0 SHOWING CONFORMANCE

0.1 Options

0.1.1 There are four options to demonstrate conformance when applying this system procedure:

a. Follow the defined system procedure using the recommended guidance and tools, including allowed variations and options.

b. Use an equivalent process and tool set generated elsewhere and document evidence of procedural equivalence.

c. Use a bespoke process and tool set for the project and document how the bespoke procedure achieves the objectives defined for this system procedure.

d. Where the procedure is considered to be not relevant, document the basis for this decision.

1 INTRODUCTION

1.1.1 A **Hazard Log** is defined in Def Stan 00-56 Issue 4 as:

"The continually updated record of the Hazards, accident sequences and accidents associated with a system. It includes information documenting risk management for each Hazard and Accident."

1.1.2 These Hazards, accident sequences and accidents are those which could conceivably happen, and not only the ones which have already been experienced.

1.1.3 The term Hazard Log is somewhat misleading, because the information stored relates to the entire Safety Programme and covers Accidents, Controls, Risk Evaluation and ALARP justification, as well as data on Hazards.

1.2 Purpose

1.2.1 A Hazard Log is used and maintained as the principal means of establishing progress on resolving risks associated with identified Hazards. It provides traceability of the Hazard management process to show how Safety issues are being dealt with and resolved.

1.2.2 Outstanding issues in the Hazard Log should be regularly reviewed by the Project Safety Committee to make sure that actions are completed and unacceptable Risks are resolved.

2 PROCEDURE OBJECTIVES

2.1.1 The Hazard Log contains the traceable record of the Hazard Management process for the Project and therefore:

a. Ensures that the Project Safety Programme uses a consistent set of Safety information;

b. Facilitates oversight by the PSC and other stakeholders of the current status of the Safety activities;

c. Supports the effective management of possible Hazards and Accidents so that the associated Risks are brought to and maintained at a tolerable level;

d. Provides traceability of Safety decisions made.

3 RESPONSIBILITIES

3.1 Accountability

3.1.1 The IPTL is accountable for the completion of this procedure.

3.2 Procedure Management

3.2.1 The IPTL may delegate the management of this procedure to a member (Safety Manager) or members of the IPT.

3.2.2 It is the responsibility of the IPT to define the scope and format of the Hazard Log and to ensure that the information it contains is current and reviewed at appropriate intervals.

3.3 Procedure Completion

3.3.1 The Hazard Log ensures that a common set of information can be shared by all parties with a genuine need for access. A single Hazard Log should therefore be maintained that is accessible by all these parties.

3.3.2 The Hazard Log may be run by the Prime Contractor or the MOD Project Team or a third party such as a Safety Assessment contractor. Indeed the Hazard Log may pass from one authority to another at key stages in the programme. For example, the Prime Contractor is likely to have greatest need of the Hazard Log during System Development, but the MOD Project Team may be a more appropriate controller when the System is in service.

3.3.3 The Hazard Log should be under the control of a Hazard Log Administrator, who is responsible to the Prime Contractor's Project Safety Engineer or the MOD's Safety Manager. The Hazard Log Administrator should have full access to the Hazard Log allowing him to add, edit or close Hazards. All other personnel requiring access to the Hazard Log are allowed read only access. This allows for visibility of Hazards to all but the strict control and administration of Hazards is limited to the Hazard Log Administrator.

4 WHEN

4.1 Initial Production

4.1.1 The Hazard Log should be established at the earliest stage of the programme and be maintained thereafter as a 'live' document or database to reflect the current design standard.

4.2 Review, Development and Acceptance

4.2.1 A review of the Hazard Log is essential at regular intervals to ensure that Hazards are being successfully managed and that the robustness of the safety arguments in the Safety Case can be established.

5 REQUIRED INPUTS

5.1 General

5.1.1 This procedure for Hazard Log requires inputs from:

a. Outputs from Procedure SMP01 – Safety Initiation;

b. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis;

c. Outputs from Procedure SMP05 –Hazard Identification and Analysis;

d. Outputs from Procedure SMP06 –Risk Estimation;

e. Outputs from Procedure SMP07 –Risk and ALARP Evaluation;

f. Outputs from Procedure SMP08 –Risk Reduction;

g. Outputs from Procedure SMP09 –Risk Acceptance;

h. Outputs from Procedure SMP10 –Safety Requirements and Contracts.

