Table of Contents

Table of Contents 1
4. Preliminary Hazard Identification and Analysis 2
4.1. Introduction 2
4.1.1. Definitions 2
4.1.2. Objectives 2
4.2. Procedure 3
4.2.1. Method 3
4.2.2. Records and Project Documentation 3
4.2.3. Warnings and Potential Project Risks 4
4.3. Timing 4
4.3.1. Initial Production 4
4.3.2. Review, Development and Acceptance 5
4.4. Required Inputs 5
4.5. Required Outputs 5
4.6. Annex A - Example Hazard Checklists 5
4.6.1. Hazard Checklists 5
4.6.2. General Hazard Checklist 6
4.6.3. Land Systems Hazard Checklist 8
4.6.4. Sea Systems Hazard Checklist 8
4.6.5. Aviation Hazard Categories 8
4.6.6. Ordnance, Munitions & Explosives Hazard Checklist 9
4.7. Version Control 9
4.7.1. Version 2.3 to 3.0 uplift 9
4.7.2. Version 3.0 to 3.1 uplift 9
4.7.3. Version 3.1 to 3.2 uplift 9
4.7.4. Version 3.2 to 4.0 uplift 9
4.7.5. Version 4.0 to 4.1 Uplift 9
4.7.6. Version 4.1 to 4.2 Uplift 9

4. Preliminary Hazard Identification and Analysis

ASEMS Document Version:
4.2
Effective From:
Friday, 13 May, 2022 - 00:15
Summary:
This procedure provides guidance for conducting a Preliminary Hazard Identification and Analysis in order to determine the scope of the safety requirements for the system.

4.1. Introduction

4.1.1. Definitions

4.1.1.1.

Hazard Identification is defined in Def Stan 00-056 [1] as:

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

Hazard Analysis is defined in Def Stan 00-056 [1] as:

"The process of analysing in detail the hazards and accidents associated with a system."

4.1.2. Objectives

4.1.2.1.

The objective of the PHIA 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:

1. Identifying any critical areas of Safety Risk inherent in the User's requirement, as input to Outline Business Case submission.
2. Providing the basis for the Safety Case Report for Outline Business Case.
3. Scoping the subsequent Safety activities required in the Safety Management Plan. A successful PHIA will help to gauge the effort that is likely to be required to produce an effective Safety Case, proportionate to risks.
4. Selecting or eliminating options for subsequent Assessment
5. Setting the initial Safety Requirements and criteria in the outline System Requirements Document (SRD),
6. Provides the starting point for subsequent Hazard Analysis (see Procedure SMP05 – Hazard Identification and Analysis [2]).
7. Initiate Hazard Log (see Procedure SMP11-Hazard Log [3]).

4.1.2.2.

PHIA 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.

4.1.2.3.

Usually PHIA is based on a structured brainstorming exercise using Hazard Analysis techniques such as Structured What-If Technique (SWIFT) [4], supported by Hazard Checklists [5]. 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. More information can be found in the ASEMS Toolkit.

4.1.2.4.

Preliminary Hazard Identification and Analysis (PHIA) 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 Management Plan (SMP).

4.1.2.5.

Preliminary Hazard Identification and Analysis seeks to answer, at an early stage of the project, the question:

“What Hazards and Accidents might affect this system and how could they happen?”

4.2. Procedure

4.2.1. Method

4.2.1.1.

The Concept of Use (CONUSE) as set out in the User Requirements Document (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 capability will have to comply, can be determined. A level of tolerability against which risks identified in the subsequent phases might then be judged.

4.2.1.2.

The form, nature and depth of the PHIA 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:

1. Hazard Checklist [5];
2. Accident and History Review;
3. Functional Failure Mode and Effects Analysis (FMEA) [6];
4. Structured What If Technique (SWIFT); [4]
5. Hazard and Operability Study (HAZOP) [7].

4.2.1.3.

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 will be used in order to maximise the proportion of hazards identified.

4.2.1.4.

PHIA will usually be a qualitative exercise based primarily on expert judgement. Most PHIA 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 PHIA are:

1. SWIFT [4];
2. HAZOP [7].

4.2.1.5.

Hazards are diverse, and many different techniques are available for PHIA. While some techniques have become standard for particular applications, it is not be necessary or desirable to specify which approach can 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.

4.2.1.6.

In either case Hazard Checklists and history of similar systems will be available as inputs.

