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 **Hazard Identification** is defined in Def Stan 00-56 Issue 4 as:

> *"*The process of identifying and listing the hazards and accidents associated with a system.*"*

1.1.2 **Hazard Analysis** is defined in Def Stan 00-56 Issue 4 as:

> *"The process of describing in detail the hazards and accidents associated with a system, and defining accident sequences."*

1.1.3 **Hazard Identification and Analysis (HI&A)** is the ongoing process of identifying credible hazards, accidents and accident sequences through the project life cycle. It confirms and extends the Preliminary Hazard Identification and Analysis (see Procedure SMP04 – Preliminary Hazard Identification and Analysis) by including consideration of system design aspects and by developing more details of hazards as the design develops. Hazard Identification and Hazard Analysis are parts of the Risk Management process and they are often conducted together or in direct sequence.

1.1.4 At successive stages of the project and in progressively greater detail, Hazard Identification and Analysis seeks to answer the question:

> *"What Hazards and Accidents might affect this system and how could they happen?"*

2 PROCEDURE OBJECTIVES

2.1.1 The objective of HI&A is to identify in detail all credible hazards and accidents that may arise during the life of the system so that the associated risks can be managed. It provides input to:

a. Refining the safety requirements and criteria in the SRD;

b. Identification of Regulatory requirements;

c. Design decision making;

d. Risk Evaluation;

e. Option selection;

f. Hazard Log;

g. Safety Case Reports for Main Gate and subsequent System Acceptance and Introduction to Service;

h. Identifying any critical areas of safety risk as input to Main Gate.

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.

3.3 Procedure Completion

3.3.1 The Project Safety Manager will be responsible for the completion of the procedure. However, in most cases a large part of the detailed work will be carried out by contractors. In all cases PSC members and other stakeholders should be involved in providing input and agreeing outputs.

3.3.2 Where different contractors are in competition with each other and have carried out separate Hazard Analyses, contractual and managerial arrangements should be made for the output from all to be made available to the successful contractor. This will reduce the likelihood of hazards being missed.

3.3.3 In large or complex projects, the Project Safety Manager must co-ordinate HI&A across the project to ensure that all relevant and credible hazards identified through

HI&A by any party, including those outside the scope of a particular Contractor's control, are captured and managed through the Hazard Log.

4 WHEN

4.1 Production

4.1.1 HI&A is an iterative process, commencing in Assessment and continuing through Demonstration and Manufacture as the design is refined. At each phase the HI&A will be a major input to the Safety Case Report.

4.1.2 In addition, any significant changes in use or application identified during the In-service phase will require HI&A, and HI&A for the disposal phase should be updated with latest information in preparation and planning for disposal.

4.2 Review, Development and Acceptance

4.2.1 Each major update to the HI&A shall be endorsed by the ISA (where the project requires ISA) and the Safety Panel, through endorsement of the Hazard Log and Safety Case Reports for Main Gate, System Acceptance and Introduction to Service.

4.2.2 If HI&A is updated, management measures should ensure that the Hazard Log, Safety Case Report, Safety Case and other dependent activities are also updated.

5 REQUIRED INPUTS

5.1.1 This procedure for HI&A requires inputs from:

a. Outputs from Procedure SMP03 – Safety Planning;

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

c. Outputs from Procedure SMP11 –Hazard Log;

d. Outputs from Procedure SMP12 –Safety Case and Safety Case Report.

5.1.2 The HI&A methods and timing will be defined in the Project Safety Plan, if appropriate by reference to the Contractor's Safety Plan.

5.1.3 The HI&A may use the following reference inputs, as available:

a. Design Description;

b. Preliminary HI&A;

c. URD and Outline SRD;

d. Hazard Checklists (eg appended to Procedure SMP04 – Preliminary Hazard

Identification and Analysis or from individual Safety Management Offices);

e. Relevant Previous Hazard Logs/Analyses

f. Accident and incident history from relevant existing systems in service.

6 REQUIRED OUTPUTS

6.1.1 The primary outputs of the HI&A are the initial Hazards, Accidents and Accident Sequences recorded in the Hazard Log for the project.