5.1.2 The Hazard Log is a database which references all the major items of Safety documentation relating to a project. This can include the following:

a. Safety Criteria Report;

b. Safety Requirements;

c. Hazard Identification Reports;

d. Hazard Analysis Reports;

e. Risk Analysis and Assessment Reports;

f. Safety Audit and Inspection Reports;

g. Safety Case Reports.

5.1.3 The Hazard Log stores information on hazards, accidents and accident sequences which might be associated with the system. Thus it records the results of all the Risk Management procedures (SMP04 to SMP09).

5.2 Supporting Documentation

5.2.1 Where the Hazard Log has adequate capacity and resources permit, the following supporting documentation should also be either directly embedded or cross-referenced by hypertext link where the Log is an electronic format:

a. Material/system survey reports;

b. Design defect reports, concessions and production permits;

c. System/equipment breakdown and failure reports;

d. Reports of technical design/material state reviews;

e. Reports of quality, reliability and safety audits;

f. Accident and incident reports, during construction, maintenance or in-service operation.

6 REQUIRED OUTPUTS

6.1 Hazard Log Report

6.1.1 The Hazard Log is a continuously evolving record (database or document) which should stay with the System throughout its life cycle. A Hazard Log Report is a snap shot of the Hazard Log status on a given date.

6.1.2 Hazard Log Reports will be produced for the purpose of review (eg by the PSC or the ISA) or communication of the current status of the Safety Programme. Where a computer tool is used to implement the Hazard Log, it must be capable of producing a range of reports, from detailed to summary.

6.1.3 Hazard Log Reports must be capable of showing the linkages between Hazards, Accidents and Controls (ie which Hazards could lead to which potential Accidents, possibly with many-to-many relationships, and which Controls relate to which Hazards and Accidents). They must also differentiate between Controls which are already in place and those which are being considered or planned.

7 DESCRIPTION

7.1 Hazard Log Fundamentals

7.1.1 The Key features associated with the Hazard Log are identified below:

a. The Hazard Log is a live document and as such should be updated throughout the programme. The Hazard Log should be set up at the initial stages of a project and remains current throughout the CADMID life cycle of a system.

b. The Hazard Log provides a record of all safety assessment information and evidence associated with a programme.

c. The Hazard Log provides documentation of all Safety Risk Evaluations conducted on a programme.

d. The Hazard Log provides an auditable tracking mechanism for a programme, showing what decisions were taken, when and why.

e. The Hazard Log provides a cross reference to all other Safety Analysis and documentation for a programme.

7.2 Content of Hazard Logs

7.2.1 Typical Hazard Log contents are described in **Guidance Sheet SMP11/G/01** - Hazard Log Contents.

7.2.2 The Hazard Log should describe the system to which it relates, and record its scope of use, together with the safety requirements.

7.2.3 When Hazards are identified, the Hazard Log will show how these Hazards were evaluated and the resulting residual risk assessed, and will either recommend further action to mitigate the Hazards, or formally document the acceptance of these Hazards and the ALARP justification.

7.2.4 The Hazard Log is a structured way of storing and referencing safety Risk Evaluations and other information relating to an equipment or system, it is to be co-ordinated and controlled whilst maintaining an auditable record of that information. It is the principal means of tracking the status of all identified Hazards, decisions made and actions undertaken to reduce the risk and should be used to facilitate oversight by the PSC and other stakeholders.

7.2.5 The Hazard Log is a tracking system for Hazards, their closures, and residual risk and must be maintained throughout the system life cycle as a “live” document. As changes are integrated into the system, this Hazard Log is updated to incorporate added or changed Hazards and the associated residual risk to reflect the current design standard.

7.2.6 The Log should capture the inputs to and outputs from Hazard Analysis and Risk Evaluation sessions. ALARP justification arguments and conclusions should be recorded when mitigation actions are complete.

