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 **Risk Estimation** is defined in Def Stan 00-56 Issue 4 as:

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

1.1.2 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 (see SMP05 – Hazard Identification and Analysis). This provides a basis for assessing whether the risk is acceptable.

1.1.3 Like Hazard Identification and Analysis, 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 Risk and ALARP Evaluation and the Safety Case.

1.1.4 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?"

2 PROCEDURE OBJECTIVES

2.1.1 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:

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

b. Design decision making;

c. Risk Evaluation;

d. Option selection;

e. Hazard Log;

f. Safety Case Reports;

g. 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 In large or complex projects, the Project Safety Manager must co-ordinate Risk Estimation across the project to ensure that all a consistent and coherent approach to Risk Estimation is adopted by all parties.

4 WHEN

4.1 Production

4.1.1 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.

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

4.2 Review, Development and Acceptance

4.2.1 Each major update to the Risk Estimation 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 Risk Estimation 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 Risk Estimation 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;

e. Outputs from Procedure SMP05 –Hazard Identification and Analysis.

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

a. Design Description;

b. Hazard Analysis;

c. URD and Outline SRD;

d. Relevant Previous Hazard Logs/Analyses;

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

6 REQUIRED OUTPUTS

6.1.1 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.

7 DESCRIPTION

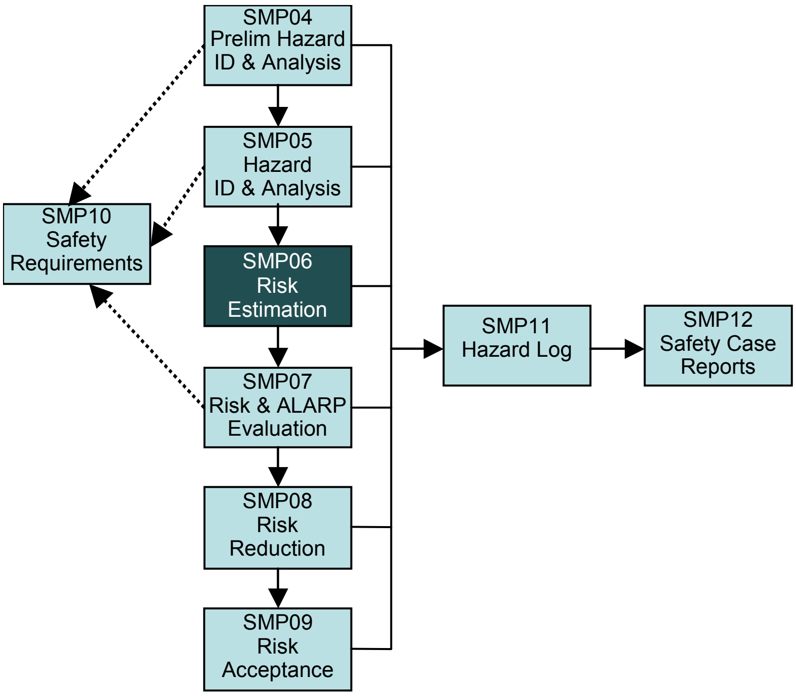
7.1.1 Risk Estimation determines (quantitatively or qualitatively) the risk consequences of individual Hazards, Accidents and Accident Sequences. It provides the basis for assessing risks against requirements, the needs for risk reduction, the selection between alternative options on safety grounds and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

7.1.2 The Project shall 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 shall determine systematically the overall risk posed by the system.

7.1.3 The Project shall 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.

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

7.1.5 The diagram below shows how Risk Estimation relates to other elements of Risk Management in the Safety Management System.



7.2 Method

7.2.1 Once the process of identifying the hazards and accidents, and defining the associated accident sequences, 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.

7.2.2 Where contractors are carrying out all or part of the Risk Estimation, the Project Safety Manager will need to 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

7.2.3 In addition to addressing individual risks, it is important that the aggregation of risk is considered, so that the total risk due to all causes is determined.

7.2.4 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 (eg novel technology), a quantitative methodology may be adopted either for the entire system or for specific areas. Otherwise a qualitative methodology should be used.

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

7.2.6 For each hazard, the Risk Estimation should be sufficiently detailed and robust to demonstrate that the risk has not been underestimated or insufficiently understood. The 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 should 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.

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

8 RECORDS AND PROJECT DOCUMENTATIONS

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 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 for more details.

8.1.3 The results of the Risk Estimation 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 Risk Estimation process and the suitability of the techniques employed.

9 RECOMMENDED TOOLS AND FORMS

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

10 GUIDANCE

10.1.1 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.

10.1.2 The risk can then be estimated either quantitatively or a qualitatively (see 7.2.4) from the product of 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.

10.1.3 The risk estimates are based upon calculations which have used a number of approximations or assumptions for usage, etc. but also an assessment of how often an event will occur, which may never have actually happened but can be foreseen. In these circumstances there will be no mathematical certainty in the results 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.

10.1.4 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:

a. Graphical techniques such as Event Tree Analysis (ETA) or Fault Tree Analysis (FTA) 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 (EIA) or those from Human Factors Integration (HFI) including performance studies using Human Reliability Analysis (HRA) can prove useful supplements for the quantification of risks;

b. Other useful data may come from other disciplines including quality assurance, Occupational Health & Safety (OH&S) workplace Risk Evaluations, Availability, Reliability and Maintainability Studies (AR&M). AR&M, HFI or project Risk Analyses can contribute to Safety Assessment. Sharing information between different systems engineering domains is encouraged, as it ensures that there is a common understanding of the system and makes best use of available resources as part of life-cycle costing.

c. See also the Safety Manager's Toolkit for further guidance on techniques available for Risk Estimation, together with information on their strengths and weaknesses.

10.2 Domain-Specific Guidance and References

10.2.1 Additional guidance on Risk Estimation is contained in the following references:

a. Land Systems: JSP 454 Issue 4:

   i. Part 2 Section 6.4.3

b. Ship Safety Management: JSP 430 Issue 3: (10.5)

c. Airworthiness: JSP 553 1st Edition:

   i. Chapter 4 (4.33)

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

   i. Chapter 3 (0303)

e. Nuclear Propulsion: JSP 518 Issue 1.2

   i. Chapter 4 (0431)
   ii. Chapter 6 (0605)
   iii. Annex G (G08)

10.3 Guidance for Different Acquisition Strategies

10.3.1 The requirements for Risk Estimation 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.

10.3.2 Where the project involves a mid-life update, existing history will obviously provide a major input to Risk Estimation. 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 determine whether likelihoods or consequences are affecter by the proposed use in a UK context, through new interfaces, different support and usage environments, different operational employments, etc.

10.4 Warnings and Potential Project Risks

10.4.1 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 that 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 unexpected accidents in service. At the very least, late identification of errors in Risk Estimation (eg by ISA) could result in delays in acceptance and rework.

10.4.2 Failure to provide adequate quality control and traceability of the basis for Risk Evaluation can undermine the Safety Case and seriously delay acceptance.

10.4.3 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 are advised to seek adequate assurance of competence of Risk Estimation staff.

10.4.4 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.

10.4.5 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.