

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 1

<b>0</b>	<b>SHOWING CONFORMANCE</b>
<b>0.1</b>	<b>Options</b>
0.1.1	<p>There are four options to demonstrate conformance when applying this system procedure:</p> <ol style="list-style-type: none"> <li>a. Follow the defined system procedure using the recommended guidance and tools, including allowed variations and options.</li> <li>b. Use an equivalent process and tool set generated elsewhere and document evidence of procedural equivalence.</li> <li>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.</li> <li>d. Where the procedure is considered to be not relevant, document the basis for this decision.</li> </ol>
<b>1</b>	<b>INTRODUCTION</b>
1.1.1	<p><b>Hazard Identification</b> is defined in Def Stan 00-56 Issue 4 as:</p> <p><i>“The process of identifying and listing the hazards and accidents associated with a system.”</i></p>
1.1.2	<p><b>Hazard Analysis</b> is defined in Def Stan 00-56 Issue 4 as:</p> <p><i>“The process of describing in detail the hazards and accidents associated with a system, and defining accident sequences.”</i></p>
1.1.3	<p>Preliminary Hazard Identification and Analysis (PHI&amp;A) is intended to assist projects in determining the scope of the safety activities and requirements. It identifies the main hazards likely to arise from the capability and functionality being provided. It is carried out as early as possible in the project life cycle, providing an important early input to setting Safety requirements and refining the Project Safety Plan.</p>
1.1.4	<p>PHI&amp;A seeks to answer, at an early stage of the project, the question:</p> <p><i>“What Hazards and Accidents might affect this system and how could they happen?”</i></p>
1.1.5	<p>PHI&amp;A has a separate procedure to SMP05 – Hazard Identification and Analysis. This is both to recognise that different techniques may be required, basing the work on function and capability rather than design solution, and also to emphasise the importance of high-level examination at an early stage.</p>

Issue	Authorised by CESO DE&S	ISSUE LEVEL:	Release V2.2s
Approval	Authorised by DG S&E	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 2

<p><b>2</b></p> <p><b>PROCEDURE OBJECTIVES</b></p> <p>2.1.1 The objective of the PHI&amp;A is to identify, as early as possible, the main Hazards and Accidents that may arise during the life of the system. It provides input to:</p> <ul style="list-style-type: none"> <li>a. Identifying any critical areas of Safety risk inherent in the User’s requirement, as input to Initial Gate submission.</li> <li>b. Providing the basis for the Safety Case Report for Initial Gate.</li> <li>c. Scoping the subsequent Safety activities required in the Safety Plan. A successful PHI&amp;A will help to gauge the proportionate effort that is likely to be required to produce an effective Safety Case, proportionate to risks.</li> <li>d. Selecting or eliminating options for subsequent Assessment</li> <li>e. Setting the initial Safety requirements and criteria in the Outline SRD,</li> <li>f. Provides the starting point for subsequent Hazard Analysis (see Procedure SMP05 – Hazard Identification and Analysis).</li> <li>g. Initiate Hazard Log (see Procedure SMP11-Hazard Log).</li> </ul>
<p><b>3</b></p> <p><b>RESPONSIBILITIES</b></p> <p><b>3.1 Accountability</b></p> <p>3.1.1 The IPTL is accountable for the completion of this procedure.</p> <p><b>3.2 Procedure Management</b></p> <p>3.2.1 The IPTL may delegate the management of this procedure to a member (Safety Manager) or members of the IPT.</p> <p><b>3.3 Procedure Completion</b></p> <p>3.3.1 The Project Safety Manager will be responsible for the completion of the procedure. However, for complex projects the IPT may choose to commission advisors or contractors to complete the procedure. In either case, PSC members and other stakeholders should be involved in providing input.</p>
<p><b>4</b></p> <p><b>WHEN</b></p> <p><b>4.1 Initial Production</b></p> <p>4.1.1 PHI&amp;A should be performed as early in the project life cycle as possible in order to obtain maximum benefit by understanding what the Hazards and Accidents are, why and how they might be realised. The PHI&amp;A should be conducted during the Concept</p>

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 3

stage as an input to Initial Gate and outline SRD Production, based on the capability and concept of use defined in the URD.