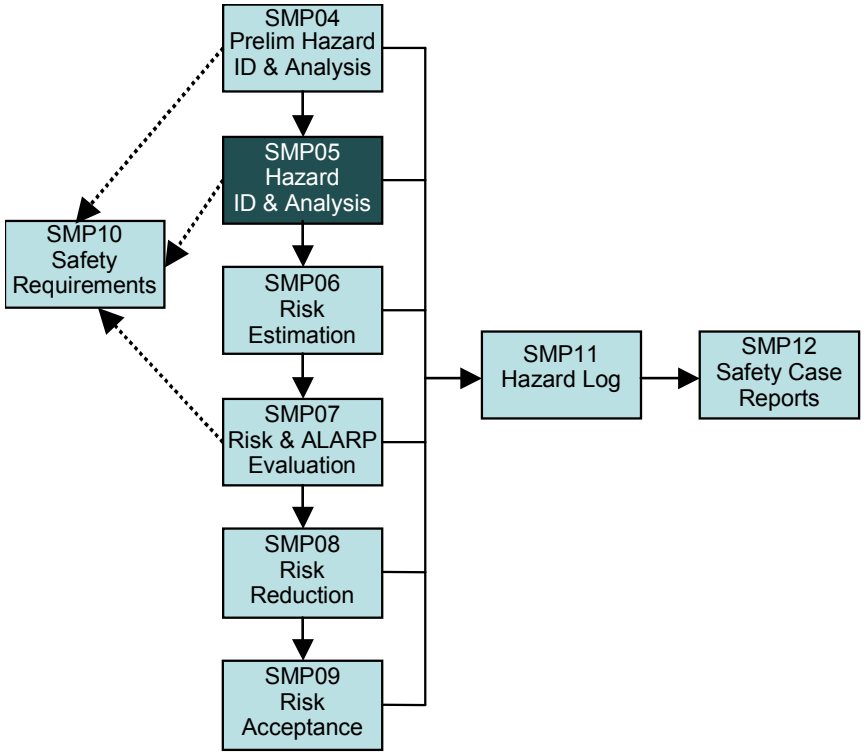
6.1.2 These results form part of the Safety Case body of evidence and may be recorded in a standalone report or as part of a wider report on Safety (eg Safety Assessment Report or Safety Case Report).

7 DESCRIPTION

7.1.1 HI&A provides the basis for all other safety activities on the project. It provides the detailed identification of hazards, the associated accidents and accident sequences. This information then provides the basis for assessing risks and ultimately the acceptability of the system.

7.1.2 The project shall carry out HI&A to identify credible hazards and accidents associated with the system and to determine the related accident sequences. The HI&A shall be reviewed and revised through the life of the project, as the design changes or as more information becomes available. The project shall demonstrate the adequacy of the HI&A process and the suitability of the techniques employed.

7.1.3 The relationship of this activity with other Risk Management activities is illustrated below:



7.2 Method

7.2.1 The form, nature and depth of the HI&A should be proportionate to the complexity and significance of the project, considering any safety-related functionality. There are a number of techniques that may be used to assist in the identification of Hazards and Accidents and in understanding Accident sequences:

a. Hazard Checklist;

b. Accident and History Review;

c. Functional Failure mode and Effects Analysis (FMEA);

d. Structured What If Technique (SWIFT);

e. Hazard and Operability Study (HAZOP).

7.2.2 Different approaches and techniques are best suited to different systems or technologies and no single approach is likely to be sufficient on its own. Usually a combination of complementary techniques should be used in order to maximise the proportion of hazards identified. The adequacy of the technique/s adopted should be justified in the Safety Case. The project should ensure that any Hazard Analyses carried out by contractors use appropriate techniques and are consistent across the project.

7.2.3 The project should ensure that the techniques selected are suitable for identifying hazards and accidents arising from:

a. Systematic and random failures.

b. Credible failures arising from normal and abnormal use in all operational scenarios.

c. Predictable misuse and erroneous operation.

d. Common cause and common mode failures.

e. Interactions between systems, sub-systems or components.

f. The defined operating environment.

g. Procedural, managerial and cultural activities.

h. Storage, transportation, disposal and other such activities.

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.

8.1.2 The Hazard Log is the primary mechanism for recording all Hazards, Accidents and Accident Sequences identified through HI&A. It is a live document, updated with the results of each HI&A as they become available. See Procedure SMP11 – Hazard Log, for more details.

8.1.3 The results of the HI&A should be reported in a form which records the following:

a. The input information used (eg URD version, Concept of Use document, design standard);

b. The approach adopted (eg: tools and techniques used);

c. The people consulted;

d. The Hazards, Accidents and Accident Sequences identified.

8.1.4 These results form part of the Safety Case body of evidence and may be recorded in a standalone report or as part of a wider report on Safety (eg Safety Assessment Report or Safety Case Report).

8.1.5 The Safety Case Report (Procedure SMP12 – Safety Case and Case Report) is where the project should demonstrate the adequacy of the HI&A process and the suitability of the techniques employed.

9 RECOMMENDED TOOLS AND FORMS

9.1.1 Detailed information on tools and techniques is provided in the Safety Manager's Toolkit.

10 GUIDANCE

10.1.1 The project should ensure that Hazard Analyses are carried out in a planned and structured manner throughout the project. In a major project this will involve multiple Analyses for different sub-systems as well as the complete system, and at different stages of design or demonstration. The planning of this must ensure that:

a. Hazards and accidents are identified at times where action can be taken to mitigate or eliminate them most efficiently (ie. at an appropriate point in the design cycle).

b. Comprehensive, up to date hazard analysis is available to support development of the Safety Case Reports.

c. Adequate operational experience (see below) and historical data is available to support HI&A sessions.

