given aspect of the railway's operations

<b>authorisation</b>	The formal permission to introduce a system, product or other change into the railway within specified application constraints.
<b>barrier</b>	(In the context of risk assessment) anything which may act to prevent a hazard giving rise to an accident. Barriers may be physical, procedural or circumstantial
<b>broadly acceptable risk</b>	A risk which is generally acceptable without further reduction.
<b>causal factor</b>	Any event, state or other factor which might contribute to the occurrence of a hazard.
<b>code of practice</b>	A statement of best practice whose use is not mandated by the issuing authority.
<b>compliance</b>	A demonstration that a characteristic or property of a system, product or other change satisfies the stated requirements.
<b>consequence</b>	The results arising from the addition of energy, or exposure, to a hazard. These may range from benign results to accidents. Several consequences may be associated with a hazard.
<b>Data Recording and Corrective Action System (DRACAS)</b>	<p>A closed-loop system for ensuring that failures and other incidents are thoroughly analysed and that any necessary corrective action, particularly if it affects safety, is identified and carried through.</p> <p><i>See appendix E.</i></p>
<b>endorse</b>	Approve a document, piece of equipment, etc, as being fit for purpose.
<b>Engineering Safety Management (ESM)</b>	<p>The activities involved in making a system, product or other change safe and showing that it is safe.</p> <p><i>Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering.</i></p>
<b>Engineering Safety Management System</b>	A systematic and documented approach to ESM.
<b>error</b>	A deviation from the intended design which could result in unintended system behaviour or failure.
<b>event</b>	A significant happening that may originate in the system, product or other change or its domain.
<b>Event Tree Analysis</b>	A method of illustrating the intermediate and final outcomes which may arise after the occurrence of a selected initial event.
<b>failure</b>	A deviation from the specified performance of a system, product or other change. A failure is the consequence of a fault or error.

<b>fault</b>	A fault is a defect in a system, product or other change which may cause an error.
<b>Fault Tree Analysis</b>	A method for representing the logical combinations of various states which lead to a particular outcome (top event). <i>See appendix E.</i>
<b>FMEA</b>	Failure Mode and Effects Analysis. A process for hazard identification where all known failure modes of components or features of a system, are considered in turn and undesired outcomes are noted. <i>See appendix E.</i>
<b>FMECA</b>	Failure Mode, Effects and Criticality Analysis. An extension to FMEA in which the criticality of the effects is also assessed. <i>See appendix E.</i>
<b>group</b>	Group of people exposed to railway operations. Such as: employees (trackside staff), passengers and the public.
<b>handover</b>	Used to mean the process of handing over part of the railway to the infrastructure controller so that it can put into or back into service. <i>Note: this process is referred to as 'Handback' within Railtrack.</i>
<b>hazard</b>	A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product. <i>Note: this broadly corresponds to a 'precursor (cause)' in the Railtrack S&amp;SD Safety Risk Model</i>
<b>Hazard Analysis Report</b>	A document identifying the potential hazards and accidents of a system, product or other change and analysing the causal factors of the hazards.
<b>Hazard Log</b>	A document which records details of hazards and potential accidents identified during safety analyses of a system, product or other change and logs safety documentation produced.
<b>HAZOP</b>	Hazard and Operability Study. A study carried out by application of guide words to identify all deviations from the design intent with undesired effects for safety or operability. <i>See DEF STAN 00-58 [F.19]</i>
<b>incident</b>	Unplanned, uncontrolled event, which under different circumstances could have resulted in an accident.

<b>individual risk</b>	The individual risk experienced by a person, is their probability of fatality per unit time, usually per year, as a result of a hazard in a specified system.
<b>intolerable risk</b>	A risk which cannot be accepted and must be reduced.
<b>loss</b>	A measure of harm to people.
<b>potential equivalent fatality</b>	A convention for aggregating harm to people by regarding major and minor injuries as being equivalent to a certain fraction of a fatality.
<b>Project Manager</b>	The person in overall control of a project. Also responsible for the safety of the products produced during the project, although may delegate this role to a Project Safety Manager (but remains accountable).
<b>Project Safety Manager</b>	The person responsible for safety on a project and for producing all safety-related documentation.
<b>railway operator</b>	An infrastructure controller, train operator or station operator
<b>random hardware failure</b>	Failures resulting from one or more of the possible degradation mechanisms in the hardware. These failures occur at predictable rates but at unpredictable (that is random) times.
<b>reliability</b>	The probability that an item can perform a required function under given conditions for a given time interval.
<b>remit</b>	Terms of reference, in particular for a Safety Audit or Safety Assessment
<b>risk</b>	Combination of the likelihood of occurrence of harm and the severity of that harm.
<b>risk analysis</b>	A structured process which identifies both the likelihood and extent of adverse consequences arising from a given activity of facility.
<b>risk assessment</b>	The combination of risk analysis and risk evaluation.
<b>risk assessment report</b>	A document containing an analysis of the risks of accidents occurring.
<b>risk benchmark</b>	A target for the average individual probability of fatality per annum experienced by a group, for all the railway's operations
<b>risk classification</b>	A scheme to classify risk according to likelihood of harm occurring and the severity of the harm.
<b>risk evaluation</b>	The appraisal of the significance of a given quantitative (or, where applicable, qualitative) measure of risk.

<b>safety</b>	Freedom from unacceptable risk. <i>Criteria for accepting risk are described in chapter 8.</i>
<b>safety analysis</b>	A general term encompassing identifying hazards, analysing hazards and assessing risk.
<b>safety approval</b>	The process by which a Safety Authority grants its approval for a proposed change to the railway to proceed.
<b>Safety Assessment</b>	The process of analysis to determine whether a system, product or other change to the railway has met its Safety Requirements and that the Safety Requirements are adequate.
<b>Safety Assessment Remit</b>	A form capturing a request for a Safety Assessment and the terms of reference.
<b>Safety Assessment Report</b>	A report on the activity carried out to check that the Safety Requirements are being met on a project.
<b>Safety Assessor</b>	The person who carries out Safety Assessments.
<b>Safety Audit</b>	An activity to check and ensure that a project is being run according to its Safety Plan. It will also address the adequacy of the Safety Plan.
<b>Safety Audit Remit</b>	A form capturing a request for a Safety Audit and the terms of reference.
<b>Safety Audit Report</b>	A report on the activity carried out to check that the Safety Plan and safety management procedures are being carried out on a project.
<b>Safety Auditor</b>	The person appointed to carry out Safety Audits on a project.
<b>Safety Authority</b>	The body responsible for certifying that the safety-related system, product or other change is safe, fit for service and complies with all statutory and regulatory requirements.
<b>Safety Case</b>	A formal presentation of evidence, arguments and assumptions aimed at providing assurance that a system, product or other change to the railway has met its Safety Requirements and that the Safety Requirements are adequate. <i>Early issues may present analysis and assessment information, plans and requirements.</i>
<b>Safety Certificate</b>	A certificate authorising system, product or other change for use. Usually refers to third-party equipment.
<b>safety control</b>	A quality control with the potential to reveal hazardous faults.
<b>Safety Engineering</b>	The application of technical methods to ensure achievement of the Safety Requirements.

<b>Safety Integrity</b>	The likelihood of a system, product or other change satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.
<b>Safety Integrity Level (SIL)</b>	Discrete level (1 out of a possible 5) for specifying the safety integrity requirements of the safety functions to be allocated to a system, product or component, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 0 is reserved for functions which are not relied upon at all to control risk.
<b>safety lifecycle</b>	The additional series of ESM activities carried out in conjunction with the system lifecycle for safety-related systems.
<b>Safety Plan</b>	A document detailing the activities to be carried out, and responsibilities of people to ensure the safety of work being carried out.
<b>Safety Planning</b>	An activity to define the activities to be carried out and the staff responsibilities to be assigned to ensure the safety of work to be carried out. Results in the preparation of a Safety Plan.
<b>Safety Records Log</b>	A reference to every safety document produced and used by a project.
<b>safety-related</b>	An item is safety-related if any of its features or capabilities have the potential to contribute to or prevent an accident.
<b>Safety Requirements Specification</b>	Specification of the requirements that a product, system or change to the railway must satisfy in order to be judged safe.
<b>safety standard</b>	A document which establishes criteria or requirements by which the safety of products or processes may be assessed objectively.
<b>safety value</b>	The monetary value of reductions in safety losses likely to be achieved by implementation of a risk mitigation option.
<b>severity</b>	<i>See accident severity</i>
<b>standard</b>	An authorised document, including specification, procedure, instruction, directive, rule or regulation, which sets mandatory requirements for use in service.
<b>system supplier</b>	Any organisation supplying systems or products to be used on the railway.
<b>systematic failure</b>	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

---

<b>tolerability region</b>	A region of risk which is neither high enough to be unacceptable nor low enough to be broadly acceptable. Risks in this region must be reduced ALARP (see ALARP principle)
<b>upper limit of tolerability</b>	A measure of the average individual risk of fatality per annum, defined for each group, and representing the boundary between tolerable and intolerable risk for the group.
<b>Value of Preventing a Fatality (VPF)</b>	A defined monetary figure which is used to indicate what it is regarded as reasonably practicable to spend in the expectation of preventing a single fatality.

This page left intentionally blank

# Appendix B

## Document Outlines

This appendix provides suggested document outlines for the following ESM documents:

- 1 Safety Plan (see chapter 12)
- 2 Hazard Log (see chapter 13)
- 3 Safety Assessment and Audit Remits (see chapter 14)
- 4 Safety Assessment and Audit Reports (see chapter 14)

The outlines do not show administrative document sections such as change history, terminology and referenced documents sections which should be added according to your own document standards.

## B.1 Outline Safety Plan

The scope and coverage of this outline is designed to be consistent with the CENELEC standard prEN 50126 [F.8]. This is one of a group of European standards for safety within the rail industry. prEN 50126 defines a process for the management of Reliability, Availability, Maintainability, and Safety (RAMS). The letters in square brackets refer to the CENELEC requirement detailed in clause 6.2.3.4 of prEN 50126.

The recommended structure for the Safety Plan is as follows:

<b>Introduction</b>	<b>Aims and objectives</b>
	(describe the aims and objectives of this Safety Plan for readers unfamiliar with ESM or this project)
	<b>Scope [b]</b>
	(include the lifecycle phases this Safety Plan addresses)
	<b>Structure</b>
	(describe the structure of the plan)
	<b>Background and requirements</b>
	<b>Summary of system [c, m]</b>
	(include, or refer to, a description of the system, including interfaces to other related programmes)
	<b>Outline of project [a]</b>
(a brief description of the conduct of the project, to include a statement of compliance with the organisation's safety policy, or a justification of an alternative approach)	
<b>Safety requirements [f]</b>	
(a summary of the safety requirements or a reference to them and a description of the process by which the safety requirements were established and maintained; where none are available the Safety Plan should indicate how and when the Safety Requirements are to be determined)	
<b>Risk assessment criteria [f]</b>	
(a brief description of the criteria used to derive risk tolerability targets for the system)	
<b>Assumptions and constraints [n]</b>	
(list any assumptions or constraints on the system or the project)	

*(cont.)*

**Safety management activities****Safety roles and responsibilities [d, f]**

(indicate and justify competence and independence of appointments)

- Project Manager;
- Project Safety Manager;
- Safety Assessor;
- Safety Auditor;
- Safety Authorities.