4.2.1.7.

Although both the SWIFT [4]and HAZOP [7]methods are systematic, creative examinations made by a multi-disciplinary team, they are dependent on different levels of system information. As such, the most appropriate technique will be selected for any particular system, in order that the PHIA activity is effective.

4.2.2. Records and Project Documentation

4.2.2.1.

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

1. System Requirements Document – for any specific safety requirements;
2. Customer Supplier Agreement – to document agreements on safety information to be delivered by the

Delivery Team;
3. Through Life Management Plan;
4. Safety elements of Outline Business Case and Full Business Case submissions.

4.2.2.2.

The Hazard Log [8] is the primary mechanism for recording all hazards identified through PHIA. It is a live database or document, updated with the results of each Hazard Analysis as they become available. See Procedure SMP11 – Hazard Log [3], for more details.

4.2.2.3.

The results of the PHIA should be reported in a form which records the following:

1. The input information used (e.g. User Requirements Document version, design standard);
2. The approach adopted (e.g. checklist used);
3. The people consulted;
4. The Hazards, Accidents and Accident Sequences identified.

4.2.2.4.

The Safety Case Report (Procedure SMP12 – Safety Case and Safety Case Report [9]) is where the project will demonstrate the adequacy of the Hazard Analysis process and the suitability of the techniques employed.

4.2.3. Warnings and Potential Project Risks

4.2.3.1.

It is essential the appropriate team of experts are used in the PHIA process, who together can provide a sound understanding of:

1. The System description, its boundaries, together with its interactions with its Environment, including systems with which it interfaces and is dependent upon;
2. Operational profiles, maintenance, operator competencies within a given Functional Environment;
3. The application and limitations of the selected Hazard Identification (HAZID) techniques;
4. The existing and/or commonly known hazards of this or similar systems;
5. Validity of historical data adjusted to account for its context;
6. If the team contributing to the PHIA do not contain this expertise, then it is likely that some significant hazards will be missed.

4.2.3.2.

PHIA 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 PHIA activity can thus severely undermine the Risk Evaluation process.

4.2.3.3.

A Hazard Checklist [5] is useful for most Risk Evaluations, but should not be the only PHIA method, except for standard installations whose hazards have been studied in more detail elsewhere.

4.2.3.4.

When identifying hazards, the scope should not be restricted to the steady-state operational scenario, but consider all aspects of the Systems Lifecycle, from installation to final decommissioning and disposal, including Maintenance and Upgrades (i.e. CADMID). Emergency scenarios and associated Contingency Modes of Operation will also be considered.

4.2.3.5.

If the PHIA 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.

4.3. Timing

4.3.1. Initial Production

4.3.1.1.

PHIA should be performed as early as 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 PHIA should be conducted during the Concept stage as an input to Outline Business Case and outline Statement of requirement Documentation Production, based on the CONUSE defined in the URD.

4.3.2. Review, Development and Acceptance

4.3.2.1.

In principle, PHIA is a one off analysis. However, in a complex project with an extended Concept Phase, the PHIA will be reviewed if there are major changes to the requirements or options being identified.

4.3.2.2.

The PHIA and any updates shall be endorsed by the PSC, through endorsement of the Hazard Log and Safety Case Reports for Full Business Case. An endorsed PHIA shall be available as an input to outline the Statement of Requirement Document development, Safety Case generation and the subsequent Hazard Analysis (in later phases). If the PHIA is updated, management measures will ensure that these dependent activities are also updated.

4.4. Required Inputs

4.4.0.1.

This procedure for PHIA requires inputs from:

1. Outputs from Procedure SMP01 – Safety Initiation [10];
2. Outputs from Procedure SMP02 – Safety Committee [11];
3. Outputs from Procedure SMP03 – Safety Planning [12].

4.4.0.2.

The PHIA method and timing will be defined in the Project SMP.

4.4.0.3.

The PHIA may use the following reference inputs, as available:

1. User Requirements Document;
2. Hazard Checklists [5] ;
3. Relevant Previous Hazard Logs/Analysis;
4. Accident and incident history from relevant existing systems in service.

4.5. Required Outputs

4.5.0.1.

The primary outputs of the PHIA are the initial Hazards, Accidents and Accident sequences recorded in the Hazard Log [8] for the project.

4.5.0.2.

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 (e.g. Safety Case Report).

4.5.0.3.

