Table of Contents

6. Risk Estimation

ASEMS Document Version:
4.0
Effective From:
Thursday, 1 August, 2019 - 00:15
Summary:
This procedure provides guidance through development of the Hazards and Accidents identified previously, to estimate the level of Safety Risk posed by each.

6.1. Introduction

6.1.1. Definitions:

6.1.1.1.

Risk Estimation is defined in Def Stan 00-056 [1]:

"The systematic use of available information to estimate risk."

6.1.2. Objectives

6.1.2.1.

The objective of Risk Estimation is to determine the likelihood and consequences of individual Hazards and Accidents, and the overall aggregation of Safety Risk for the project. It provides input to:

1. Refining the Safety Requirements and criteria in the SRD;
2. Design decision making;
3. Risk Evaluation;
4. Option selection;
5. Hazard Log;
6. Safety Case Reports;
7. Identifying any critical areas of Safety Risk as input to Main Gate.

6.1.2.2.

Risk Estimation should determine (quantitatively or qualitatively) the Risk consequences of individual Hazards, Accidents and Accident Sequences. It provides the basis for assessing risks against requirements, the needs for Risk Reduction, the selection between alternative options on safety grounds and ultimately the acceptability of the system.

6.1.2.3.

The project should carry out Risk Estimation to systematically determine the severity of the consequence and the likelihood of occurrence for the Hazards and Accidents, within each Accident Sequence. The project should determine systematically the overall risk posed by the system.

6.1.2.4.

The project should demonstrate the effectiveness of the Risk Estimation process and the suitability of the techniques employed. All assumptions, data, judgements and calculations underpinning the analysis shall be recorded in the Safety Case, such that the analysis can be reviewed in detail.

6.1.2.5.

The Risk Estimation will be reviewed and revised through the life of the contract, as the design changes or as information becomes available.

6.1.2.6.

Risk Estimation estimates the level of risk posed by each accident (and through the Accident Sequences, the associated Hazards) identified in the Hazard Identification and Analysis (HIA (see SMP05 – Hazard Identification and Analysis [2])). This provides a basis for assessing whether the risk is acceptable.

6.1.2.7.

Like HIA, this is usually an iterative process, becoming more detailed as the design develops, and often involves considerable detailed work by the contractor to provide the evidence necessary to support the isk and ALARP evaluation and the Safety Case.

6.1.2.8.

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

“What level of Safety Risk is posed by the identified Accidents, individually and in total?”

6.2. Procedure

6.2.1. Method

6.2.1.1.

Once the process of HIA is complete, the next step is to determine the likelihood and consequences of each scenario. This will enable the risk of each identified situation to be assessed.

6.2.1.2.

Where contractors are carrying out all or part of the Risk Estimation, the Project Safety Manager will ensure that a consistent and coherent approach is adopted by all parties, and that contractors have access to MOD sources of in-service data and experience to underpin probability and consequence estimates.

6.2.1.3.

In addition to addressing individual risks, the aggregation of risk is considered. The total risk due to all causes can then be determined.

6.2.1.4.

The project should demonstrate the effectiveness of the Risk Estimation methodology within the Safety Case. If sufficiently accurate, suitable and complete data is available and the risks posed by the system are high or uncertain (e.g. novel technology), a quantitative methodology may be adopted either for the entire system or for specific areas. Otherwise a qualitative methodology will be used.

6.2.1.5.

Where Cost-Benefit Analysis will be used as part of the Risk Evaluation, the project will adopt a quantitative methodology for Risk Estimation.

6.2.1.6.

For each Accident Sequence, the Risk Estimation will be sufficiently detailed and robust to demonstrate that the risk has not been underestimated or insufficiently understood. Risk Estimation should be based on objective data where possible. Where data is used, sensitivity analysis should be applied. Where data cannot be obtained, or is of limited applicability, subjective judgement may be used, but will be used cautiously and subject to expert scrutiny. Any such judgements or any assumptions made during the analysis should be documented in the Safety Case.

6.2.1.7.

Risk Estimation is an iterative process. As the development of the system progresses through its life, Accident Sequences should be re-examined to ensure that the Risk Estimation remains valid. Furthermore, additional hazards will undoubtedly be identified that need to be addressed.

6.2.1.8.