**Safety lifecycle [e]**

(describe and relate the project and safety lifecycles)

**Safety analysis [f]**

(describe and justify the approach, see chapter 8)

**Safety deliverables [g]**

(justify exclusion of key deliverables)

**Safety standards**

(justify use of Safety Standards on project)

**Safety assessments [f, p]**

(justify frequency of assessments)

**Safety audits [f, p]**

(justify frequency of audits)

**Safety case and certification [h, i]**

(describe certification requirements additional to those of ESM)

**Contractor management [o]**

(refer to contractor-produced plans and other documentation where appropriate)

**Configuration management**

(refer to technical and quality planning documentation where appropriate)

**Safety training**

(including contractors where appropriate)

**System operation, modification and maintenance [j, k]**

(briefly describe, or refer to, process and approval mechanisms for analysing operation, system modification, and performing system maintenance)

*(cont.)*

<b>Safety controls</b> [p]	(define controls, for instance formal review, approvers and standards for safety deliverables, including: <ul style="list-style-type: none"><li>• Hazard Log</li><li>• Hazard Analysis</li><li>• Risk Assessment</li><li>• Safety Req Spec</li><li>• Safety Case</li></ul>
<b>Safety docn.</b> [f, l]	(describe production, approval and maintenance of each document; justify any not produced) <ul style="list-style-type: none"><li>• Preliminary Hazard Analysis</li><li>• Risk assessment report</li><li>• Hazard Log</li><li>• Safety Requirements Specification</li><li>• Safety Audit and Safety Assessment Reports</li><li>• Safety Case</li><li>• Design and Test Specifications</li><li>• Review reports</li><li>• Testing and Acceptance records</li><li>• Training records</li></ul>
<b>Safety engineering</b> [f]	(indicate activities to meet and validate Safety Requirements for each phase of the lifecycle)
<b>Validation and verification of external items</b> [f]	(justify a decision to not validate and verify any external items)

## B.2 Outline Hazard Log

The scope and coverage of this outline is designed to be consistent with the CENELEC standard prEN 50126 [F.8]. The Hazard Log contains the following sections:

The recommended structure for the Hazard Log is as follows:

**Introduction** This section will describe the purpose of the Hazard Log and indicate the environment and safety requirements to which the system safety characteristics relate.

The following should be included:

- The aim, purpose and structure of the Hazard Log in sufficient detail to enable understanding by all project personnel;
- A unique identifier of the system to which the Hazard Log relates and a reference to a description and the scope of the system;
- A reference to the Safety Plan (in early stages of the project this will have to be omitted);
- A reference to the system Safety Requirements Specification or, if this has yet to be written, the safety analysis documentation;
- The process for managing the Hazard Log, such as who may modify it and the approval process for each new entry.

**Journal** The Journal should describe all amendments to the Hazard Log in order to provide a historical record of its compilation and provide traceability. It should record, for each amendment:

- The date of the amendment (not necessary if a diary format is used);
- A unique entry number;
- The person making the amendment;
- A description of the amendment and the rationale for it; and
- The sections in the Hazard Log that were changed.

If the Hazard Log is stored in a database then it may be possible to use the intrinsic change recording facilities to maintain a Journal semi-automatically.

*(cont.)*

**Directory**

The Directory, sometimes known as the Safety Records Log, should give an up-to-date reference to every safety document produced and used by the Project. The documents referred to should include (but not be limited to) the following, where they exist:

- Safety Plan;
- Safety Requirements Specification;
- Safety standards;
- Safety Documents;
- Incident/accident reports;
- Analyses, assessment and audit reports;
- Safety Case;
- Correspondence with the relevant Safety Authorities.

For each document the Directory should include the following:

- A unique reference;
- The document title;
- The current version number and issue date;
- The physical location of the master.

*It may be convenient to keep the Directory separate from the rest of the Hazard Log, or event to integrate it with a project document management system.*

*(cont.)*

**Hazard data** This section should record every identified hazard.

For each hazard, the information listed below should be recorded, as soon as it becomes available. Data collected during Hazard Analysis and Risk Assessment should be transcribed to the Hazard Log when the reports have been endorsed.

- a unique reference;
- a brief description of the hazard which should include the system functions or components affected and their states that represent the hazard;
- the causes identified for the hazard;
- a reference to the full description and analysis of the hazard;
- assumptions on which the analysis is based and limitations of the analysis;
- the severity for the related accident, the likelihood of the hazard occurring and the likelihood of an accident occurring with the hazard as a contributing factor;
- the predicted risk associated with the hazard;
- target likelihood for its occurrence;
- the status of the hazard; Typically one of the following:
  - Open (action to close the hazard has not been agreed);
  - Cancelled (the event has been determined not to be a hazard or to be wholly contained within another hazard);
  - Resolved (action to close the hazard has been agreed but not completed);
  - Closed (action to close the hazard has been completed);
- if the hazard is not closed or cancelled then the name of a person or company who is responsible for progressing it towards closure;
- a description of, or a reference to, the action to be taken to remove the hazard or reduce the risk from the system to an acceptable level; This should include:
  - a statement as to whether the hazard has been avoided or requires further action (with a justification if no further action is to be taken);
  - details of the risk reduction action to be taken;
  - a discussion of the alternative means of risk reduction and justification for actions considered but not taken;
  - a comment on the need for accident sequence re-evaluation following risk reduction actions;
  - a reference to any design documentation that would change as a result of the action;
  - a reference to all Safety Requirements associated with this hazard.

*(cont.)*

**Incident data** This section should be used to record all incidents that have occurred during the life of the system or equipment. It should identify the sequence of events linking each accident and the hazards that caused it. For each incident the following should be provided:

- a unique reference;
- a brief description of the incident;
- a reference to a report describing an investigation of the incident;
- a description of any action taken to prevent recurrence or justification of the decision not to take any.

**Accident data** This section should be used to record every identified possible accident. It should identify possible sequences of events linking identified accident with the hazards that may cause it. For each accident the following should be provided:

- a unique reference;
- a brief description of the potential accident;
- a reference to a report giving a full description and analysis of the accident sequence;
- a categorisation of the accident severity and the highest tolerable probability of the accident (the accident probability target);
- a list of the hazards and associated accident sequences that could cause the accident.

### B.3 Outline Safety Audit and Assessment remits

The following structure is recommended for either an audit or an assessment remit.

<b>Safety Auditor/Assessor</b>	The name of the auditor/assessor.
<b>Independence</b>	Requirements for auditor/assessor independence.
<b>Qualifications and Experience</b>	Requirements for auditor/assessor qualifications and experience.
<b>Requirements</b>	Requirements for the audit/assessment itself, including <ul style="list-style-type: none"><li>• the scope of the audit/assessment);</li><li>• the purpose of the audit/assessment);</li><li>• the documents that the project will be audited against, and the prevailing legal framework for accepting risk;</li><li>• any previous assessments or audits which should be taken into account.</li></ul>
<b>Other Information</b>	As required.
<b>Report to be issued by</b>	Target date.
<b>Commissioned by:</b>	Name of person commissioning the audit/assessment.

## B.4 Outline Safety Audit and Assessment reports

### B.4.1 Outline Safety Audit report

The following structure is recommended for an audit report.

<b>Summary</b>	Management summary of rest of document.
<b>Requirements</b>	This section should state the audit requirements and identify any areas where the audit deviated from it.
<b>Audit details</b>	This section should provide details of the conduct of the Safety Audit, such as who was interviewed and what was examined.
<b>Findings</b>	<p>This section should list each finding and should discuss its impact. Evidence to support each finding should be given.</p> <p>Chapter 14 contains a suggested classification for findings.</p>
<b>Conclusions and recommendations</b>	<p>This section should include a judgement on the extent of the Project's compliance with the Safety Plan and a statement about the adequacy of the Safety Requirements. The degree of compliance may be graded as:</p> <ul style="list-style-type: none"><li>• Unqualified compliance with the Safety Plan;</li><li>• Compliance qualified by the need for implementation of minor recommendations that are based on each non-compliance of minor impact;</li><li>• Non-compliance requiring implementation of major recommendations that are based on each non-compliance of major impact, followed by a subsequent Safety Audit.</li></ul>

This section may also provide a prioritised list of recommended actions for improvement to be carried out to resolve findings. The recommended actions should state who should do what, and by when. The recommendations may also include general suggestions for improvement beyond that required for compliance.

The completed audit checklist should be included as an appendix to the report.

The audit report should provide evidence to justify the Safety Auditor's findings and conclusions. The report should be dated and signed by the Safety Auditor.

### B.4.2 Outline Safety Assessment report

The following structure is recommended for an assessment report.

<b>Summary</b>	Management summary of rest of document.
<b>Requirements</b>	This section should state the assessment requirements and identify any areas where the assessment deviated from it.
<b>Assessment Details</b>	This section should provide details of the conduct of the Safety Assessment, such as who was interviewed and what was examined.
<b>Findings</b>	This section should list each finding and should discuss its impact. Evidence to support each finding should be given.  Chapter 14 contains a suggested classification for findings.
<b>Conclusions and recommendations</b>	This section should state the Safety Assessor's opinion as to the degree of compliance of the system or equipment with its Safety Requirements, in one of the following four forms: <ul style="list-style-type: none"> <li>a) The Safety Assessor concludes that the system meets its safety requirements.</li> <li>b) The Safety Assessor concludes that the system will meet its safety requirements provided that specified recommendations are carried out and without a further assessment.</li> <li>c) The Safety Assessor cannot be sure that the system will meet its safety requirements.</li> <li>d) The Safety Assessor concludes that the system does not meet its safety requirements.</li> </ul>

The Safety Assessor should state the reasons for the conclusions. The assessor should quantify the discrepancy between the safety requirements and the assurance achieved. A further assessment should be required before safety approval.

This section may also contain a numbered, prioritised list of proposed actions that should be carried out to resolve findings.

The assessment should give a professional judgement on the acceptability of the risk associated with the system or equipment.

The critical and most sensitive arguments of the document should be clearly and concisely highlighted and a professional opinion should be given as to the robustness of the argument. Where the argument is contained in whole or part within other documents or is part of existing custom and practice this should be clearly identified. A professional opinion should also be given, with regard to the railway system as a whole, as to the practicality of any measures used to mitigate against the hazards raised.

The assessment should identify any non-compliances with respect to the relevant standards and legal requirements.

This page left intentionally blank

# Appendix C

## Checklists

This appendix provides checklists to support the following activities:

- 1 Hazard Identification and Risk Assessment (see chapter 8)
- 2 Safety Planning (see chapter 12)
- 3 Updating the Hazard Log (see chapter 13)

## C.1 Hazard identification and risk assessment

### C.1.1 Hazard identification checklists

Example checklists are supplied below which may be used if there are no existing, well-established checklists. They may be applied to the whole system or to a component of it. Each item should be interpreted as widely as circumstances permit in the endeavour to unearth possible hazards. No checklist can be exhaustive and the analyst should bring his or her full experience to bear in searching for hazards.

The **Functional Checklist** should be applied to a functional specification of the item being considered in an attempt to unearth hazards arising from unspecified functionality or specified functionality in unforeseen circumstances:

- a) Alarms and warnings,
- b) Indication of failure,
- c) Interlocks,
- d) Maintenance and support,
- e) Point setting,
- f) Signal aspects,
- g) Terrorist action,
- h) Software malfunction,
- i) Software crash.

The **Mechanical Checklist** should be applied to mechanical drawings to unearth hazards involving physical interactions:

- a) Corrosion,
- b) Cryogenic fluids,
- c) Derailment,
- d) Exhaust gases,
- e) Fire,
- f) Foreign bodies and dust,
- g) Insect, rodent or mould damage,
- h) Lasers,
- i) Overheating,
- j) Pressure systems,
- k) Shock and vibration,
- l) Vandalism,
- m) Ventilation.

The **Construction Checklist** should be applied to civil engineering drawings and plans to unearth construction hazards:

- a) Access hazards at site,
- b) Site preparation hazards,
- c) Construction hazards,
- d) Environmental effects,
- e) Vandalism,
- f) Interference with normal railway operating procedures,
- g) Training and control of contractors.

The **Electrical Checklist** should be applied to circuit diagrams to unearth hazards involving electrical interactions:

- a) Electromagnetic interference and compatibility,
- b) Fire and explosion initiation,
- c) Insulation failure,
- d) Lightning strikes,
- e) Loss of power,
- f) Traction current,
- g) Protection against earth faults,
- h) Indirect and direct contact,
- i) Emergency switching and isolation,
- j) Overcurrent protection and effects of disconnection,
- k) Current rating.

The **Operation and Support Checklist** should be applied to operating and maintenance instructions to unearth hazards occurring during or triggered by operating and maintenance activities:

- a) Accessibility for maintenance,
- b) Documentation,
- c) Failure to activate on demand,
- d) Human factors,
- e) Inadvertent activation,
- f) Lighting,
- g) Manuals,
- h) Spares,
- i) Training,
- j) Start-up,
- k) Closedown,
- l) Re-setting.