Detailed information on tools and techniques is provided in the ASEMS Toolkit.

4.6. Annex A - Example Hazard Checklists

4.6.1. Hazard Checklists

4.6.1.1.

This guidance contains information which should be used to generate Hazard Checklists [5] for use in the conduct of PHIA to identify possible Hazards and Accidents which might be associated with a system. Any Hazard checklist should be used in a “brainstorming”, imaginative way to stimulate discussions between stakeholders who have a good understanding of the system, its context and usage/maintenance environment. Checklist application in a narrow way or by those with a vague appreciation of the system will be very much less effective.

4.6.2. General Hazard Checklist

4.6.2.1.

The following headings should be used as a basis for the compilation of checklists to assist Preliminary Hazard Listing and PHIA. The contents of the annex are not exhaustive. The objective is to identify hazards, their direct and indirect causes, and significant contributing factors.

4.6.2.2.

Hazardous components:

1. Flammable substances; e.g. solid, liquid or gaseous;
2. Lasers;
3. Explosives;
4. Asphyxiants, toxic or corrosive substances;
5. High temperature or cryogenic fluids;
6. Hazardous construction materials;
7. Pressure systems;
8. Electrical sources;
9. Ionising and non-ionising radiation sources;
10. Hydraulic arms or rotational machinery;
11. Other energy sources including those due to motion;
12. Exhaust gases;
13. Passive obstacles;
14. Hazardous surfaces;
15. Cut and puncture projections.

4.6.2.3.

Safety related interfaces between the various elements of the system, e.g.:

1. Material compatibilities;
2. Electromagnetic interference and compatibility;
3. Inadvertent activation;
4. Fire and explosion initiation and propagation;
5. Hardware and software controls.

4.6.2.4.

Factors due to the operating domain, or that the system may add to the operating domain, e.g.:

1. Drop;
2. Shock and vibration, including seismic;
3. Extreme temperatures, pressures and climatic conditions;
4. Noise;
5. Exposure to toxic or corrosive substances;
6. Fire or explosion;
7. Insect, rodent or mould damage;
8. Foreign bodies and dust;
9. Electrostatic discharge including lightning;
10. Electromagnetic interference;
11. Ionising and non-ionising radiation, including laser radiation;
12. Faults in supporting systems; e.g. power supplies, hydraulic systems;
13. Exhaust gases.

4.6.2.5.

Operating, test, maintenance and emergency procedures, e.g. :

1. Operation under peace, exercise, war;
2. Human factors considerations;
3. Adequacy and effectiveness of instruction, training and rehearsal;
4. Health hazards;
5. User error, including failure to activate;
6. Effect of factors such as equipment layout, ergonomics and lighting;
7. Potential exposure to toxic materials, noise and radiation;
8. Life support systems;
9. Crash safety, egress, rescue and survival;
10. Repair and salvage.

4.6.2.6.

Enemy action, e.g. :

1. Hostile acts;
2. Inaction of active protective systems;
3. Ineffectiveness of passive protective systems;
4. Damage containment.

4.6.2.7.

Damage control measures, e.g. :

1. Damage containment;
2. Damage repair;
3. Hazard containment;
4. Egress, rescue and survival.

4.6.2.8.

Facilities, e.g. :

1. Support equipment;
2. Training;
3. Provisions for storage of hazardous materiel;
4. Provisions for assembly of hazardous materiel;
5. Provisions for proof testing of hazardous materiel.

4.6.2.9.

The adequacy of safety related equipment, safeguards and failure containment measures, e.g. :

1. Fire suppression systems;
2. Relief valves;
3. Energy containment vessels;
4. Electrical protection;
5. Toxic substance control;
6. Electrical, air and hydraulic supplies;
7. Personal protective equipment;
8. Ventilation;
9. Noise or radiation barriers;
10. Alarms and warnings.

4.6.2.10.

The defences against common mode failure, e.g. :

1. Systems redundancy and diversity;
2. Interlocks;
3. Fail safe design.

4.6.2.11.

Compliance with systems safety guidelines and standards, e.g. :

1. Understanding of systems by personnel;
2. Incident recording and monitoring, including near misses;
3. Operator deviation;
4. Design deviation;
5. Deviation in supervision and checking;
6. Component substitution.

4.6.2.12.

Threats to programmable electronic systems, e.g. :

1. Viruses;
2. Security breaches.
3. Electromagnetic interference e.g. interruption to signals used for determining location or timing (applications such as; navigation (e.g. GPS receivers), targeting, synchronisation etc.)