7.3 Designing the Hazard Log

7.3.1 The process for a Hazard Log requires a number of initial steps to be undertaken prior to Hazard Log population. This is to ensure that there is a suitable infrastructure in place before Hazard information is stored.

a. A method by which the Hazard Log is to be implemented must be selected; this can either be in paper or electronic form. It is important at the outset to identify the appropriate tool/administration method for the Hazard Log.

b. A Hazard Log administrator must be appointed. The Hazard Log administrator will be responsible for the maintenance, upkeep and configuration control of the Hazard Log. All non administrators should be allowed read only access if the Hazard Log is in electronic format.

c. The Hazard Log must be ‘set up’. This will include activities such as inclusion of the Risk Classification scheme that has been agreed, determination of appropriate Hazard categories, status definitions and general set up activities to ensure that the Hazard Log will operate as required. The latter may be in the form of a guidance note for a paper based system or checking of the robustness of an electronic system.

7.4 Starting the Hazard Log

7.4.1 Once the system and its boundaries have been defined and the Hazard Identification process has begun, the Hazard Log should be established in order to keep a record of the Hazards and proposed or implemented mitigation measures to ensure that the Hazards are being appropriately controlled.

7.5 Running and Using the Hazard Log

7.5.1 The Hazard Log is the configuration control mechanism for the Safety Assessment process, and Hazards should not be deleted from the Hazard Log, but closed and marked if no longer relevant. A procedure is to be defined for the management and control of the Hazard Log. The Hazard Log is to be retained for the entire system life cycle and it should act as the primary source of the Logical arguments, or Safety Case, for the deployment of the system into service.

7.5.2 Review of the Hazard Log is essential at regular intervals to ensure that Hazards are being successfully managed and that the robustness of the established safety arguments in the Safety Case are not being compromised.

7.5.3 Generally the Hazard Log update might occur whenever:

a. A relevant Hazard or potential accident is identified, either through formal analysis or as a result of a change to the design/procedure/operating environment.

b. A relevant incident occurs, perhaps during testing or demonstration.

c. Further information relating to existing Hazards, incidents or accidents comes to attention; or safety documentation is created or re-issued.

7.5.4 In order to provide project awareness of Hazard and Accident data, the Hazard Log should be accessible to all of the appropriate project staff. This should include, but not necessarily be limited to the Project Safety Panel.

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

7.6 Hazard Log Process

7.6.1 Since the Hazard Log is a repository for managing identified Hazards, it is possible for Hazard identification to begin prior to the implementation of the Hazard Log.

7.6.2 Once the initial steps have been undertaken, the process of information entry can be started. The generic flow of the process is shown in the following steps:

a. Hazard Identification – Initially taken from procedures such as Preliminary Hazard Analysis, and then augmented by subsequent Risk Management activities.

b. Accident sequence development associated with the identified Hazards.

c. Formal Risk Evaluation of each accident sequence.

d. Mitigation identification – The recording of the appropriate and agreed mitigation for each accident.

e. Mitigation/control owners established – This should ensure that the mitigation or controls identified are put in place and the Hazard is addressed.

f. Cross checking to see if there are any other, previously identified Hazards or accident sequences linked with this Hazard.

g. Resolution – Status changes completed as required, formal closures recorded, including reference to evidence and ALARP justification recorded.

h. Ongoing Hazards managed and new Hazards added as required.

i. Production of a Hazard Log Report as determined by the Project Safety Plan.

7.7 “Ownership” of Hazards and Controls

7.7.1 Where the Project Safety Programme identifies Hazards that are the responsibility of another Project, then the information must be passed to the person with delegated Authority for that area. The Project Hazard Log must record that this was done.

7.7.2 Because Hazards and Accidents usually have a range of Control measures of different types associated with them, there is no single Hazard “owner” who is responsible for mitigating the associated Risks, other than the overall Delegated Authority. When a Control measure is agreed for implementation, it should be clearly assigned to an “owner”. This might be the Prime Contractor for a design change, the Training Authority for a topic to be covered in Maintainer training, or the User for a procedural control solution.

7.8 Closure or Removal of Entries

7.8.1 It is considered best practice for the Hazard Log to record each Hazard as “open” and for ALARP arguments to be provisional until all mitigation actions are confirmed to be satisfactorily completed. An example is where the mitigation depends upon production of an operational procedure that may not be written for a considerable time after the Hazard is first identified at an early stage of design or construction.