Identified Accidents should be systematically evaluated to estimate their severity and likelihood of occurrence for all possible events, as far as is reasonably practicable. This severity of a hazard’s consequence should be predicted in terms of harm to personnel, the platform, its equipment and the effect on others who may be affected. The likelihood of occurrence should be calculated using engineering judgement or on the basis of past experience and precedent.

6.2.1.9.

The risk should then be estimated either quantitatively or a qualitatively from the product of the

consequence and its likelihood. The factors of past experience and precedent should be used to influence how the individual risks are ranked and can be used to benchmark or “reality check” the risk levels estimated. This approach is of particular importance when considering societal perceptions, for hazards that might have otherwise received a lower risk ranking.

6.2.1.10.

Across DE&S projects, the technique most commonly used for this purpose is the Safety Risk Classification Matrix (or Risk Matrix), which maps values for probability (quantitative or qualitative) and consequence onto a matrix to establish a representation of the level of Risk. The following sections provide guidance on the use of Risk Matrices and explain the underlying principles; there is also a leaflet dedicated to Risk Matrices in the ASEMS Toolkit. However, it is emphasised that Delivery Teams should consider their own projects and optimise each element to meet their specific situation.

6.2.1.11.

The basic principles are described below:

1. Each accident severity should be categorised during Risk Estimation. Table 6.1 provides typical definitions but, if these definitions are not appropriate for the system being considered, they may be modified to include other aspects such as loss of system or platform, or different groups of people who may be harmed. The definitions should be agreed by the Project Safety Committee and the accident severity categories used for the system should be recorded in the Hazard Log.

6.2.1.12.

Category	Definition
Catastrophic	Multiple deaths
Critical	A single death; and/or multiple severe injuries or severe occupational illnesses
Marginal	A single sever injury or occupational illness; and/or multiple minor injuries or minor occupational illnesses
Negligible	At most a single minor injury or minor occupational illness

Table 6.1 Accident severity categories

6.2.1.13.

2. Table 6.2 illustrates how probabilities may be categorised during Risk Estimation but again, if the definitions are not appropriate for the system being considered they should be modified to reflect the specific application. Where appropriate, numerical probabilities may be assigned to each category, by taking into account the operational profile of the system and the population at risk. Definitions should be agreed by the Project Safety Committee and the probability categories used for the system should be recorded in the Hazard Log.

6.2.1.14.

Accident Frequency	Occurence *during operational life considering all instances of the system*
Frequent	Likely to be continually experienced
Probable	Likely to occur often
Occasional	Likely to occur several times
Remote	Likely to occur some times
Improbable	Unlikely, but may exceptionally occur
Incredible	Extremely unlikely that the event will occur at all, given the assumptions recorded about the domain and the system

Table 6.2 Probability Ranges

6.2.1.15.

3. The outputs of Tables 6.1 and 6.2 are then used to populate a Risk Matrix, such as the one illustrated in Table 6.3. This shows the risk class of each accident severity/probability combination and should be agreed by the Project Safety Committee and recorded in the Hazard Log. For the purpose of the Accident Risk Classification Scheme, Accidents are considered single events. Any subsequent changes made to the Risk Matrix will also be agreed by the Project Safety Committee and the Hazard Log will be updated.

6.2.1.16.

	Catastrophic	**Critical**	**Marginal**	**Negligible**
Frequent	**A**	**A**	**A**	**B**
Probable	**A**	**A**	**B**	**C**
Occasional	**A**	**B**	**C**	**C**
Remote	**B**	**C**	**C**	**D**
Improbable	**C**	**C**	**D**	**D**
Incredible	**C**	**D**	**D**	**D**

Table 6.3 Example Risk Classification Scheme

6.2.1.17.

4. The resultant risk classifications are not a measure of risk but can be used to rank risks and focus resources and design effort to achieve the optimum balance between capability and safety performance. A risk that has been deemed high (A or B) needs more robust scrutiny than more acceptable levels of Risk (C and D). The same approach can be applied to the in-service management of equipment and at the same time using the classification to ensure the correct level of attention and monitoring is given to Risks. Tables 6.4 and 6.5 give some guidance on the level of management activity expected for risks of various classifications.

6.2.1.18.

5. The tolerability of risk classes can also be categorised using a Risk Class table such as that shown in Table 6.4, with mandated actions specified for each class of risk defined in a table such as that represented by Table 6.5.

6.2.1.19.