The **Occupational Health Checklists** should be applied to a general description to unearth hazards to personnel installing, operating, maintaining or disposing of the item:

- a) Asbestos,
- b) Asphyxiates,
- c) CFCs,
- d) Corrosive materials,
- e) Cryogenic fluids,
- f) Electrocutation,
- g) Exhaust gases,
- h) Fire,
- i) High temperatures,
- j) Injury from moving parts,
- k) Lasers,
- l) Noise,
- m) Pressure systems,
- n) Radioactive materials,
- o) Toxicity,
- p) Electrical overheating.

### C.1.2 Operation and maintenance responsibilities checklist

This checklist may be used to assist in thorough control of risks related to operation and maintenance.

Actions to be taken by the Project Manager:

- a) Define responsibilities for operation and support in project requirements;
- b) Establish communications on operation and support with users.

Operating Information and Documentation checklist:

- c) Provide operating instructions prior to commissioning, emphasising safety aspects and precautions as appropriate;
- d) Consider need to alter current operating instructions and advise Users accordingly;
- e) Include instructions to be followed in event of system or equipment failure;
- f) Include instructions to be followed to render system safe and to maintain operational capabilities where possible;
- g) Include instructions to be followed in the event of an accident resulting from a system or equipment failure;
- h) Define requirements for review and exercising of the safety aspects of operating instructions.

Operator interface design checklist:

- i) Consider safety aspects of man-machine interface in system or equipment;
- j) Check that required operating tasks are within intended operators' physical and mental capabilities;
- k) Ensure that implications of emergency actions are clearly defined in operating instructions.

Operational safety features checklist:

- l) Check that operator safeguards have been considered;
- m) Check clarity of instructions for operator safety systems;
- n) Consider requirements for periodical safety checks, by operating and maintenance personnel.

Operational Record checklist:

- o) Determine requirements for failure reporting;
- p) Issue instructions for the recording and analysis of failures;
- q) Define procedures for the incorporation of alterations to systems and equipment for safety reasons.

Operator Training and Competence checklist:

- r) Determine requirements for operator safety training;
- s) Consider need for training aids and facilities;
- t) Define skill levels and calibre of operators and maintainers.

#### Maintenance Instructions checklist

- u) Provide maintenance specifications and identify safety-related requirements;
- v) Define fault-diagnosis, condition monitoring and test equipment;
- w) Provide maintenance task instructions;
- x) Define skill levels required;
- y) Provide maintenance schedules;
- z) Provide a maintenance recording system;
- aa) Provide a defect reporting system;
- bb) Provide a system for the incorporation of changes to a design.

#### System Definition and Spares Identification checklist

- cc) Create a database of system and equipment support information;
- dd) Identify safety aspects of spares and support equipment;
- ee) Define safety requirements for packaging, handling, storage and transport of spares.

#### Maintenance Specifications and Mandatory Items checklist

- ff) Identify mandatory preventive maintenance;
- gg) Define data reporting, analysis and corrective action system;
- hh) Designate team of specialists for monitoring data reports.

#### Safe Maintenance Practices and Accessibility checklist

- ii) Provide instructions for gaining safe access to systems for repairs;
- jj) Provide instructions for the promulgation of safety precautions;
- kk) Provide instructions for a 'permit-to-work' procedure.

#### Change Control checklist

- ll) Establish procedures for the safe management of changes and alterations to systems;
- mm) Define requirements for testing and commissioning after changes have been incorporated.

#### Checklist of Regulations on Safety in Operation and Support

- nn) HSE Guidance Note GS27. Protection against electric shock;
- oo) IEC publication 479. Effects of current passing through the human body (1984 or later edition);
- pp) IEC Guide 105. Principles concerning the safety of equipment electrically connected to a telecommunications network;
- qq) IEE Wiring Regulations (15th edition);
- rr) Control of Substances Hazardous to Health Regulations 1988.

### C.1.3 Checklist of decommissioning/disposal considerations

This checklist may be used to assist in thorough control of risks related to decommissioning and disposal.

Checklist of actions to be completed

- a) Has the hazard listing identified possible hazards in decommissioning, dismantling and disposal?
- b) Has the hazard analysis classified the severity or consequences of any potential accidents in decommissioning or disposing of a system or equipment at the end of its life?
- c) Has the system been designed to eliminate potential hazards of disposal?
- d) Has guidance for the safe disposal of systems and equipment been included in the Hazard Log and the Safety Case?
- e) Does the Safety Plan cover the decommissioning of systems and equipment?
- f) Is there any risk due to interaction between a decommissioned system and any remaining systems?
- g) If any parts of systems have been designated for salvage on decommissioning, have instructions for re-certification been prepared?
- h) Are all decommissioning and disposal procedures defined along with any special testing requirements they imply?

Checklist of hazardous components (*not exhaustive*)

- i) Flammable substances,
- j) Explosives,
- k) Asphyxiates, toxic, corrosive or penetrating substances,
- l) Allergenic substances,
- m) Pressurised systems,
- n) Electrical sources or batteries,
- o) Radiation sources,
- p) Rotational machinery, moving parts,
- q) Hazardous surfaces,
- r) Cutting edges and sharp projections,
- s) Heavy weights.

#### C.1.4 Checklists of installation and handover considerations

This checklist is intended to be used to check whether or not all required safety management activities have taken place prior to safety approval.

- a) Have any incidents with safety implications been reported during the site trial?
- b) Has the Safety Case been updated to reflect the validation activities?
- c) Has the Safety Case been reviewed by the Safety Assessor and issued for approval?
- d) Have these incidents involved changes to the information on which the Safety Case was based (thereby requiring a reworking of the Safety Case)?
- e) Have all changes to the Safety Case been approved by the Safety Authority?
- f) Has all operational support documentation with safety connotations been reviewed during this phase?
- g) Have these reviews caused changes to the information on which the Safety Case was based (thereby requiring a reworking of the Safety Case)?
- h) Has all safety-related documentation necessary for the use of the operational support team been handed over?
- i) Has all training documentation in safety aspects been reviewed and approved?
- j) Have all Procedures, Work Instructions and method statements required been defined and approved, including any variations to existing standards?
- k) Have all required as-built diagrams, drawings, photographs and other documentation been supplied?
- l) Has all required training for the operational team been carried out?
- m) Has a formal channel of communication been established between the operational support team and the development team to ensure that data about operational safety is fed back into the future developments?

## C.2 Safety planning

These checklists have been produced to assist the creation and evaluation of the ESM Activities section of the Safety Plan. They provide guidance on safety planning for safety activities throughout the system lifecycle.

The Safety Plan should define responsibilities and time-scales for each ESM activity scheduled.

### C.2.1 General considerations

The safety-related activities listed below should be considered throughout the lifecycle.

- a) Maintain Hazard Log;
- b) Revisit Safety Plan and update and re-issue where appropriate;
- c) Revisit Safety Analysis work and re-issue all affected documentation as appropriate;
- d) Establish criteria for risk tolerability;
- e) Carry-out Safety Audits and Safety Assessments as scheduled in the Safety Plan.

### C.2.2 Concept and feasibility

- a) Preliminary Hazard Analysis scheduled;
- b) Analysis of safety implications of each proposed technical approach scheduled;
- c) Production of report on this analysis scheduled;
- d) Guidance provided on safety analysis (chapter 8) considered.

### C.2.3 Requirements definition

- a) Guidance provided on establishing Safety Requirements (chapter 9) considered;
- b) Production of acceptance test plan scheduled.

### C.2.4 Design

- a) Design techniques and procedures specified;
- b) Standards for the production of design documentation specified;
- c) Allocation of safety requirements to top-level sub-systems scheduled;
- d) Allocation of random and systematic elements of the hazard probability targets to high-level sub-systems scheduled;
- e) Diagrammatic method of allocation referred to in item d) above described;
- f) Guidance provided on Risk Assessment (chapter 8) considered;
- g) Re-use of sub-systems and/or components clearly identified and justified;
- h) Plans for the review and testing of built components and documentation scheduled;
- i) System integration plan production scheduled;
- j) Occupational Health and Safety issues, related to operation and maintenance, considered;
- k) Production of validation and verification plan scheduled;
- l) Independent formal reviews of design and its associated design documentation against safety requirements scheduled.

### C.2.5 Implementation

- a) Implementation techniques specified;
- b) Procedures, standards and working practices specified;
- c) Automatic testing tools and integrated development tools specified;
- d) Occupational Health and Safety issues, related to operation and maintenance, considered;
- e) Review of validation and verification plan scheduled;
- f) Implementation of reviewed verification plan scheduled.

### C.2.6 Installation and handover

- a) Strategy for installation and handover defined;
- b) States for start-up, steady-state (normal operation), shut-down, maintenance and abnormal operation addressed;
- c) Required approvals of acceptance plan specified (should include client);
- d) Requirement for client attendance at acceptance testing specified;
- e) Independence of acceptance testing team defined;
- f) Requirements for acceptance testing documentation defined;
- g) Means of safe and controlled integration of the system with existing systems and procedures defined;
- h) Start-up of the system addressed;
- i) Parallel operation of the replacement system and the existing system addressed;
- j) Sub-system versus full system switch-overs addressed;
- k) Cross validation of results between existing and replacement systems addressed;
- l) Fallback to the existing system if the replacement system fails addressed;
- m) Safety training required for operators, users, maintainers and managers of the system identified;
- n) Means of ensuring system integrity following installation defined;
- o) Inspections and Safety Assessments scheduled where appropriate;
- p) Guidance provided on transfer of safety responsibility (chapter 3) considered;
- q) All documentation or manuals that provide operational or maintenance support to ensure safe operation of the system identified;
- r) Occupational Health and Safety issues, related to operation and maintenance, considered;
- s) Approval authorities for support material identified;
- t) Reviews of support material scheduled.

### C.2.7 Operations and maintenance

- a) Maintenance plan included or referred to;
- b) Plan agreed by Project Manager and Operations Manager;
- c) Testing and auditing of the system scheduled;
- d) Routine actions which need to be carried out to maintain the 'as designed' functional safety of the system or equipment identified;
- e) Actions and constraints required during start-up, normal operation, foreseeable disturbances, faults or failures, and shutdown to ensure safety identified;
- f) Records which need to be maintained showing results of maintenance, audits, tests and inspections identified;
- g) Records which need to be maintained on hazardous incidents (or incidents with the potential to create hazards), system failure and availability rates identified;
- h) Actions to be taken in the event of hazards, incidents or accidents occurring identified;
- i) Comparisons of system performance with design assumptions scheduled;
- j) Procedure for assessing deviations for safety implications and for proposing modifications defined;
- k) Procedures for modifying the system in-service defined;
- l) System performance below tolerable risk addressed;
- m) Identification of systematic faults addressed;
- n) New or amended safety legislation identified and taken into account;
- o) Modifications to the safety requirements addressed;
- p) Need for analysis of the effect of a proposed modification on system safety addressed;
- q) Approval of modification implementation plan defined;
- r) Need for maintenance of documentation effected by modifications highlighted;
- s) Inspection, testing and/or analysis of modifications addressed;
- t) Occupational Health and Safety issues, related to operation and maintenance, considered;
- u) Criteria for withdrawal of the system from service identified.

### C.2.8 Decommissioning and disposal

- a) Safety-related considerations for decommissioning the system or equipment identified;
- b) How the system or equipment is to be removed, including the safe disposal of any hazardous material addressed;
- c) The phasing in of any replacement system or equipment addressed;
- d) Any gaps in the level of service provided by removing the system or equipment addressed.

### **C.3 Updating the Hazard Log**

These checklists have been produced to assist the use and evaluation of the Hazard Log.

#### **C.3.1 How to enter new hazard data**

In the Hazard Data section

- a) New reference created;
- b) Hazard briefly described;
- c) Reference to full description and analysis provided;
- d) Assumptions recorded;
- e) Severity category of related accident recorded;
- f) Likelihood of hazard and related accident recorded;
- g) Random probability of hazard recorded;
- h) Target likelihood recorded;
- i) 'Open' hazard status recorded;
- j) Name of person or company responsible recorded;
- k) Actions for risk reduction recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'New hazard identified';
- e) New hazard referenced.

#### **C.3.2 How to modify existing hazard data**

In the Hazard Data section

- a) Hazard reference identified;
- b) New hazard data recorded;
- c) Latest hazard status recorded;
- d) Any actions for further risk reduction recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'Modification to hazard data';
- e) Affected sections referenced.