10.1.2 HI&A should be undertaken using a combination of techniques with the aim of providing confidence that the greatest number of credible hazards and accidents have been identified taking into account the nature and complexity of the system. This should include the anticipated use in wartime or other operational scenarios. However, an appropriate and proportionate approach should be adopted and the operational scenarios agreed with the Customer.

10.1.3 All available, relevant data should be considered, including accident and incident data from similar systems. Reasonable effort should be made to ensure that all possible Hazards are examined. It is essential that the appropriate team of experts is used in the HI&A process, providing a sound understanding of:

a. The system description;

b. Operational profiles, maintenance, operator and maintainer competencies;

c. The application and limitations of selected HAZID techniques;

d. The existing and/or commonly known Hazards of this or similar types of system;

e. Validity of historical data adjusted to account for its context.

10.1.4 Justification that the selected techniques are sufficient to identify the full range of credible hazards and accidents should be provided in the Safety Case and summarised in the Safety Case Report. The project should ensure that there is sufficient communication of design, technical and operational information to allow HI&A to be carried out effectively. In addition, the credibility of hazards identified should be discussed, together with the possibility of resultant accidents and the consequences of such accidents; it is important that realism is taken into account whilst still ensuring the widest coverage of potential accident sequences. This should include identifying and involving individuals with expertise in specialist areas, where necessary.

10.1.5 The identification of hazards and their associated accident sequences should be a continual, iterative process. Inevitably, new safety requirements will be derived as the system evolves. This highlights the importance of the Hazard Log in tracking the management of hazard-related activities and why the Hazard Log should be created at project inception. [Based on Def Stan 00-56 Issue 4 Part 2].

10.2 Alignment with Environment

10.2.1 The key alignment opportunity in SMP05 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.

10.2.2 It is also important to plan and conduct assessment studies which can meet both safety and environmental evaluation requirements. Where this is not possible, alignment should help ensure that results of safety assessments are reviewed for environmental implications and vice versa.

10.3 Domain-Specific Guidance and References

10.3.1 Additional guidance on HI&A is contained in the following references:

a. Land Systems: JSP 454 Issue 4:

i. Part 2 Section 6.3.4

b. Ship Safety Management: JSP 430 Issue 3:

i. Part 1 Section 11 Safety Cases (11.6)

c. Airworthiness: JSP 553 1st Edition:

i. Chapter *4 (4.3)*

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

i. Chapter 3 Section I

ii. Chapter 4 (0413, 0416 and 0429)

e. Nuclear Propulsion: JSP 518 Issue 1.2

i. Appendix F to Annex A (AF12, AF20)

ii. Appendix H to Annex A (AH08)

iii. Annex G (G08)

10.4 Guidance for Different Acquisition Strategies

10.4.1 The requirements for HI&A do not change for Acquisition conducted through intergovernmental agreements, OCCAR, multilateral or collaborative programmes. It is MOD policy that the same standards are met, and that assurance that these standards have been met can be demonstrated.

10.4.2 Where the project involves a mid-life update, existing history will obviously provide a major input to HI&A. Similarly, where the project is likely to involve COTS or MOTS solutions (including non-UK solutions) the existing history of these solutions provides a starting point. However, in all these cases there is still a need to carry out HI&A to determine whether any new Hazards are introduced by the proposed use in a UK context, through particular safety-related functionality, new interfaces, different support and usage environments, different operational employments, etc.

10.5 Warnings and Potential Project Risks

10.5.1 If inadequate operational and domain knowledge is available for HI&A, it is likely that important hazards will be missed or that unrealistic hazards will be included in the Hazard Log. It can be difficult to correct these errors later in the programme, when important requirements and design decisions have been implemented.

10.5.2 If IPTs do not ensure a controlled and effective exchange of information on Hazards throughout the project, it is likely that there will be areas of design and implementation where lack of awareness will result in higher risk solutions.

10.5.3 A Hazard checklist is useful for most Hazard Analyses, but should not be the only method, of HI&A (except for standard installations whose hazards have been studied in more detail elsewhere). In all other cases some form of structured brainstorming (eg SWIFT or HAZOP) is highly desirable.

10.5.4 When identifying Hazards, the scope should not be restricted to the steady-state operational scenario, but must consider all aspects of the system's life cycle, from installation to final decommissioning and disposal, including Maintenance and Upgrades (ie CADMID). Emergency scenarios and associated Contingency modes of Operation should also be considered.

10.5.5 Absence of a systematic and comprehensive HI&A activity can severely undermine the Risk Management process. In the worst case, this can create an illusion of Safety and a false sense of confidence, and can miss opportunities to eliminate a hazard in the earliest stages of a project when the greatest range of options still exist.