

Chapter 13

Configuration Management, Documentation and Records

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

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

13.1 Guidance from volume 1

13.1.1 Configuration management

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

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

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

13.1.2 Documentation and records

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

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

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

13.2 Background

A convincing demonstration of safety rests on good housekeeping.

Certain items within a system need to be accurately identified and changes to them need to be assessed for any safety implications and then monitored and tracked. This provides information on the different versions that may exist for that item, its relationship with other items, and the history of how it has developed and changed.

This chapter describes how to identify items whose configuration should be recorded and kept under control. It explains why configuration management should be applied to safety-related system items and documents and how it may be monitored.

There are three main reasons for keeping records of safety-related activities:

- 1 to show others that you have reduced risk to an acceptable level;
- 2 to explain to people making future changes why decisions were taken, so that they do not undo the work that you have done; and
- 3 to support the hand-over of safety responsibilities to other people.

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

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

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

This chapter is written for:

- Project Managers who are responsible for controlling the configuration of safety-related projects,
- engineering staff who make changes to any safety-related item, and
- managers and engineers who are responsible for preparing or updating safety records.

13.3 Roles and responsibilities

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

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

The Project Manager is responsible for the creation and maintenance of the Hazard Log and other safety records until the transfer of overall safety responsibility to another party.

The Project Manager may delegate this role to a Project Safety Manager but should retain overall responsibility. Guidance on transferring safety responsibility is provided in chapter 2.

13.4 Identification of configuration items

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

You should place all items which will support the Safety Case under configuration management. You should consider placing the following items under configuration management:

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

The following information should be maintained for each item

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

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

Section 13.5.4 details considerations specific to software items.

13.5 Configuration management plan

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

- a) a list of the types of configuration items;
- b) responsibilities for configuration management within the project, including the person responsible for approving updates to configuration items;
- c) the baselines that will be produced;

- d) the version control arrangements;
- e) the change control process;
- f) software configuration management arrangements (if required); and
- g) any configuration management tools used.

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

13.5.1 Baselines

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

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

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

13.5.2 Version control

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

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

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

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

13.5.3 Change control process

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

13.5.4 Software configuration management

All software programs that are deliverable, or affect the delivered product, should be held under change control, including:

- application programs,
- test programs,
- support programs,
- sub-programs used in more than one higher-level program,
- firmware components,
- programs for operation in different models,
- sub-programs from separate sources to be used in one higher-level program.

13.5.5 Configuration management tools

Configuration management requires a means of storing and controlling the configuration items. Some form of electronic database may be the best option and there are many tools available to perform this function. However, it is possible to perform configuration management without using electronic tools.

It is not necessary to contain all items under the same system. In fact it is often more efficient to separate the items into logical groups, such as software items, documentation, physical items, and so on and to choose the best tool for each group.

You should consider whether there is any plausible way in which a configuration management tool could contribute to a system hazard. If there is then you should regard the tool as safety-related and collect evidence of its dependability for inclusion in the Safety Case for the system.

13.6 Safety records

All safety-related projects should produce at least the following safety records:

- Hazard Log,
- Safety Plan,
- Safety Case.

Further records may be required for many projects. The extent of the safety records maintained by a project will depend on the complexity and level of risk presented by the project. Simple and low-risk projects will carry out only a small number of safety-related activities and the records required of these will be small. High-risk and complex projects will produce more safety records.

Safety records are valuable and difficult to replace. Appropriate security and backup safeguards should be employed to ensure their integrity.

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

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

Figure 13-1 illustrates the relationship between the Hazard Log and other safety records.

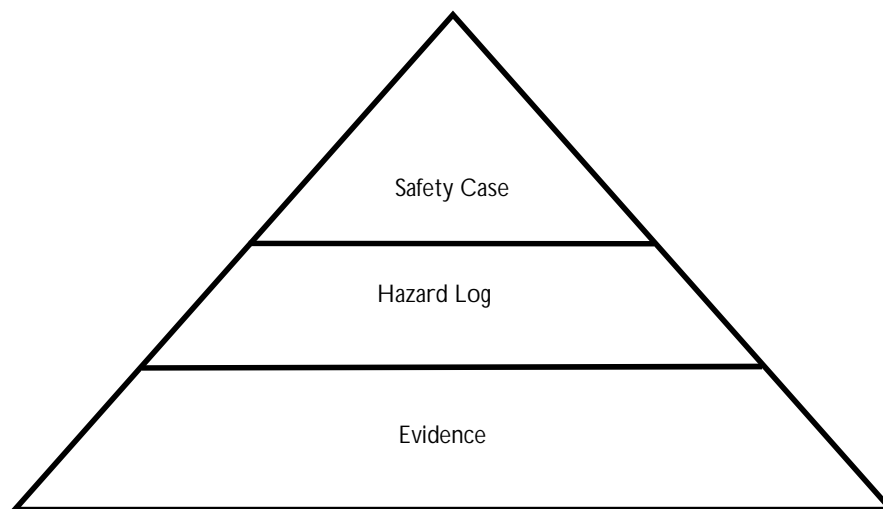


Figure 13-1 - Pyramid of safety management documentation

Note: there is variation in terminology in the industry and the phrases 'Safety Case' and 'Hazard Log' are sometimes used to include the evidence below them in Figure 13-1.

13.7 Management and control of the Hazard Log

The Hazard Log evolves and should be updated whenever:

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

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

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

The Hazard Log should be available for inspection by the Safety Auditor, the Safety Assessor and representatives of the relevant Safety Authorities.

The Project Manager should ensure that adequate provision is made for security and backup of the Hazard Log and other safety records.

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

13.8 Related guidance

Chapter 8 provides guidance on assessing and mitigating any safety implications of changes.

Safety Audits and Assessments of safety documentation are described in chapter 14.

Appendix B provides an outline Hazard Log.

Appendix C provides checklists for updating the Hazard Log.

This page left intentionally blank