**C.3.3 How to enter new incident/accident data**

In the Incident/Accident Data section

- a) New reference created;
- b) Incident/accident briefly described;
- c) Reference to full description and analysis provided;
- d) Incident/accident severity category recorded;
- e) Incident/accident probability target recorded;
- f) Causes of incident/accident recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'New Incident' or 'New Accident';
- e) New hazard referenced.

**C.3.4 How to modify existing incident/accident data**

In the Incident/Accident Data section

- a) Incident/accident reference identified;
- b) New incident/accident data recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'Modification to accident/incident data';
- e) Modified accident/incident referenced.

**C.3.5 How to enter directory data**

In the Directory

- a) New reference created;
- b) Document title recorded;
- c) Current version number and issue date recorded;
- d) Physical location of document recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'New document';
- e) New document referenced.

**C.3.6 How to modify existing directory data**

In the relevant section

- a) Document reference identified;
- b) New document data recorded.

In the Journal section

- a) Date recorded;
- b) New journal entry number created;
- c) Name of person entered;
- d) Journal entry described as 'Modification to document entry';
- e) Modified document entry referenced.

# Appendix D

## Examples

This appendix provides examples of the following:

- 1 Safety policies (see chapter 3)
- 2 Hazard ranking matrix (see chapter 8)
- 3 Risk assessment (see chapter 8)
- 4 Safety Assessment remit (see chapter 14)
- 5 Safety Audit checklist (see chapter 14)
- 6 Safety Assessment checklist (see chapter 14)

## D.1 Example safety policies

This section contains extracts from the safety policies of three different rail companies:

- Railtrack plc, the infrastructure controller for the UK mainline railway,
- Virgin Trains, a UK mainline train operator,
- WS Atkins Rail Limited, a UK rail engineering and consultancy firm.

The organisations concerned have given permission for their safety policies to be included in the Yellow Book as a public demonstration of their commitment to safety. They are provided in the hope that they may prove useful to other organisations wishing to formulate safety policies. Please bear in mind that these policy statements are subject to revision. You should contact the organisations concerned directly if you wish to make sure that you have an up-to-date statement.

### D.1.1 Railtrack plc

*Railtrack plc have issued the following Safety Policy Statement.*

Railtrack PLC has prime responsibility for the safety and security of the railway it controls and for the health and safety of those who may be affected by the company's activities. As the Infrastructure Controller, our responsibility extends to ensuring safety within the entire Railway Group, through our own efforts and through the co-operation and compliance of our suppliers and the train and station operating companies that use our system. We seek and welcome recommendations for continuous improvement from both our staff and from theirs.

We view safety in the widest context - for us, it means protection from the risk of death, injury and poor health arising from our activities. It also means the avoidance of damage to property and the environment from whatever cause - accident, fire, explosion or loss of security. We will adopt a robust and cost-effective loss control policy in all that we do, recognising that good safety performance is good business - for us and our customers.

We accept that our responsibility extends to all who are involved in any way in our industry - our travellers, our workforce and those contracted to work for us, or on our property, the general public when on our property, and our neighbours.

Our commitment to a safe railway comprises:

- Improving safety through the setting of goals and targets and adherence to defined standards of excellence for all those involved in the provision of rail transport.
- The development of access and contract agreements designed to maintain a safe railway for all.
- Robust monitoring and investigation systems to enable us thoroughly to evaluate and manage risk.
- The maintenance of effective communication and systems to manage the interfaces between parties.
- A continuing policy of safety awareness for those working for our railway and all who use it.
- An intolerance of failures to establish safe methods of work or to comply with legislation, formal procedures and commitments.

Safety is fundamental to all contract and trading agreements between all parties whose activities impact on the railway. Evidence of professional safety management practice is, and will remain, a condition of access to our railway.

We will, through our operationally independent Safety and Standards Directorate, provide strategic leadership to secure the continuous improvement in safety performance necessary to deliver the ten year vision contained within the Railway Group Safety Plan.

I, as your Chairman, and the Railtrack Board, commit ourselves to uphold these principles in the efficient and effective conduct of our business and will provide adequate resources for this purpose.

Our approach to safety is dynamic and we will revise this policy to take account of any and all improvements to safety. Our policy will be reviewed at least annually.

SIR PHILIP BECK Chairman, Railtrack PLC  
August 1999

### D.1.2 Virgin Trains

*Virgin Trains issue a Health and Safety Policy as a small booklet. The policy starts with the following Chief Executive's Statement.*

#### **Nothing is more important than Safety**

Safety is the responsibility of all of us, all of the time and in everything we do. Whatever our job we each have a constant duty to ensure that there is no harm to our customers, colleagues, contractors, the general public or the environment.

Working safely is a condition of our employment and anyone who aborts work on the grounds of Health and Safety will be given my full support and that of my managers.

#### **I am committed to:-**

Continuous improvement in the Health, Safety & Welfare of all our people and all those affected by our operations, including customers, contractors and visitors.

Co-operating fully with Railtrack, other operators, and rail industry suppliers to ensure that risks to our customers, colleagues, contractors, the general public, and risks to our operations and assets, are identified and eliminated or controlled.

Setting safety performance objectives and implementing improvement actions, which will be published in our annual Safety Improvement Plan, and reviewed by Safety Council.

Ensuring adequate resources and funding are prioritised to meet our Safety commitments.

I need and acknowledge your help in eliminating hazards, which may result in personal injury, illness, fire and damage to property, harm to the environment or loss due to breaches in security.

Chris Green  
VIRGIN TRAINS     June 1999

**D.1.3 WS Atkins Rail Limited**

*WS Atkins Rail Limited have issued the following Safety Policy Statement.*

WS Atkins Rail is committed to implementing policies for health, safety, security and welfare and encouraging positive attitudes and behaviour. Through the WS Atkins Rail Limited Safety Policy we seek continuous improvement, compliance with legislation and standards, giving proper regard to protection of people, premises, property, processes and the environment.

All WS Atkins Rail Limited staff have a responsibility to ensure the safety of clients, colleagues, contractors and the general public. As Chairman I accept the ultimate responsibility for the safety of the organisation and I shall seek to promote a climate in which we are aware of risks and proper safeguards are taken, in line with the WS Atkins corporate Health and Safety Policy.

Suggestions from the staff on how safety arrangements can be improved and unsafe acts prevented will always be welcomed and actively encouraged within WS Atkins Rail Limited.

As head of WS Atkins Rail Limited, my Directors and I are totally committed to the implementation of these policies by personal involvement.

Safety is everyone's responsibility and a condition of our employment. We look for the support and professionalism of our employees at all levels at making this policy truly effective not only for their personal Health and Safety, but also for others whom their acts or omissions could affect.

J Doyle  
Chairman

**D.2 Example hazard ranking matrix**

The following matrix may be used in the initial ranking of hazards. The higher the rating, the more priority should be assigned to the hazard.

		Severity of Potential Harm/Loss				
		5	4	3	2	1
Safety Harm		Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly		25	20	15	10	5
4= Monthly to yearly		20	16	12	8	4
3=1 to 10 yearly		15	12	9	6	3
2=10 to 100 years		10	8	6	4	2
1= Less than 100 yearly		5	4	3	2	1

Table D-1 - Example hazard ranking matrix

## D.3 Risk assessment

### D.3.1 Introduction

The example presented in this appendix is provided to illustrate application of the risk assessment framework detailed in this document. The example does not necessarily relate to actual operational circumstances and **the data used within the example is provided for the purposes of illustration only**. In order to simplify the example, some crude assumptions have been made that are unlikely to apply in practice.

### D.3.2 Background to example

The undertaking subject to analysis is the operation of an Automatic Half Barrier level crossing in a particular location. There is scope for making improvements to the operation and use of this system. The aim of this risk assessment is therefore to determine whether changes are required in order to reduce the risk presented by the particular Automatic Half Barrier to a level that is compliant with the principle of ALARP.

It should be noted that the Automatic Half Barrier concerned has, to date, been in operation for a period of 20 years. There is, therefore, some considerable operational experience of its use.

### D.3.3 Hazard Identification

The operation of an Automatic Half Barrier level crossing is not a novel process. Hence the hazards associated with this undertaking were predominantly identified from a checklist.

The likely frequency and severity of each hazard has been estimated using the categorisation detailed in Table D-2 and Table D-3.

For each hazard, its estimated frequency and severity have been multiplied to obtain the hazard's 'rank'. Table D-4 presents the results of hazard identification and ranking.

<b>Frequency category</b>	<b>Definition</b>
1	Less than 100 yearly
2	10 to 100 years
3	1 to 10 yearly
4	Monthly to yearly
5	Daily to monthly

**Table D-2 - Categorisation for estimated hazard frequency**

<b>Severity category</b>	<b>Definition</b>
1	Minor injury
2	Major injury
3	Multiple major injuries
4	Single fatality
5	Multiple fatalities

**Table D-3 - Categorisation for estimated hazard severity**

Hazard Ref.	Hazard Description	Estimated Frequency	Estimated Severity	Hazard Rank	Comments/Rationale
1	Works Crossing is Used When Not Authorised	N/A	N/A	N/A	The crossing under analysis is not a works crossing. Hence, this hazard is not relevant
2	Failure of Level Crossing to Protect Public From Train	2	4	8	During the period for which this crossing has been in operation (20 years), no such failure has occurred. The low traffic supported by this crossing reduces the hazard severity
3	Barrier Operates Without Being Caused By Train	3	4	12	Failures of this type result mainly in service disruption. However, there is a possibility that subsequent manual operation of the barrier will result in an accident
4	Misuse of Level Crossing by Road User	4	2	8	Accidents of this type are most likely to result from a road user swerving around the closing barriers. The most likely consequence is impact with the infrastructure, resulting in a major injury
5	Use of Crossing Exceeds Original Design Limits	N/A	N/A	N/A	The current use of the crossing is well within the original design limits
6	SPAD at Signal Protecting Level Crossing	1	4	4	During the period for which this crossing has been in operation, no such SPAD has occurred. Additionally, the long signal overlap would mitigate most occurrences of this hazard
7	Poor Sighting of Level Crossing	5	4	20	Risks associated with poor sighting of the crossing occur each time a road user approaches the crossing when it is in use by a train.

Table D-4 - Results of hazard identification

### D.3.4 Causal Analysis

Causal Analysis has been conducted to estimate the annual frequency of occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard.

For the purposes of this illustrative example, only the results of Causal Analysis of Hazard 2 are presented – 'Failure of Level Crossing to Protect Public from Train'. The simple fault tree constructed to evaluate the frequency of occurrence of the hazard is presented in Figure D-1.