**4.2 Review, Development and Acceptance**

4.2.1 In principle, PHI&A is a once-off analysis. However, in a complex project with an extended Concept Phase, the PHI&A should be reviewed if there are major changes to the requirements or options being identified.

4.2.2 The PHI&A and any updates shall be endorsed by Safety Panel, through endorsement of the Hazard Log and Safety Case Reports for Main Gate. An endorsed PHI&A shall be available as input to outline SRD development, Safety Case generation and the subsequent Hazard Analysis (in later phases). If the PHI&A is updated, management measures should ensure that these dependent activities are also updated.

**5 REQUIRED inputs**

5.1.1 This procedure for PHI&A requires inputs from:

- a. Outputs from Procedure SMP01 – Safety Initiation;
- b. Outputs from Procedure SMP02 – Safety Committee;
- c. Outputs from Procedure SMP03 – Safety Planning.

5.1.2 The PHI&A method and timing will be defined in the Project Safety Management Plan.

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

- a. URD;
- b. Hazard Checklists (eg from individual Safety Management Offices);
- c. Relevant Previous Hazard Logs/Analyses;
- d. Accident and incident history from relevant existing systems in service.

**6 REQUIRED OUTPUTS**

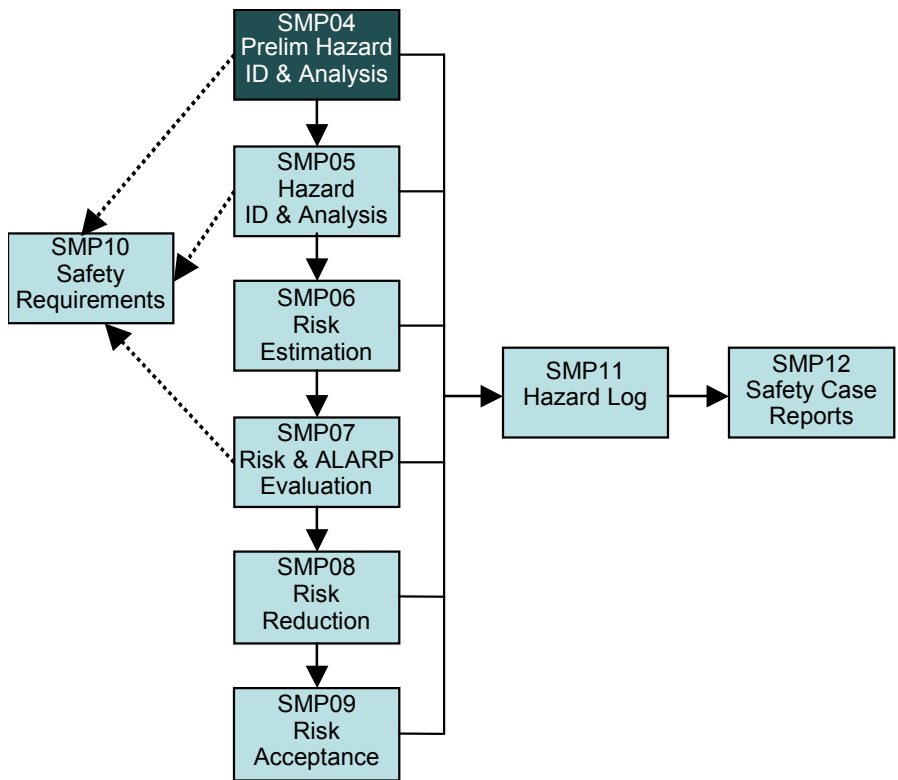
6.1.1 The primary outputs of the PHI&A are the initial Hazards, Accidents and Accident Sequences recorded in the Hazard Log for the project.

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).

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

**7 Description**

7.1.1 PHI&A is an important part of Risk Management, project planning and requirements definition as it helps to identify the main system hazards and helps target where more thorough analysis should be undertaken. The relationship of this activity with other Risk Management activities is illustrated below:



7.1.2 Usually PHI&A is based on a structured brainstorming exercise using Hazard Analysis techniques such as SWIFT (Structured What-If Technique), supported by hazard checklists. A structured approach is necessary to minimise the possibility of missing an important hazard, and to demonstrate that a thorough and comprehensive approach has been applied.