Risk Class	**Interpretation**
Class A	Intolerable unless there are exceptional reasons for the activity to take place
Class B	Undesirable, and **should** only be accepted when risk reduction is impracticable

Class C	Tolerable with the endorsement of the Project Safety Committee
Class D	Tolerable with the endorsement of the normal project reviews

Table 6.4 Risk Class Table

6.2.1.20.

Risk Class	In procurement	In service
A	The assessment and subsequent mitigations should be subjected to independent review. Where the potential consequences are likely to involve multiple deaths independent analysis of the assessment should be considered. If it is not feasible to mitigate risks and they are taken on by the operator agreement must be reached at 2* level with the Front Line Top Level Budget, and managed through the Project Safety Committee.	Risks classified at this level before mitigation should be closely monitored even if mitigations have reduced the residual risk to an acceptable level. If such risks are to be/have been taken on and mitigated by process or procedure by the operator, agreement at 2* level with the Front Line Top Level Budget must be recorded.
B and C	Risks must be justified a ALARP. A clear agreement must be made with the Front Line Command Top Level Budget authority responsible for the equipment, as a stakeholder on the Project Safety Committee, that the risks and the mitigation requirements are accepted and understood.	B class risks require continuous monitoring. An active programme should be in place to reduce the risk at the first opportunity. C class risk risks need to be monitored through regular reviews and opportunity to reduce the risk taken as resources and programmes permit.
D	Accepted through normal project reviews by all stakeholders through the Project Safety Committee.	Subjected to regular planned reviews by the Project Safety Committee and monitoring of DRACAS (Data Reporting, Analysis and Corrective Action System) and accident reports, by the Project Safety Committee.

Table 6.5 Risk Management Actions

6.2.1.21.

Risk Estimations are based upon calculations which have used a number of approximations or assumptions such as usage. These approximations may include an assessment of how often an event will occur, which

may never have actually happened but can be foreseen and consequently these results must be treated with caution. However, the band widths for frequency and tolerability are wide and generally the accuracy should be sufficient to put risks in an appropriate category. Sensitivity analysis should be performed to show whether small variations in the inputs to risk calculations would have an effect on the outcome. When the accuracy of the input data is questionable, this can help give assurance that the right classification has been made. In the final analysis, what is important is that possible accidents are identified and that appropriate and proportional mitigation measures are taken which will reduce the possibility of those accidents occurring.

6.2.1.22.

Many techniques for identifying the consequences of individual component/subsystem failures are often used within other Systems Engineering communities (logistics, human factors, reliability etc.). Therefore the results of such assessment studies may be readily available, albeit for a slightly different context or focus. The main techniques are discussed below:

6.2.1.23.

1. Graphical techniques such as Event Tree Analysis (ETA) [3] or Fault Tree Analysis (FTA) [4] can prove very powerful when used on their own or in conjunction with bottom-up techniques such as Failure Modes and Effects and Criticality Analysis (FMECA), Consequence Modelling Analysis and other detailed Risk Evaluation techniques. However, these traditional techniques are poor at studying systems interactions and capturing human error. Techniques such as Environmental Impact Assessment or those from Human Factors Integration including performance studies using Human Reliability Analysis can prove useful supplements for the quantification of risks;

6.2.1.24.

2. Other useful data may come from other disciplines including Quality Assurance, Occupational Health & Safety Risk Evaluations and Availability, Reliability & Maintainability Studies. Availability, Reliability & Maintainability Studies, Human Factors Integration or project Risk Analyses can contribute to Safety Assessment. Information will be shared between different Systems Engineering domains, as it ensures that there is a common understanding of the system and makes best use of available resources as part of lifecycle costing.

6.2.1.25.

3. See the ASEMS Toolkit [5] for further guidance on techniques available for Risk Estimation, together with information on their strengths and weaknesses.

6.2.2. Records and Project Documentation

6.2.2.1.

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 Initial Gate and Main Gate submissions.

6.2.2.2.

The Hazard Log is the primary mechanism for recording the Risk Level estimates identified through Risk Estimation. It is a live document, updated with the results of each Hazard Analysis as they become available. See Procedure SMP11 – Hazard Log [6], for more details.

6.2.2.3.

The results of the Risk Estimation 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.

6.2.2.4.

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 Case Report).

6.2.2.5.

The Safety Case Report (Procedure SMP12 – Safety Case and Safety Case Report [7]) is where the project should demonstrate the adequacy of the Risk Estimation process and the suitability of the techniques employed.

6.2.3. Warnings and Potential Project Risks

6.2.3.1.