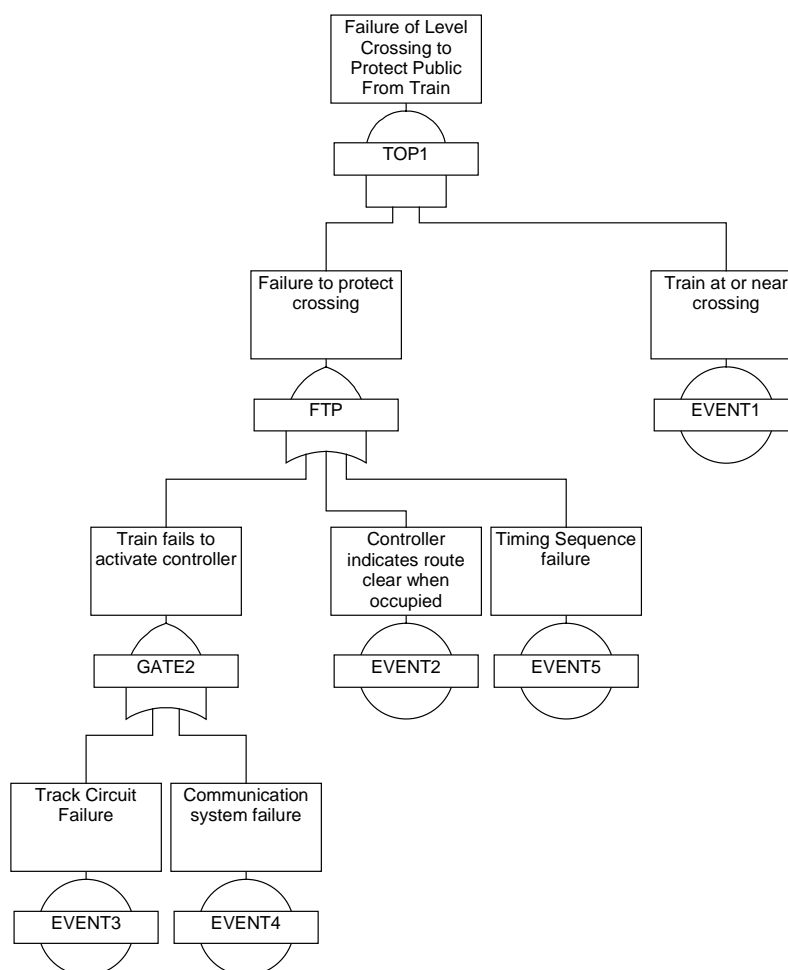


Figure D-1 - Fault tree for hazard 2

The fault tree has been quantified on the basis of the following analysis:

- From examination of the timetable it has been determined that an average of four trains traverse the crossing per hour. Protection is required for the crossing of each train for a period of approximately 90 seconds. At any time, therefore, the probability of the event 'Train at or near level crossing' is as follows:

$$\text{Probability} = \frac{90 \times 4}{3600} = 0.1$$

- There is some considerable operational experience of use of the level crossing controller employed at this crossing, both within the Railtrack network and overseas. On the basis of the records of this experience, it has been determined that the probability of the event 'Controller indicates route clear when occupied' is  $5.0 \times 10^{-3}$  per annum per controller.
- Similarly, there is considerable experience of use of the particular type of track circuit employed in this undertaking to indicate the presence of an approaching train to the level crossing controller. Records maintained by Railtrack suggest that, for the rolling stock type used on the line concerned, the probability of the event 'Track circuit failure' is  $2.5 \times 10^{-3}$  per annum.
- An independent contractor has previously been employed by Railtrack to determine the likelihood of failure of communications to the level crossing controller. Analysis conducted by this contractor suggests that the probability of the event 'Communication System Failure' is  $1.5 \times 10^{-3}$  per annum.
- The event 'Timing Sequence Failure' covers the situation when there is a pedestrian or vehicle on the crossing when the barriers fall. Operational experience gained from use of the level crossing suggests that slow moving pedestrians and traffic cause protection to be removed from this crossing twice per year on average. Hence the probability of the event 'Timing Sequence Failure' is 2.0 per annum.

Using the above values of each of the fault tree base events, the probability of Hazard 2 has been determined as follows:

$$\text{Probability} \approx \left( (2.5 \times 10^{-3} + 1.5 \times 10^{-3}) + 5.0 \times 10^{-3} + 2.0 \right) \times 0.1 = 0.20$$

Note that the probability of the hazard is dominated by the probability of the event 'Timing Sequence Failure'.

### D.3.5 Consequence Analysis

Consequence Analysis has been conducted to determine those incidents, which may arise from occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard, in a similar manner to that for Causal Analysis.

For the purposes of this illustrative example, only the results of Consequence Analysis of Hazard 2 are presented – 'Failure of Level Crossing to Protect Public from Train'. The particular method of consequence analysis used to analyse this hazard is the 'Cause Consequence' modelling technique. This is an inductive method of analysis where the hazard under consideration is displayed at the bottom of a decision-tree structure. Possible protective barriers affecting event escalation are then identified, classified and assessed. The potential outcomes (consequences) as a result of success or failure of the barriers are presented at the top of the page. The consequences can range from benign, essentially safe conditions to major or catastrophic accidents.

The simple cause-consequence models constructed to investigate the consequences of Hazard 2 are presented in Figure D-2. The consequences to pedestrians and other road users are modelled separately.

For the purposes of this analysis it has been estimated that, on average, 500 pedestrians use the crossing per day, taking 9 seconds each to traverse the crossing. Since trains run for 15 hours per day on this line, this leads to the following probability of a pedestrian being present at the crossing at any given time whilst trains are running:

$$\text{Probability} = \frac{500 \times 9}{3600 \times 15} = 8.3 \times 10^{-2}$$

Similarly, to estimate the probability of a road user being present at the crossing it has been estimated that, on average, 1000 vehicles use the crossing per day, taking 5 seconds to traverse the crossing.

It can be seen from the analysis, that most occurrences of the hazard do not lead to an accident, due to mitigating factors such as the vigilance of pedestrians and other road users and other, circumstantial factors, such as there being no traffic at the crossing when the hazard occurs.

*Note: The estimates of the probability with which a vehicle or pedestrian takes successful emergency action have to take account of the fact that, in most cases where the hazard occurs, it is as a result of a slow moving vehicle or pedestrian in the first place.*

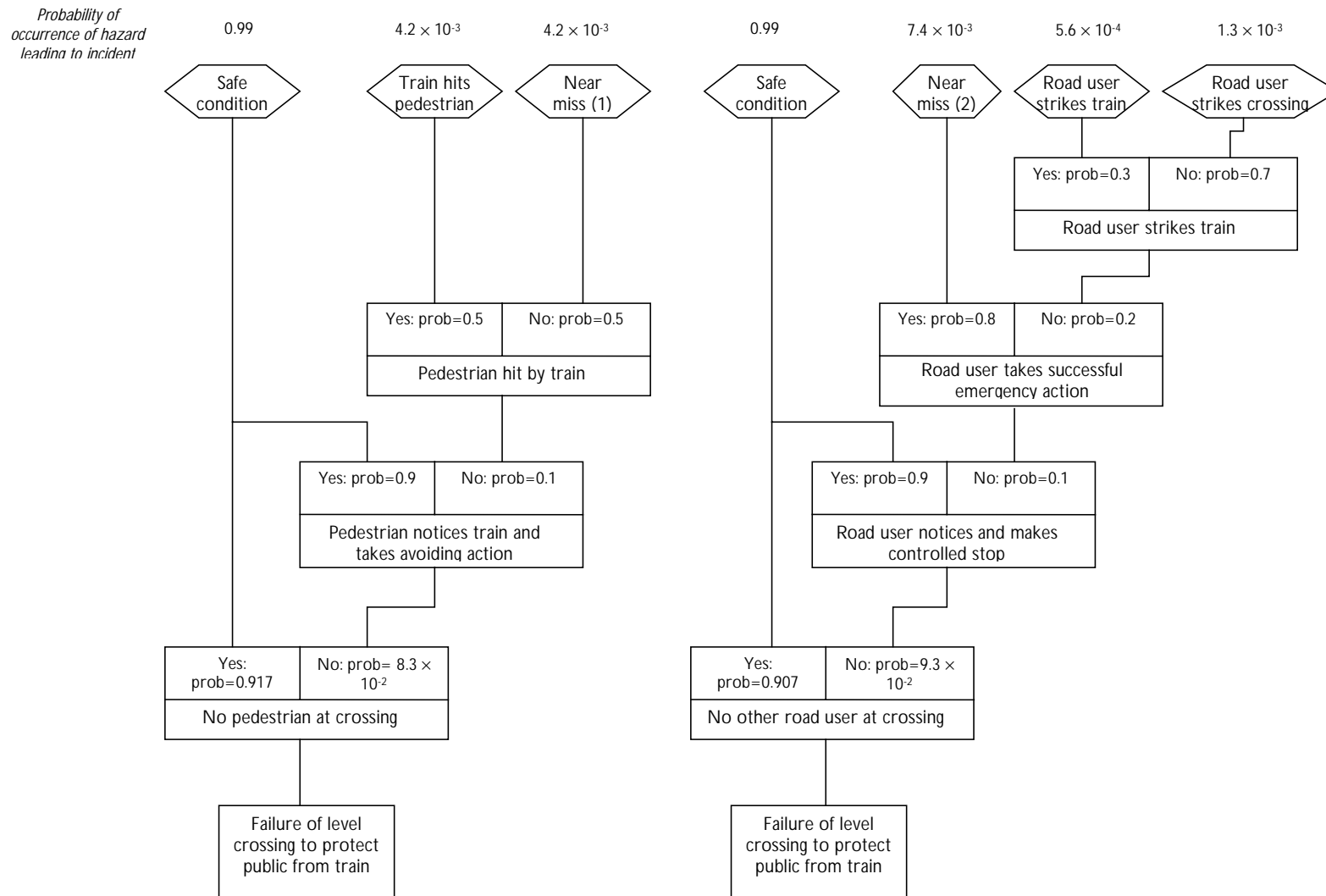


Figure D-2 - Cause-consequence models for Hazard 2

### D.3.6 Loss Analysis

Loss Analysis has been conducted to determine the magnitude of potential safety losses associated with each hazard.

For the purposes of this illustrative example, only the results of Loss Analysis of Hazard 2 are provided – 'Failure of Level Crossing to Protect Public from Train'. Table D-5 presents details of the loss modelling conducted. The incidents (consequences) have been taken from the cause consequence diagram presented earlier. The following incidents were identified:

- Safe Condition,
- Near Miss,
- Train Hits Pedestrian,
- Road User Strikes Train,
- Road User Strikes Crossing.

It has been assumed that no losses arise from a Safe Condition. A Near Miss is judged not to result in safety losses, although it can result in significant train delays. The remaining consequences all result in both safety and commercial losses.

Following analysis of Railtrack accident statistics, for circumstances similar to the level crossing under study, it has been assumed that:

- the incident 'Train Hits Pedestrian' results in no injuries to passengers, but 1 fatality to a member of the public;
- the incident 'Road User Strikes Train' results in 2 minor injuries to passengers and a single major injury to a member of the public;
- the incident 'Road User Strikes Crossing' results in 1 minor injury to passengers and 1 major injury to a member of the public.

The injuries associated with each incident have been converted to a corresponding Potential Equivalent Fatality (PEF) figure using the following currently accepted Railtrack convention:

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

Incident	Frequency (per annum)	Safety loss per incident (PEF)		Safety loss per annum (PEF)	
		Passenger	Public	Passenger	Public
Train Hits Pedestrian	$8.4 \times 10^{-4}$	-	1	-	$8.4 \times 10^{-4}$
Near Miss (1)	$8.4 \times 10^{-4}$	-	-	-	-
Near Miss (2)	$1.5 \times 10^{-3}$	-	-	-	-
Road User Strikes Train	$1.1 \times 10^{-4}$	$10^{-2}$	0.1	$1.1 \times 10^{-6}$	$1.1 \times 10^{-5}$
Road User Strikes Crossing	$2.6 \times 10^{-4}$	$5 \times 10^{-3}$	0.1	$1.3 \times 10^{-6}$	$2.6 \times 10^{-5}$
Total per annum				$2.4 \times 10^{-6}$	$8.8 \times 10^{-4}$

**Table D-5 - Results of Loss Analysis for hazard 2**

It should be noted that, in order to demonstrate compliance with the ALARP criteria, in a subsequent stage of risk assessment, safety losses have been determined individually for the following Groups defined by Railtrack as exposed to the risk of railway operations: passengers and the public. The hazard has not been determined to lead to any losses to employees (trackside workers).

The annual frequency of each incident has been determined by multiplying the estimated frequency of the hazard (derived during Causal Analysis) by the estimated probability of the hazard leading to the incident once the hazard has occurred (derived during Consequence Analysis).

Commercial losses have been estimated by means of expert judgement and through knowledge of previous incidents.

### D.3.7 Options Analysis

Both structured brainstorming and a suitable checklist have been used to identify potential risk mitigation options for each hazard. The checklist that has been used records known mitigation measures employed elsewhere throughout the Railtrack network. Use of brainstorming and the checklist together provide a high degree of confidence that all significant options for risk mitigation have been identified.

Table D-6 summarises those risk mitigation options that have been identified.

Option costs have been derived from knowledge of previous application of protective measures at similar level crossings and, for measures such as provision of Automatic Train Protection, through use of expert judgement.

### D.3.8 Impact Analysis

Each of the potential risk mitigation options identified in the previous stage of risk assessment have been analysed further to determine their effects upon the losses associated with operation and use of the level crossing.

Estimates of the reductions in losses achieved through use of each option have been calculated by modifying the Causal or Consequence models associated with the option (developed in the previous stages of risk assessment).