**7.2 Method**

7.2.1 The capability and concept of use as set out in the URD must be reviewed, and potential hazards identified. This preliminary list of hazards should then be assessed for likely impact. From this, the regulatory requirements as well as any standards, with which the requirement will have to comply, and a level of tolerability is to be determined against which risks identified in the subsequent phases might be judged.

7.2.2 The form, nature and depth of the PHI&A should be proportionate to the complexity and significance of the project, considering any safety-related functionality. There are a number of Hazard Analysis/Identification techniques that may be used:

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 5

- 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).
- 7.2.3 Different approaches and techniques are more suited to different systems 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.

- 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 identified through PHI&A. It is a live database or document, updated with the results of each Hazard Analysis as they become available. See Procedure SMP11 – Hazard Log, for more details.
- 8.1.3 The results of the PHI&A should be reported in a form which records the following:
- a. The input information used (eg. URD version, design standard);
  - b. The approach adopted (eg checklist 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 Safety Case Report) is where the project should demonstrate the adequacy of the Hazard Analysis process

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 6

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 Hazard Analysis is fundamental to System Safety Management. If you do not identify a Hazard, you can take no specific action to remove it, or reduce the risk of the Accident(s) associated with it. Absence of a systematic and comprehensive PHI&A activity can thus severely undermine the Risk Evaluation process.

10.1.2 Hazards are diverse, and many different techniques are available for hazard identification and PHI&A. While some techniques have become standard for particular applications, it is not necessary or desirable to specify which approach should be adopted in particular cases. The mix of techniques should be chosen to meet the objectives as efficiently as possible given the available information and expertise.

10.1.3 PHI&A is usually a qualitative exercise based primarily on expert judgement. Most PHI&A exercises involve a group of experts, since few individuals have expertise on all hazards, and group interactions are more likely to stimulate consideration of hazards that even well-informed individuals might overlook. The techniques most suitable for group PHI&A activities are

- a. Structured What If Technique (SWIFT)
- b. Hazard and Operability Study (HAZOP)

10.1.4 In either case hazard checklists and history of similar systems should be available as inputs.

10.1.5 Although both the SWIFT and HAZOP methods are systematic, creative examinations by a multi-disciplinary team, they are dependent on different levels of system information. As such, the most appropriate technique should be selected for any particular system, in order that the Hazard Identification process is effective.

### **10.2 Alignment with Environment**

10.2.1 The key alignment opportunity in SMP04 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

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 7

implications and vice versa.

### **10.3 Domain-Specific Guidance and References**

10.3.1 Additional guidance on PHI&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 8 Safety Cases (8.4)
- c. Airworthiness: JSP 553 1<sup>st</sup> Edition:
  - i. Nil
- d. Ordnance, Munitions & Explosives (OME): JSP 520 Issue 2.0:
  - i. Chapter 3 Section I
  - ii. Chapter 4 Section II (0413, 0418 and 0429)
- e. Nuclear Propulsion: JSP 518 Issue 1.2:
  - i. Nil

### **10.4 Guidance for Different Acquisition Strategies**

10.4.1 The requirements for PHI&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 the process. 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 PHI&A to determine if 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 It is essential the appropriate team of experts are used in the PHI&A process, who together can provide a sound understanding of:

- a. The System description, its boundaries, together with its interactions with its Environment, including systems with which it interfaces and is dependent upon;
- b. Operational profiles, maintenance, operator competencies within a given Functional Environment;
- c. The application and limitations of the selected HAZID techniques;

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP04
<b>SMP04: Preliminary Hazard Identification and Analysis</b>		Page 8

<ul style="list-style-type: none"> <li>d. The existing and/or commonly known Hazards of this or similar systems;</li> <li>e. Validity of historical data adjusted to account for its context.</li> <li>f. If the team contributing to the PHI&amp;A do not contain this expertise, then it is likely that some significant hazards will be missed.</li> </ul> <p>10.5.2 A Hazard checklist is useful for most Risk Evaluations, but should not be the only PHI&amp;A method, except for standard installations whose hazards have been studied in more detail elsewhere.</p> <p>10.5.3 When identifying Hazards, the scope should not be restricted to the steady-state operational scenario, but consider all aspects of the Systems 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.</p> <p>10.5.4 If the PHI&amp;A is not carried out early enough, there is a risk that unrecognised hazards or requirements will be discovered later in the project, by which time it may be more difficult to eliminate or mitigate them.</p>
---

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007