4.6.3. Land Systems Hazard Checklist

4.6.3.1.

If there are no domain-specific hazard checklists, use generic checklists.

4.6.4. Sea Systems Hazard Checklist

4.6.4.1.

Naval Authority Key Hazards:

1. Surface Ship Stability;
2. Surface Ship Structural Strength;
3. Surface Ship Escape and Evacuation;
4. Fire Safety (Ship and Submarine);
5. Propulsion and Manoeuvring Systems (Ship and Submarine);
6. Submarine Stability;
7. Submarine Structural Strength;
8. Submarine Manoeuvring and Control;
9. Submarine Atmosphere Control;
10. Submarine Watertight Integrity.

4.6.5. Aviation Hazard Categories

4.6.5.1.

Hazard category	Key hazards assigned to hazard category
1. Fire	• Fire
2. Explosion	• Explosion
3. Disruption	• Structural break up • EMC • Deliberate 3rd party • Incompatibilites (procedures/interoperability)
4. Human performance	• Design performance and handling characteristics of aircraft and systems in the air or on the ground. • Crew incapacitation • Congestion • Inappropriate competence • Inexperience • Inappropriate/Inadequate communication • Inadequate procedure • Unfit for duty • Lack of currency • In-discipline • Inadequate supervision • Human capacity Workload
5. Operating hazard	• Natural operating hazards • Man-made operating hazards • Inadvertent 3rd party
6. Survival	• Post-accident survival
7. Environment*	• Noise • Vibration • Hazardous materials • Pollution • Emissions

* Assessment of environmental impacts should take place through the application of POEMS.

4.6.6. Ordnance, Munitions & Explosives Hazard Checklist

4.6.6.1.

See AOP-15 Ed3 (STANAG 4297 Ed2) “Guidance on the Assessment of the Safety and Suitability for Service of Non-Nuclear Munitions for NATO Armed Forces [1].”

4.7. Version Control

4.7.1. Version 2.3 to 3.0 uplift

4.7.1.1.

Major uplift from the Acquisition System Guidance (ASG) to online version. POEMS has undergone major revision. Refer to the POEMS Transition Document for details.

4.7.2. Version 3.0 to 3.1 uplift

4.7.2.1.

A minor uplift to correct spelling, grammar, and to remove some duplication of text

4.7.3. Version 3.1 to 3.2 uplift

4.7.3.1.

Reference to 'Safety Manager's Toolkit' amended to 'ASEMS Toolkit' following the release of the Sustainable Procurement Tool.

4.7.4. Version 3.2 to 4.0 uplift

4.7.4.1.

Major uplift:

- Further guidance is now part of the main procedure
- Restructure the SMP into a format consistent with all other SMPs
- An Annex A for hazard checklists, this inlcudes examples for Land systems, Sea systems, Ammunition and Ordnance, Munitions & Explosives hazards
- Records and Documentation have been moved from Required Outputs to the main procedure.
- Paragraphs on responsibilities and alignment with Environment have been removed and included with the POSMS introduction.

4.7.5. Version 4.0 to 4.1 Uplift

4.7.5.1.

Minor amendment to replace reference to Initial Gate and Main Gate and change these to Strategic Outline case, Outline Business Case and Full Business Case. This change brings terminology in line with JSP 655.

4.7.6. Version 4.1 to 4.2 Uplift

4.7.6.1.

Addition to guidance of Threats to programmable electronic systems, at part c, within General Hazard Checklist.

Links
[1] https://www.asems.mod.uk/ExtReferences
[2] https://www.asems.mod.uk/guidance/posms/smp05
[3] https://www.asems.mod.uk/guidance/posms/smp11
[4] https://www.asems.mod.uk/toolkit/swift

[5] https://www.asems.mod.uk/toolkit/hazard-checklist
[6] https://www.asems.mod.uk/toolkit/fmeafmeca
[7] https://www.asems.mod.uk/toolkit/hazop
[8] https://www.asems.mod.uk/toolkit/hazard-log
[9] https://www.asems.mod.uk/guidance/posms/smp12
[10] https://www.asems.mod.uk/guidance/posms/smp01
[11] https://www.asems.mod.uk/guidance/posms/smp02
[12] https://www.asems.mod.uk/guidance/posms/smp03