Hazard Ref.	Hazard Description	Hazard Rank	Option	Option Cost (£ pa)
2	Failure of Level Crossing to Protect the Public From Passing trains (Wrong Side Failure of Level Crossing)	8	1. Modify crossing to have more reliable controller	750
			2. Modify crossing sequence to provide greater crossing time	750
			3. Rewire cables to controller to replace degraded cabling	1000
4	Barrier Operates Without Being Caused By Train	12	4. Provide CCTV to protect crossing from vandalism/abuse	2500
5	Misuse of Level Crossing by Road User	8	5. Provide warning signs at approach to level crossing	300
7	SPAD at Signal Protecting Level Crossing	4	6. Provide Automatic Train Protection	20000
8	Poor Sighting of Level Crossing	20	7. Provide warning signs to indicate to road user the state of route ahead	2000
			8. Re-routing of approaching road	50000

**Table D-6 - Results of Options Analysis**

For the purposes of this illustrative example, only the results of the analysis of one of the options are presented – modify crossing sequence to provide greater crossing time. To further analyse this option it has been estimated that by increasing the crossing time, the probability of the event 'Timing Sequence Failure' can be reduced by an order of magnitude.

Applying this revised failure probability within the previous causal analysis of the hazard leads to a reduced annual probability of occurrence of the hazard of  $2.1 \times 10^{-2}$ . The loss analysis conducted previously has therefore been revised and the results of this revised analysis are presented in Table D-7.

Incident	Frequency (per annum)	Safety loss per incident (PEF)		Safety loss per annum (PEF)	
		Passenger	Public	Passenger	Public
Train Hits Pedestrian	$8.8 \times 10^{-5}$	-	1	-	$8.8 \times 10^{-5}$
Near Miss (1)	$8.8 \times 10^{-5}$	-	-	-	-
Near Miss (2)	$1.6 \times 10^{-4}$	-	-	-	-
Road User Strikes Train	$1.2 \times 10^{-5}$	$10^{-2}$	0.1	$1.2 \times 10^{-7}$	$1.2 \times 10^{-6}$
Road User Strikes Crossing	$2.7 \times 10^{-5}$	$5 \times 10^{-3}$	0.1	$1.4 \times 10^{-7}$	$2.7 \times 10^{-6}$
Total losses per annum (with mitigation) – (A)				$2.6 \times 10^{-7}$	$9.2 \times 10^{-5}$
Total losses per annum (without mitigation) – (B)				$2.4 \times 10^{-6}$	$8.8 \times 10^{-4}$
Total mitigated losses per annum (B-A)				$2.1 \times 10^{-6}$	$7.9 \times 10^{-4}$

**Table D-7 - Revised Loss Analysis assuming modified crossing sequence time**

### D.3.9 Demonstration of ALARP and Compliance

Railtrack currently define three Groups exposed to the risks of their operations: employees (trackside staff), passengers and the public.

Table D-8 details the ALARP and Benchmark criteria currently adopted by Railtrack for each Group and specified in Railtrack's Railway Safety Case. Each of the values represents an average risk of fatality per annum for an individual in the respective Group.

Group	Upper Limit of Tolerability	Broadly Acceptable bound	Benchmark
Employee	$10^{-3}$	$10^{-6}$	$10^{-4}$
Passenger	$10^{-4}$	$10^{-6}$	$10^{-5}$
Public	$10^{-4}$	$10^{-6}$	$10^{-5}$ §

**Table D-8 - ALARP and Benchmark criteria currently employed by Railtrack for all of its operations**

§ It should be noted that Railtrack's actual Benchmark figure is lower than this value. This value is however used for the purposes of this illustrative example

Previous investigations and analysis conducted by Railtrack suggest that automatic half barrier level crossings contribute 10%, 20% and 50% of the total risk of all of Railtrack's operations, to Employees, Passengers and the Public respectively.

There are known to be 300 such crossings in the Railtrack network. Whilst some crossings are known to pose slightly increased risk compared to others, analysis conducted by Railtrack suggests that the majority of crossings are associated with similar risk levels.

Hence, it can be assumed that the fraction of Railtrack's total safety risk which is associated with a single automatic half barrier level crossing is as follows:

$$\begin{aligned} \text{Fraction of total safety risk to Employees} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.1) / 300 = 3.3 \times 10^{-4}$$

$$\begin{aligned} \text{Fraction of total safety risk to Passengers} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.2) / 300 = 6.7 \times 10^{-4}$$

$$\begin{aligned} \text{Fraction of total safety risk to Public} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.5) / 300 = 1.7 \times 10^{-3}$$

The apportioned ALARP and Benchmark criteria which the level crossing under consideration should meet can therefore be determined by multiplying the criteria given in Table D-8 by the above fractions. The resulting apportioned criteria are given in Table D-9.

Group	Apportioned Upper Limit of Tolerability	Apportioned Broadly Acceptable bound	Apportioned Benchmark
Employee	$3.3 \times 10^{-7}$	$3.3 \times 10^{-10}$	$3.3 \times 10^{-8}$
Passenger	$6.7 \times 10^{-8}$	$6.7 \times 10^{-10}$	$6.7 \times 10^{-9}$
Public	$1.7 \times 10^{-7}$	$1.7 \times 10^{-9}$	$1.7 \times 10^{-8}$

**Table D-9 - Apportioned ALARP and Benchmark criteria for the undertaking concerned**

In order to determine the total safety losses associated with the undertaking, the estimated safety losses associated with each of the hazards, prior to application of mitigation measures, have been summed together. The results of this summation are presented in Table D-10 (note that only the estimated safety losses associated with Hazard 2 have previously been presented as part of this illustrative example).

Group	Total Safety Losses Associated with Undertaking per annum
Employee	0
Passenger	$5.2 \times 10^{-7}$
Public	$8.0 \times 10^{-4}$

**Table D-10 - Total safety losses associated with undertaking per annum**

It is estimated that, on average, 10000 different individuals are regular daily users of the crossing. The average risk to each of these individuals, associated with the undertaking, is therefore as presented in Table D-11. It should be noted that significantly more than 10000 different individuals use the crossing per year. However, outside of the 10000 regular daily users, other individuals use the crossing very infrequently and are not therefore considered in this risk apportionment.

Group	Average Safety Losses per Individual per annum
Employee	0
Passenger	$5.2 \times 10^{-11}$
Public	$8.0 \times 10^{-8}$

**Table D-11 - Average safety losses per individual associated with undertaking per annum**

Comparison of the average individual risk with the apportioned ALARP and Benchmark criteria suggests that the risks to employees and passengers fall below the Apportioned Broadly Acceptable Bound. However, the average risk to a member of the public falls within the tolerability region (above the Apportioned Broadly Acceptable Bound and below the Apportioned Upper Limit of Tolerability). It is therefore necessary to determine those risk mitigation measures which should be applied in order to reduce risks to ALARP levels.

For the purposes of this exercise we use a VPF of £1.63M.

Table D-12 presents a summary of each of the risk mitigation options and the annual reductions in safety losses to which they may lead (note that only the reductions in safety losses associated with modified crossing sequence time have previously been presented as part of this illustrative example). The table employs the VPF value detailed above. Net costs are derived by subtracting any mitigated commercial losses from the direct costs.

Risk mitigation option	Direct costs per annum (£)	Net costs per annum (£)	Annual mitigated safety loss (PEF)	Annual monetary value of mitigated loss (£)
1	750	710	$3.9 \times 10^{-5}$	64
2	750	690	$7.9 \times 10^{-4}$	1300
3	1000	950	$9.1 \times 10^{-5}$	150
4	2500	2400	$6.3 \times 10^{-5}$	100
5	300	290	$2.3 \times 10^{-5}$	37
6	20000	20000	$7.1 \times 10^{-5}$	120
7	200	1900	$5.6 \times 10^{-5}$	91
8	50000	49000	$6.3 \times 10^{-5}$	100

**Table D-12 - Cost-benefit analysis of potential risk mitigation options**

It can be seen that only option 2 is reasonably practicable to implement. Hence, the risks associated with the undertaking are reduced to ALARP levels through implementation of option 2 only and without any further mitigation measures.

The residual risk of the undertaking after implementation of option 2 is as follows:

$$\text{Residual risk} = 8.0 \times 10^{-4} - 7.9 \times 10^{-4} = 1.0 \times 10^{-5} \text{ per annum}$$

The average residual risk to the 10000 regular daily users of the crossing is therefore  $1.0 \times 10^{-9}$  per annum. This is less than the apportioned Railtrack benchmark.

## D.4 Safety Assessment remit

The following generic wording is used and recommended by the Railtrack System Review Panels as a starting point for writing remits for safety assessments:

*The assessment shall:*

- *State the safety targets which have been used in carrying out the assessment.*
- *Give a professional recommendation on the suitability and acceptability of the document with regard to its stated purpose.*

*The critical and most sensitive arguments of the documents should be clearly and concisely highlighted and a professional opinion shall be given as to the robustness of the argument. Where the argument of contained in whole or part within other documents or is part of existing custom and practice this should be clearly identified.*

*A professional opinion should also be given, with regard to the railway system as a whole, as to the practicality of any measures used to mitigate against the hazards raised.*

- *Identify any non-compliances to Railway Group or Railtrack Line Standards and legal requirements.*
- *Supply related technical advice as required by the Client, or as perceived necessary by the advisor.*

*All assessor observations are to be uniquely numbered and classified into one of the following three Classes, categories 1 to 3 should be used where operational use is being sought and categories A to C where other documents are under review (additional subclasses are permitted to aid clarity):*

### ***Documents seeking Operational Authority***

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

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

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

**Other Documents**

*Category A* Concerns, errors, omissions or questions that have a direct bearing on the acceptability of the document, which it is necessary to resolve prior to the consideration of downstream or offspring documents.

*Category B* Requires satisfactory resolution prior to acceptance of complete safety submission, or within a defined time period (not normally to exceed 6 months).

*Category C* Minor errors, e.g. syntax, spelling, minor technical matters which have no direct significant safety implications. For clarity, these require to be recorded and correcting if the document is re-issued, but are not in themselves sufficiently significant to warrant re-issue on their own.

*For either the numerical or alphabetical categories, where there are a large number of lower category issues, the reviewer is to consider whether in totality they represent sufficient residual risk that they in effect equate to one or more higher category issues (e.g. that they would warrant the imposition of any additional mitigating control measures). In these circumstances, It should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document which has been reviewed.*

## D.5 Safety Audit checklist

### D.5.1 Pro forma

This section presents a pro forma for each question in the audit checklist. Each question should be entered and given a unique reference. Following the audit the answer should be ringed, evidence to support the answer entered and the impact of the answer indicated. Conformance should be indicated by ringing *OK*; or category *A*, *B* or *C* (see chapter 14). Any further comments should also be noted.

Question: <Enter question>	Ref: <Enter unique reference>
Evidence: <Enter supporting evidence>	Yes    No    n/a <Ring answer>
Comments: <Enter any other comments, if any>	OK    A    B    C <Ring impact>

### D.5.2 Example audit checklist

This section contains typical questions that might be asked during a Safety Audit. It is intended to be an example and is neither exhaustive nor mandatory.

Where a question asks if something is adequate, judgement from the Safety Auditor is required, taking into account explanations provided by the Project Manager. In general something is adequate if:

- it meets specified requirements;
- it is effective and economical;
- it is appropriate to the circumstances; and
- it represents best practice.

#### D.5.2.1 Safety planning

- a) Is there an adequate Safety Plan (see chapter 12)?
- b) Are the responsibilities for safety and the competencies of staff clearly defined?
- c) Is the Safety Plan clear, easily obtained and accessible to the project?
- d) Have appropriate safety requirements been defined for each deliverable?
- e) Have suitable controls been devised to verify the safety requirements?
- f) Has an appropriate approach to safety been chosen?

#### D.5.2.2 Safety documentation

- a) Has the Safety Documentation required for the project been identified?
- b) Has the identified documentation been produced?
- c) Is the plan for safety documentation adequate?
- d) Have the responsibilities for producing safety documentation been identified?
- e) Has the documentation been produced by the staff identified for the task?
- f) Has an appropriate standard for documentation been specified?
- g) Has the standard been consistently applied?

#### D.5.2.3 Subcontract management

- a) Has an adequate method of evaluating subcontractor capability been identified?
- b) Has this method been rigorously applied to all subcontractors?
- c) Has each subcontractor been set safety targets or requirements?
- d) Has each subcontractor produced a Safety Plan?
- e) Have these plans been reviewed and approved as defined in the project Safety Plan?
- f) Is there any evidence of subcontractor non-compliance?
- g) Have all subcontractor-identified hazards been entered in the Hazard Log?