7.8.2 Hazards should not be deleted from the Hazard Log, but closed and marked as “out of scope” or “not considered credible”, together with the justification. Where they are no longer considered relevant to the system, the Log entry should be updated to reflect this.

7.9 Archiving on Project Closure

7.9.1 At the end of the project, the Hazard Log should remain as a historical record, which may be useful to refer to for similar applications in the future.

8 RECORDS AND PROJECT DOCUMENTATION

8.1.1 Where relevant, the outputs from this procedure should feed into the following:

a. SRD (System Requirements Document) – for any specific Safety requirements;

b. CSA (Customer Supplier Agreement) – to document agreements on Safety information to be delivered by the IPT;

c. TLMP (Through Life Management Plan);

d. Safety elements of Initial Gate and Main Gate submissions.

8.2 Data Security

8.2.1 Adequate provision must be made for security and backup of the Hazard Log and other safety records.

8.2.2 The Hazard Log is a prime source of corporate knowledge and is the configuration control mechanism for the Safety Assessment process. As such it could be referred to in legal proceedings. Every effort should therefore be made by the IPT Leader to ensure that records are accurate, attributable, up to date and complete. Clear cross-referencing to supporting documents is essential.

9 RECOMMENDED TOOLS AND FORMS

9.1 Hazard Log Software

9.1.1 The DE&S's preferred corporate Hazard Log tool is the CASSANDRA database system. IPT Leaders should consider tailoring this system to meet their needs. Individual Projects or Peer Groups may develop any database or Hazard management program for their use, tailored to suit that individual projects needs, provided that the solution satisfies the objectives of this Procedure.

9.1.2 Whatever Hazard Log tool is adopted must be under strict configuration control to ensure robust audit trail.

9.1.3 CASSANDRA is a Hazard Management System designed to meet the requirements of Def Stan 00-56 Issue 4 and most other recognised safety management and assessment processes. In addition to recording information about Hazards and accidents, risk classification and control measures, required in the conventional Hazard Log, Cassandra also enables Hazards and accidents to be linked to show their relationships (one-to-many and many-to-many).

10 GUIDANCE

10.1 General Guidance

10.1.1 Since a Hazard Log is a structured way of storing and referencing data and records on Hazards, documenting the Risk Evaluation and other information relating to an equipment or system, clear cross-referencing to supporting documents is essential. The supporting documentation can be either directly embedded or cross-referenced by the Hazard Log.

10.2 Alignment with Environment

10.2.1 The key alignment opportunity in SMP11 is to cross reference Environmental Features against Safety Hazards, so that common issues are identified and where possible assessed together, and to also to ensure that the potential environmental impact of a safety hazard, or a safety impact of an environmental hazard are not overlooked.

10.3 Domain-Specific Guidance and References

10.3.1 Additional guidance on the Hazard Log is contained in the following references:

a. Land Systems: JSP 454 Issue 4:

   i. Part 1 Section 3.3.6

   ii. Part 1 Section 5.2.1

b. Ship Safety Management: (JSP 430 Issue 3):

c. Airworthiness: (JSP 553 1st Edition):

   i. Chapter 4.33.7 (Contains reference to DEF.STAN 00-56)

d. Ordnance, Munitions & Explosives (OME): (JSP 520 Issue 2.0):

   i. Section III (0429)

e. Nuclear Propulsion (JSP 518 Issue 1.2):

   i. Nil

10.4 Guidance for Different Acquisition Strategies

10.4.1 The Hazard Log is required whatever acquisition strategy is adopted.

10.5 Warnings and Potential Project Risks

10.5.1 The relationship between Hazards, accidents and their management through setting and meeting Safety Requirements could be included within the Hazard Log. However, if it is not sufficiently robust or well-structured, this may overload the Hazard Log and obscure the identification and clearance of Hazards. The requirements of this clause are an important part in demonstrating the robustness of evidence of safety and should be clearly documented and referenced

10.5.2 If Hazards are not well defined when they are entered into the Hazard Log, then the rigour enforced by the need for a clear audit trail of changes made, may make it very difficult to maintain the Hazard and Accident records in the most useful structure. An appropriate structure should therefore be designed and agreed before data entry starts.