Table of Contents

5. Hazard Identification and Analysis

ASEMS Document Version:
4.1
Effective From:
Friday, 16 July, 2021 - 00:15
Summary:
This procedure provides guidance through the Hazard Identification and Analysis process, in which all credible Hazards are identified and subsequently analysed in order to establish the associated Accidents and Accident Sequences.

5.1. Introduction

5.1.1. Definitions

5.1.1.1.

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."

5.1.1.2.

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."

5.1.2. Objectives

5.1.2.1.

The objective of HIA 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:

1. Refining the Safety requirements and criteria in the Systems Requirements Document (SRD);
2. Identification of Regulatory requirements;
3. Design decision making;
4. Risk evaluation;
5. Option selection;
6. Hazard Log;
7. Safety Case Reports for Full Buisness Case and subsequent System Acceptance and Introduction to Service;
8. Identifying any critical areas of safety risk as input to Full Business Case.

5.1.2.2.

HIA provides the basis for all other safety activities on the project. This information then provides the basis for assessing risks and ultimately the acceptability of the system.

5.1.2.3.

The project shall carry out HIA to identify credible hazards and accidents associated with the system and to determine the related accident sequences. The HIA 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 HIA process and the suitability of the techniques employed.

5.1.2.4.

Hazard Identification and Analysis (HIA) is the ongoing process of identifying credible Hazards, Accidents and Accident Sequences through the project lifecycle. It confirms and extends the Preliminary Hazard Identification and Analysis (PHIA(see Procedure SMP04 – Preliminary Hazard Identification and Analysis [2])) 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.

5.1.2.5.

At successive stages of the project and in progressively greater detail, HIA seeks to answer the question:

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

5.2. Procedure

5.2.1. Method

5.2.1.1.

The form, nature and depth of the HIA 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:

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

5.2.1.2.

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 will be used in order to maximise the proportion of hazards identified. The adequacy of the technique/s adopted will be justified in the Safety Case. The project should ensure that any HIA carried out by contractors uses appropriate techniques and is consistent across the project.

5.2.1.3.

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

1. Systematic and random failures;
2. Credible failures arising from normal and abnormal use in all operational scenarios;
3. Predictable misuse and erroneous operation;
4. Common cause and common mode failures;
5. Interactions between systems, sub-systems or components;
6. The defined operating environment;
7. Procedural, managerial and cultural activities;
8. Storage, transportation, disposal and other such activities.

5.2.1.4.

The project will ensure that HIA is 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:

1. Hazards and Accidents are identified at times where action can be taken to mitigate or eliminate them most efficiently (i.e. at an appropriate point in the design cycle);
2. Comprehensive, up to date Hazard Analysis is available to support development of the Safety Case Reports;
3. Adequate operational experience (see below) and historical data is available to support HIA sessions.

5.2.1.5.

HIA will 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.

5.2.1.6.

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 HIA process, providing a sound understanding of:

1. The system description;

2. Operational profiles, maintenance, operator and maintainer competencies;
3. The application and limitations of selected HIA techniques;
4. The existing and/or commonly known Hazards of this or similar types of system;
5. Validity of historical data adjusted to account for its context.

5.2.1.7.

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 HIA 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.

5.2.1.8.

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 00-056 [1]).

5.2.2. Records and Project Documentation

5.2.2.1.

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.

5.2.2.2.

The Hazard Log is the primary mechanism for recording all Hazards, Accidents and Accident Sequences identified through HIA. It is a live document, updated with the results of each HIA as they become available. See Procedure SMP11 – Hazard Log [7], for more details.

5.2.2.3.

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

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

5.2.2.4.

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 (e.g. Safety Assessment Report or Safety Case Report).

5.2.2.5.

The Safety Case Report (Procedure SMP12 – Safety Case and Safety Case Report [8]) is where the project will demonstrate the adequacy of the HIA process and the suitability of the techniques employed.

5.2.3. Warnings and Potential Project Risks

5.2.3.1.

If inadequate operational and domain knowledge is available for HIA, 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.

5.2.3.2.

If Delivery Teams 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.

5.2.3.3.

A Hazard Checklist is useful for most HIA, but should not be the only method used (except for standard installations whose hazards have been studied in more detail elsewhere). In all other cases some form of structured brainstorming (e.g. Structured What if Technique or Hazard Operability Study) is highly desirable.

5.2.3.4.

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 (i.e. the acquisition lifecycle). Emergency scenarios and associated Contingency modes of Operation should also be considered.

5.2.3.5.

An absence of a systematic and comprehensive HIA activity could 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.

5.3. Timing

5.3.1. Initial Production

5.3.1.1.

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

5.3.1.2.

In addition, any significant changes in use or application identified during the In-Service phase will require HIA, and HIA for the Disposal phase should be updated with latest information in preparation and planning for disposal.

5.3.2. Review, Development and Acceptance

5.3.2.1.

Each major update to the HIA should be endorsed by the Independent Safety Auditor (where the project appoints an Independent Safety Auditor) and the PSC, through endorsement of the Hazard Log and Safety Case Reports for Full Business Case, System Acceptance and Introduction to Service.

5.3.2.2.

As HIA is updated, management measures will ensure that the Hazard Log, Safety Case and other dependent activities are also updated.

5.4. Required Inputs

5.4.0.1.

This procedure for HIA requires inputs from:

1. Outputs from Procedure SMP03 – Safety Planning [9];
2. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [2];
3. Outputs from Procedure SMP11 – Hazard Log [7];
4. Outputs from Procedure SMP12 – Safety Case and Safety Case Report [8].

5.4.0.2.

The HIA methods and timing will be defined in the Project Safety Management Plan (SMP), if appropriate by reference to the contractor's SMP.

5.4.0.3.

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

1. Design Description;
2. Preliminary HIA;
3. User Requirements Document and Outline System Requirements Document;
4. Hazard Checklists (e.g. appended to Procedure SMP04 – Preliminary Hazard Identification and Analysis [2] or from individual Operating Centre Programme Management Offices);
5. Relevant Previous Hazard Logs/Analysis;
6. Accident and incident history from relevant existing systems in service.

5.5. Required Outputs

5.5.0.1.

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

5.5.0.2.

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).

5.5.0.3.

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

5.6. Version Control

5.6.1. Version 2.3 to 3.0 uplift

5.6.1.1.

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

5.6.2. Version 3.0 to 3.1 uplift

5.6.2.1.

Minor amendments to include removal of spelling mistakes, poor grammar and duplicated text.

5.6.3. Version 3.1 to 3.2 uplift

5.6.3.1.

Reference to 'Safety Managers Toolkit' amended to 'ASEMS Toolkit' following the release of the SP Tool.

5.6.4. Version 3.2 to 4.0 uplift

5.6.4.1.

The content of this SMP has been standardised and duplication of such items as Responsibilities has been removed.

5.6.5. Version 4.0 to 4.1 Uplift

5.6.5.1.

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.

Links
[1] https://www.asems.mod.uk/ExtReferences
[2] https://www.asems.mod.uk/guidance/posms/smp04
[3] https://www.asems.mod.uk/toolkit/hazard-checklist
[4] https://www.asems.mod.uk/toolkit/fmeafmeca
[5] https://www.asems.mod.uk/toolkit/swift
[6] https://www.asems.mod.uk/toolkit/hazop

[7] https://www.asems.mod.uk/guidance/posms/smp11
[8] https://www.asems.mod.uk/guidance/posms/smp12
[9] https://www.asems.mod.uk/guidance/posms/smp03