#### D.5.2.4 Testing

- a) Has testing called for in the Safety Plan been carried out?
- b) Is the test team independent of the development team?
- c) Have incidents arising from testing activities been entered in the Hazard Log?
- d) Does the testing programme adequately demonstrate the safety of the system?

## D.6 Safety Assessment checklist

Where a checklist question relates to a document or a task, the current section providing guidance for that document or task should be consulted. These have not been identified in the checklists to avoid extensive updating when changes are introduced.

Questions marked with an asterisk may require comments to be recorded separately and referenced accordingly.

### D.6.1 Commissioning an assessment

Checklist for person writing requirements:

- a) Safety Assessor has sufficient independence (see chapter 14);
- b) Safety Assessor has sufficient qualifications and experience (see chapter 14);
- c) Requirements have been discussed with Project Manager;
- d) Remit has been signed by originator;
- e) Remit has been signed by Safety Assessor;
- f) Remit has been copied to Safety Assessor and Project Manager.

### D.6.2 The assessment process

Checklist for Safety Assessor:

- a) For the system to be assessed, has the following documentation been checked:
  - Safety Plan?
  - Hazard Log?
  - Safety Requirements Specification?
  - Specification?
  - Drawings?
- b) Have safety requirements been identified in the documentation listed above?
- c) Having read the above documentation do you have any questions or points of doubt over the requirements? \*
- d) Has the system been identified functionally by means of block diagrams?
- e) Do the block diagrams cover levels of the systems from the highest down to line replaceable units?
- f) Do the block diagrams adequately represent the system as specified?
- g) Is there design documentation showing reasons for decisions made in the system design process?
- h) Do you have any comments or recommendations regarding the design disclosure document? \*
- i) Has a hazard list been compiled?
- j) Have hazards been removed/mitigated where appropriate?

- k) Do you have any comments or recommendations concerning the hazard list? \*
- l) Has a list of potential accidents been compiled?
- m) Do you have any comments or recommendations on the list of potential accidents? \*
- n) Have any novel or unproved features in the design been noted so that particular attention can be given to resolving any safety problems?
- o) Do you have any comments or recommendations regarding the novel or unproved features? \*
- p) Has any information been compiled on the safety of similar systems?
- q) Do you have any comments or recommendations on the information provided on similar systems? \*
- r) Have accident sequences been analysed for each type of potential accident?
- s) Do you have any comments on the accident sequence analyses? \*
- t) Have risk assessments been made?
- u) Has the risk been reduced ALARP?
- v) Have risk classifications been made?
- w) Have tolerable risk levels been agreed?
- x) Have accident rate targets been set?
- y) Have hazard rate targets been set?
- z) Have Safety Integrity Levels been determined for the safety elements of the design?
- aa) Has the design been assessed against the targets for the random elements of the design?
- ab) Has the design been audited against the design rules implied by the Safety Integrity Level?

### D.6.3 Assessment checklist: Requirements definition

Checklist for Safety Assessor:

- a) For the system to be assessed, have the following documents been checked:
  - Feasibility Studies Reports?
  - Statement of Requirements?
  - Drawings?
- b) Have safety targets or requirements been given in the following documents:
  - Feasibility Studies Reports?
  - Statement of Requirements?

- c) Having read the above documents, do you have any questions or areas of doubt in the requirements? \*
- d) Has a Safety Plan been prepared?
- e) Do you have any comments or recommendations concerning the Safety Plan? \*
- f) Has a Hazard Log been started?
- g) Do you have any comments or recommendations regarding the Hazard Log? \*
- h) Has the system been identified, in schematic or functional drawings?
- i) Has failure mode effect analysis been done?
- j) Do you have any comments or recommendations concerning the failure mode effect analysis? \*
- k) Have accident sequences been considered?
- l) Do you have any comments on potential accident sequences, hazards, initiating events or contributory incidents? \*
- m) Have the severities or consequences of potential accidents been determined or classified?
- n) Do you have any comments on accident severity or consequence classification? \*
- o) Has the design been altered during project definition to reduce hazards?
- p) Do you have any comments or recommendations concerning hazard reduction? \*
- q) Have the probabilities or frequencies of initiating events been determined?
- r) Do you have any comments or recommendations on the likelihood of initiating events or hazards? \*
- s) Has a Risk Assessment criteria for determining tolerability been drawn up?
- t) Does target apportionment take into account the expected number of units in service?
- u) Do you have any comments on the determination of the tolerability of risk? \*
- v) Have risks been determined for all aspects of the design? \*
- w) Are there aspects of the design which you would recommend for further risk assessment? \*
- x) Does the specification for design and development contain safety targets and requirements?
- y) Do you have any comments on the specified targets or requirements? \*
- z) Have safety targets been allocated to the lower level functions?
- aa) Do you have any comments or recommendations on the allocation of safety targets? \*

#### D.6.4 Assessment checklist: Design, build and test

Checklist for Safety Assessor for use during system design, implementation, and testing:

- a) Has a Safety Plan been formally issued?
- b) Do you have any comments or recommendations concerning the Safety Plan? \*
- c) Has a Hazard Log been started and maintained?
- d) Do you have any comments or recommendations on the contents of the Hazard Log? \*
- e) Is the system design well-defined?
- f) Have the safety-related parts of the system been made as simple as possible?
- g) Have safety-related sub-systems been identified?
- h) Has there been any development of the design to remove undesirable features or improve performance characteristics?
- i) Are there any potential accidents associated with the design? \*
- j) Have the potential accident sequences been adequately examined? \*
- k) Have Design Reviews been carried-out?
- l) Do you have any comments or recommendations on the Hazard Identification and Analysis work?
- m) Has Risk Assessment been carried out?
- n) Does this table take into account the expected number of units in service?
- o) Do you have any comments or recommendations concerning the assessment of risks? \*
- p) Have tolerable levels of risk been established?
- q) Is the tolerability of risk consistent with the relevant industry standards?
- r) Have targets for numerical accident probability or rate been agreed for each type of potential accident?
- s) Have targets for numerical accident probability or rate been agreed for elements of the accident sequence?
- t) Have targets (quantitative or qualitative) been allocated down to sub-system functional level?
- u) Have quantitative hazard rate targets been apportioned separately to the random and systematic failure modes?
- v) Has the potential effects of common cause failures been assessed?
- w) Have random hazard rate targets been apportioned to the lower level functions of the system?
- x) Have Safety Integrity Levels been defined for the systematic elements?
- y) Have Safety Integrity Levels been apportioned to lower level functions according to agreed rules (see Chapter 9)?

- z) Have the targets and criteria developed from the above been adequately recorded and reported in the Hazard Log? \*
- aa) In carrying out the Safety Assessment, it is necessary to compare the random targets with those predicted for the random elements. Is the comparison satisfactory? \*
- ab) For the Safety Assessment of the systematic elements, it is necessary to audit the design against the tolerable levels of risk, the agreed rules for Safety Integrity Levels and the design techniques. Is the design acceptable? \*

#### D.6.5 Assessment checklist: Customer acceptance and validation

Checklist for Safety Assessor:

- a) Does the Safety Plan contain an element relating to a test and acceptance programme?
- b) Are the safety features of the design identified for acceptance tests?
- c) Do you have any comments or recommendations concerning the adequacy of the test programme? \*
- d) Have the results of the safety test and acceptance programme been recorded and reported in the Hazard Log?
- e) Are the results satisfactory? \*
- f) Are there any shortcomings or outstanding items? \*
- g) Is the level of test coverage adequate?

#### D.6.6 Assessment checklist: Site trial/pilot scheme

Checklist for Safety Assessor:

- a) Does the Safety Plan contain requirements for the conduct of Site Trial?
- b) Does the Safety Plan contain requirements for the conduct of a Pilot Scheme?
- c) Are the safety features of the system design identified for Site Trial purposes?
- d) Are the safety features of the system design identified for Pilot Scheme purposes?
- e) Do you have any comments regarding the adequacy of the Site Trial to demonstrate the safety features? \*
- f) Do you have any comments regarding the adequacy of the Pilot Scheme to demonstrate the safety features? \*
- g) Has an incident or defect reporting system been set up for the Site Trial?
- h) Is the trial covered by a Safety Certificate?
- i) Is the system being used with the constraints of the Safety Certificate?
- j) Are all necessary support arrangements in place?

**D.6.7 Assessment checklist: In-service support**

Checklist for Safety Assessor:

- a) Has support of the system in service been addressed during Requirements Definition?
- b) Has support of the system in service been addressed during Design and Development?

This page left intentionally blank

# Appendix E

## Techniques

This appendix provides additional guidance on the execution of the following techniques

- 1 Failure Mode and Effects Analysis (FMEA) (see chapter 8)
- 2 Hazard and Operability Studies (HAZOP) (see chapter 8)
- 3 Fault Tree Analysis (see chapter 8)
- 4 Cause Consequence Diagramming (see chapter 8)
- 5 Data Recording and Corrective Action System (DRACAS) (see chapter 12)

## E.1 Failure Mode and Effects Analysis (FMEA)

FMEA should be carried out in compliance with established standards such as BS 5760 [F.20].

*Note that users of this standard should ensure that they use a common set of units, if they wish their risk ratings to be comparable*

The analyst should consider components at a detailed level of indenture and record their failure modes along with causes and effects. The failure effects of these sub-components then become failure modes of components at the next higher level of indenture. The process is repeated up the functional hierarchy to yield the individual failure modes of the whole system.

The depth of the analysis should be adjusted according to the preliminary appraisal of the hazards. The components which contribute to more severe hazards should be analysed in greater detail.

Checklists, HAZOP or other techniques may be used to identify basic failure modes.

The analysis is recorded on a worksheet which has at least the following columns:

<b>Item Ref</b>	The unique identifier of the sub-component being considered.
<b>Description</b>	A description of this sub-component.
<b>Failure Ref</b>	A unique identifier for the failure mode entered.
<b>Mode</b>	A description of the failure mode.
<b>Causes</b>	For this failure.
<b>Effect</b>	Of this failure (local and system-wide).
<b>Compensating Provisions</b>	Which may cause the effects of this failure not to be promulgated.
<b>How detected</b>	The means by which the failure may be detected.
<b>Remarks</b>	Any other notes made by the analyst.

This conforms to the British Standard for FMECA [F.20 §2.2.3] except that there is no column for 'Severity of effects'. Criticality is considered instead during the later stages of Risk Assessment although note that FMECA may be more appropriate for some applications.

## E.2 Hazard and Operability Studies (HAZOP)

Where detailed design information is available and a high level of assurance is required a Hazard and Operability Study or HAZOP can be carried out.

HAZOP is a systematic, creative examination of a design by a multi-disciplinary team.

HAZOP is recommended for systems with potential catastrophic accidents, novel features or for systems that span several engineering disciplines.

HAZOP is an analysis technique developed originally for the chemical industry and described in the Reference Guide [F.21] and Interim DEF-STAN 00-58 [F.19]. The technique should be carried out as described in these documents.

The principal difference between application of HAZOP in the chemical industry and application in other engineering fields is in the way in which the design documentation is examined. In the chemical industry, examination is guided by traversing the flowchart, a schematic showing the connection of vessels, pipes and valves. In engineering applications an alternative representation of the parts and their interactions, such as a mechanical drawing, circuit schematic or data flow diagram should be used. The same technique can be applied at a number of levels within the design.

If no convenient form of the design exists then the analyst should construct a **Functional Block Diagram**. At each level of indenture this shows the components of the system or a sub-system as blocks with lines drawn between each pair of boxes that directly interacts.

The team collects the design documentation, including a full functional breakdown of the system. Each component, including the interfaces, of the system is inspected in turn. The team considers the **intention** of the system and by applying a list of **guide words** attempts to reveal plausible **deviations** from the design intention.

The guide words for hardware systems typically are as follows. Alternative guide words for Programmable Electronic Systems are considered in MOD Interim Def Stan 00-58 [F.19].

