

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.