The greatest challenge in Risk Estimation is deriving realistic and relevant probabilities of occurrence. Where data is used, it is vital that the data is relevant, accurate and not misinterpreted. Where data does not exist, it is vital any qualitative assessments are based on adequate operational and domain knowledge. The consequences could be significant errors in the assessment and acceptance of risks, potentially leading to accidents in service. At the very least, late identification of errors in Risk Estimation (e.g. by Independent Safety Auditor) could result in delays in acceptance and rework.

6.2.3.2.

Failure to provide adequate Quality Control and traceability of the basis for Risk Evaluation could cause the Safety Case to be undermined, with serious delays to acceptance.

6.2.3.3.

Although Event Trees and Fault Trees are commonly used in assessing overall risks, these are often incorrectly used by inexperienced/non-specialist staff (MOD and contractor) resulting in difficulties at acceptance. Projects should seek adequate assurance of competence of Risk Estimation staff and further guidance is provided in the ASEMS Toolkit.

6.2.3.4.

All analyses must be for the current design standard. If analyses are not kept up to date with design configuration changes, there is a risk that decisions may be based on incorrect information.

6.2.3.5.

Risk Estimation must be as realistic as possible because unduly optimistic or pessimistic assessments will lead to incorrect prioritisation and incorrect targeting of resources. For this reason, unrealistic “worst case” assumptions should not be used. However, sensitivity analysis and adoption of the precautionary principle are necessary when dealing with significant areas of uncertainty.

6.3. Timing

6.3.1. Initial Production

6.3.1.1.

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

6.3.1.2.

In addition, any significant new hazards identified during the remaining phases of the project lifecycle will require Risk Estimation based on the latest information.

6.3.2. Review, Development and Acceptance

6.3.2.1.

Each major update to the Risk Estimation shall be endorsed by the Independent Safety Auditor (where the project appoints an Independent Safety Auditor) and the Project Safety Committee (PSC). This will be demonstrated through endorsement of the Hazard Log and Safety Case Reports for Main Gate, System Acceptance and Introduction to Service.

6.3.2.2.

If Risk Estimation is updated, management measures should ensure that the Hazard Log, Safety Case and other dependent activities are also updated.

6.4. Required Inputs

6.4.0.1.

This procedure for Risk Estimation requires inputs from:

1. Outputs from Procedure SMP03 – Safety Planning [8];
2. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [9];
3. Outputs from Procedure SMP11 – Hazard Log [6];
4. Outputs from Procedure SMP12 – Safety Case and Safety Case Report [7];
5. Outputs from Procedure SMP05 - Hazard Identification and Analysis [2].

6.4.0.2.

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

6.4.0.3.

The Risk Estimation may use the following reference inputs, as available:

1. Design Description;
2. Hazard Analysis;
3. User Requirements Document and Outline System Requirements Document;
4. Relevant Previous Hazard Logs/Analyses;
5. Accident and incident history from relevant existing systems in service.

6.5. Required Outputs

6.5.0.1.

The primary outputs of the Risk Estimation are the estimates of risk level associated with Hazards, Accidents and Accident Sequences recorded in the Hazard Log for the project.

6.5.0.2.

Detailed information on tools and techniques for Risk Estimation is provided in the ASEMS Toolkit [5].

6.6. Version Control

6.6.1. Version 2.3 to 3.0 uplift

6.6.1.1.

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

6.6.2. Version 3.0 to 3.1 uplift

6.6.2.1.

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

6.6.3. Version 3.1 to 3.2 uplift

6.6.3.1.

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

6.6.4. Version 3.2 to 4.0 uplift

6.6.4.1.

A major uplift

- Further guidance is now part of the main procedure
- Restructure the SMP into a format consistent with all other SMPs
- 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.

Source URL: https://www.asems.mod.uk/guidance/posms/smp06

Links
[1] https://www.asems.mod.uk/ExtReferences
[2] https://www.asems.mod.uk/guidance/posms/smp05
[3] https://www.asems.mod.uk/toolkit/event-tree-analysis
[4] https://www.asems.mod.uk/toolkit/fault-tree-analysis
[5] https://www.asems.mod.uk/toolkit
[6] https://www.asems.mod.uk/guidance/posms/smp11
[7] https://www.asems.mod.uk/guidance/posms/smp12
[8] https://www.asems.mod.uk/guidance/posms/smp03
[9] https://www.asems.mod.uk/guidance/posms/smp04