- |               |   |
|---------------|---|
| a) NO or NOT  | No part of the intention is achieved but nothing else happens |
| b) MORE       | Some quantitative increase over what was intended             |
| c) LESS       | Some quantitative decrease over what was intended             |
| d) AS WELL AS | Some qualitative increase over what was intended              |
| e) PART OF    | Some qualitative decrease over what was intended              |
| f) REVERSE    | The logical opposite of the intention happens                 |
| g) OTHER THAN | Something quite different happens                             |

The team should be constituted to cover the areas of expertise required to fully understand the system. For example, the examination of a signalling system may require a safety process expert, a hardware engineer, a software engineer, an expert in signalling principles and potential users and maintainers.

It is quite likely that the team will be unable to establish immediately whether a possible deviation can occur or what its effect can be. In that case an action can be recorded to establish this outside the meeting.

### E.3 Fault Tree Analysis

Fault Tree Analysis (FTA) is a widely known and accepted top-down or deductive system failure analysis technique. The Fault Tree Handbook, NUREG-0492 [F.22], is a comprehensive reference document for FTA, and may be used in conjunction with other FTA standards.

FTA begins with a single undesired top event and provides a method for determining all the possible causes of that event.

A correctly constructed Fault Tree is a graphical and logical model of the various parallel and sequential combinations of events that will result in the occurrence of the Top Event.

FTA can be used for both qualitative as well as quantitative analysis. The graphical nature of the technique aids the qualitative identification of potential sources of single-point failures and safety critical failure combinations.

The precise definition of the top event is critical to the success of the analysis, since an incorrect top event will, in most cases, invalidate the whole analysis.

The system is analysed, from the identified top events, in the context of its environment, and modes of operation, to find all credible causal events.

The fault tree is made up of gates, which serve to permit or inhibit the flow of fault logic up the tree. The gates show the relationship of lower events - the inputs to the gate - needed for the occurrence of a higher event - the output of the gate. The gate symbol denotes the relationship of the input events required for the output event.

The fault tree is used to produce the minimal cut sets - the minimum combination of independent base events which, if they occur or exist at the same time, will cause the top-event to occur. The minimal cut sets provide the basis for both the qualitative and quantitative analysis of the system.

Fault Trees are relatively simple in concept, but can be very difficult in practice. This is particularly true when quantitative analysis is required. Chapter V of NUREG-0492 [F.22] provides a detailed explanation of the technique. The following key concepts and rules from that document are given here to guide the analyst in the approach required to the construction of the tree.

In determining the causes of an event in a fault tree, the analyst should identify the **immediate, necessary and sufficient** causes for the occurrence of that event. The temptation to jump directly to the **basic** causes should be resisted, even if these may appear obvious.

The dependence between base events within a minimal cut set should be identified during FTA. This is achieved by performing Common Cause Failure Analysis on the Minimal Cut Sets to identify potential dependencies.

The following basic rules should be applied when constructing a fault tree:

- a) Write the statements that are entered into the event boxes as faults: state precisely **what** the fault is and **when** it occurs.
- b) If the answer to the question 'Can this fault consist of a component failure?' is 'Yes', classify the event as a '**State of Component Fault**'. If the answer is 'No', classify the event as a '**State of System Fault**'. If an event is classified as 'State of Component Fault', add an OR-gate below the event and look for primary, secondary and command faults that may cause the event. If an event is classified as a 'State of System Fault', an AND-gate, OR-gate, INHIBIT-gate, or possibly no gate at all may

be required, and the minimum, necessary and sufficient causes should be determined.

- c) If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.
- d) All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken.
- e) Gate inputs are to be properly defined fault events. Gates are not to be connected directly to other gates.
- f) Identify fixed probabilities ie non-failure conditions, with inhibit gates.

## E.4 Cause Consequence Diagramming

Cause Consequence Diagramming (or Cause Consequence Analysis) is a technique that embodies both causal and consequence analysis. However, in the context of the Yellow Book it is useful primarily as a consequence analysis tool.

The technique provides a diagrammatic notation for expressing the potential consequences of an event (normally a hazard) and the factors that influence the outcome.

The basic notation is introduced in the context of the example in figure Figure E-1. In this diagram the hazard is Ignition. The final outcomes (or 'significant consequences') are shown in octagons and vary from no incident to a major fire. The major factors that influence the outcomes are shown in 'condition vertices'.

The diagram shows that a major fire will only occur as a result of the ignition hazard if both the sprinkler and alarm system fail. If we can estimate the frequency with which the hazard will occur and the probability that the sprinkler and alarm systems will fail on demand (and, importantly, we know to what degree these failures are correlated) then we can estimate the frequency with which the hazard will give rise to this accident. This is an essential step on the way to estimating the risk arising from the hazard.

There are variations in notation. Railtrack have procured a tool, ACCA, which produces output in a slightly different format. There is an example of this output in appendix D.

The notation allows further symbols. For a slightly fuller exposition refer to 'Safeware: System Safety and Computers' [F.23], pages 332-335.

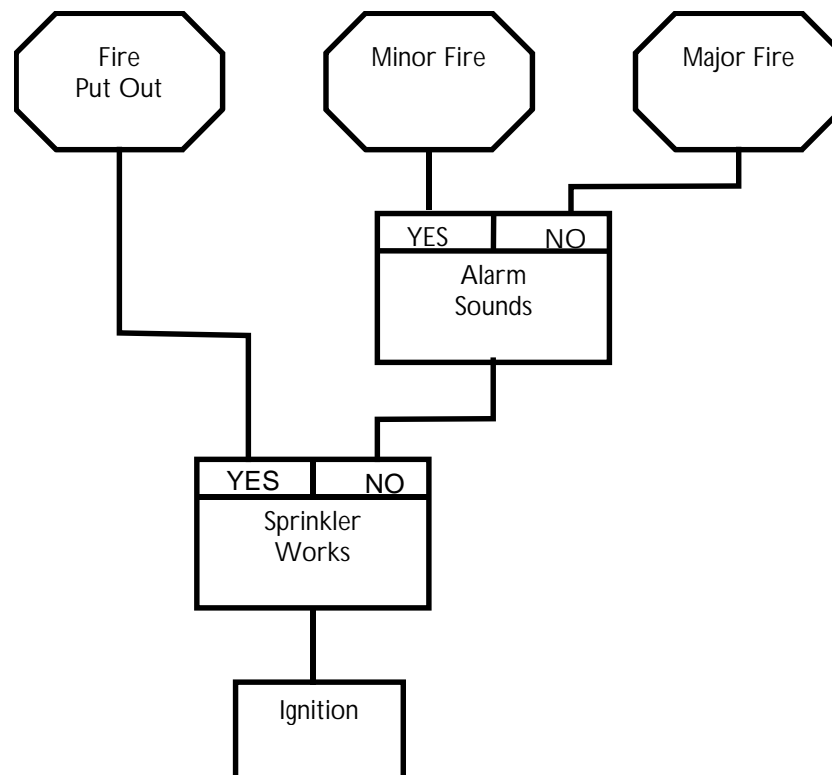


Figure E-1 - Example Cause-Consequence Diagram

## E.5 Data Reporting Analysis and Corrective Action System (DRACAS)

The Data Reporting Analysis and Corrective Action System (DRACAS) is a closed loop data reporting and analysis system. The aim of the system is to aid design, to identify corrective action tasks and to evaluate test results, in order to provide confidence in the results of the safety analysis activities and in the correct operation of the safety features.

Its effectiveness depends on accurate input data in the form of reports documenting incidents. These reports should therefore document all the conditions relating to the incident.

The Project Manager or Project Safety Manager should be part of the team that reviews the incidents, in order that their impact on the safety characteristics of the system can be quickly assessed and any corrective actions requiring design changes quickly approved.

The DRACAS process is illustrated in Figure E-2 and may be summarised as follows:

1. The incident is raised and recorded on a database.
2. A data search is carried out for related events.
3. The incident is reviewed.
4. If the incident is a new hazard it is recorded as such in the Hazard Log.
5. Corrective actions are recommended as necessary.
6. If no corrective action is required the database is updated and the process ends.
7. The corrective action is authorised and implemented and assessed for success.
8. If the corrective action is successful the database is updated and the process ends.
9. If the corrective action is unsuccessful the incident is re-reviewed (the process returns to step 4).

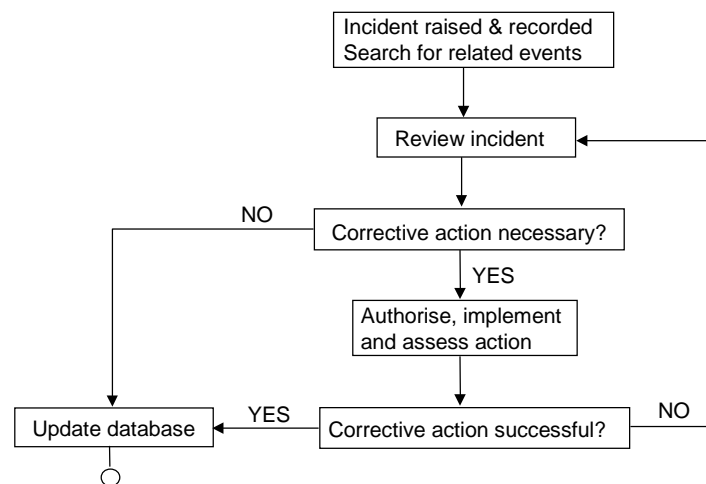


Figure E-2 - The DRACAS process

This page left intentionally blank

## Appendix F

### Referenced Documents

This appendix provides full references to the documents referred to in the body of volume 2.

- F.1 Ould M. A., *Business Processes: Modelling and Analysis for Re-engineering and Improvement*, Wiley 1995, ISBN 0-471-95352-0
- F.2 Profit R., *Systematic Safety Management in the Air Traffic Services*, Euromoney Books 1995, ISBN 1 85564 470 2
- F.3 *Guidelines on Risk Issues*, The Engineering Council, February 1993, ISBN 0-9516611-7-5
- F.4 Ministry of Defence, DEF-STAN 00-56, *Safety Management Requirements for Defence Systems*, Issue 2, December 1996
- F.5 DoD MIL-STD-882C, *System Safety Program Requirements*, 19 January 1993.
- F.6 Health and Safety Executive discussion document, *Reducing Risk, Protecting People*, 1999
- F.7 UK Offshore Operators Association, *Industry Guidelines on a Framework for Risk Related Decision Support*, issue 1, May 1999, ISBN 1 903003 00 8.
- F.8 CENELEC Draft prEN50126, *Railway applications – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)*
- F.9 Railway Group Standard GK/RT0206, *Signalling and Operational Telecommunications Design: Safety Requirements*, Issue 1, February 1998
- F.10 Railway Group Code of Practice GK/RC0701, *Signalling Design: Production Guidance*, Issue 1, October 1998
- F.11 Hessami A., *Risk – A Missed Opportunity?*, Risk and Continuity, volume 2, issue 2, June 1999, pages 17-26
- F.12 Preece J., Rogers Y., Sharp H., Benyon D., Holland S. and Carey T., *Human-Computer Interaction.*, Addison Wesley. 1994, ISBN 0-521-36570-8
- F.13 CENELEC ENV50129: 1998, *Railway applications – Safety related electronic systems for signalling*, May 1998
- F.14 International Electrotechnical Commission, IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems.*
- F.15 Ministry of Defence, Interim DEF-STAN 00-54, *Requirements for Safety Related Electronic Hardware in Defence Equipment*, Issue 1, 19 March 1999

- F.16 Ministry of Defence, DEF-STAN 00-55, *Requirements for Safety-Related Software in Defence Equipment*, Issue 2, 1997
- F.17 CENELEC Draft prEN50128: 1998, *Railway applications – Software for railway control and protection systems*
- F.18 HMRI, *Guide to the Approval of Railway Works, Plant and Equipment*, Health and Safety Executive, 1994
- F.19 Ministry of Defence, Interim Defence Standard 00-58, *HAZOP Studies on Systems Containing Programmable Electronics*, Issue 1, August 1996
- F.20 BS5760: Part 5 1991, *Reliability of systems, equipment and components: Part 5 Guide to failure modes, effects and criticality analysis*
- F.21 Chemical Industries Association, *A Guide to Hazard and Operability Studies*, Kings Buildings, Smith Square, London SW1P 3JJ, 1992
- F.22 NUREG 0492, *The Fault Tree Handbook*, 1981
- F.23 Leveson N., *Safeware: System Safety and Computers*, Addison-Wesley 1995, ISBN 0-201-11972-2