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

"The systematic process of reducing risk."

1.1.2 **Risk Reduction** is carried out throughout the project, in that efforts should be made at every stage to reduce the risks associated with any recognised hazard. This procedure focuses on risk reduction where Risk Evaluation (Procedure SMP07 – Risk and ALARP Evaluation) has shown that risks do not meet tolerability criteria, and therefore action is required.

1.1.3 The preferred means of eliminating or reducing risk is through design rather than reliance on means such as training and procedures, warning notices or operational limitations for managing residual risks.

1.1.4 **Risk Reduction** seeks to answer the question:

"How can we reduce the level of Safety Risk posed by the identified Accidents, individually and in total?"

1.1.5 This procedure covers the identification and selection of Risk Reduction options, as well as their implementation through changes to the design and the arrangements which will support it through life.

2 PROCEDURE OBJECTIVES

2.1.1 The objective of Risk Reduction is to reduce the likelihood and/or consequences of specific Hazards and Accidents so that the resultant risks can be re-assessed to be Tolerable and ALARP and then Accepted after appropriate management review. It provides input to:

a. Risk Estimation and Evaluation;

b. Hazard Log;

c. Safety Case;

d. Risk Acceptance.

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. The Project Safety Manager should monitor the scope and progress of this work.

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

3.3.3 The Project Safety Manager must also maintain the Project Risk Register up to date in respect of any emerging requirements for Risk Reduction activities, where these may affect project performance or costs.

4 WHEN

4.1 Production

4.1.1 Risk Reduction will take place whenever Risk and ALARP Evaluation identifies an Accident whose risk is either not broadly acceptable or not tolerable and ALARP. Normally this will occur during Assessment, Demonstration or Manufacture, but it will also apply to new Hazards identified in-service.

4.2 Review, Development and Acceptance

4.2.1 Risk Reduction activities carried out by Contractors will be reviewed by the Project Safety Manager.

5 REQUIRED INPUTS

5.1.1 This procedure for Risk Reduction 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;

f. Outputs from Procedure SMP06 –Risk Estimation;

g. Outputs from Procedure SMP07 –Risk and ALARP Evaluation.

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

a. Tolerability Criteria;

b. SRD;

c. Design information;

d. Operation and Maintenance information;

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

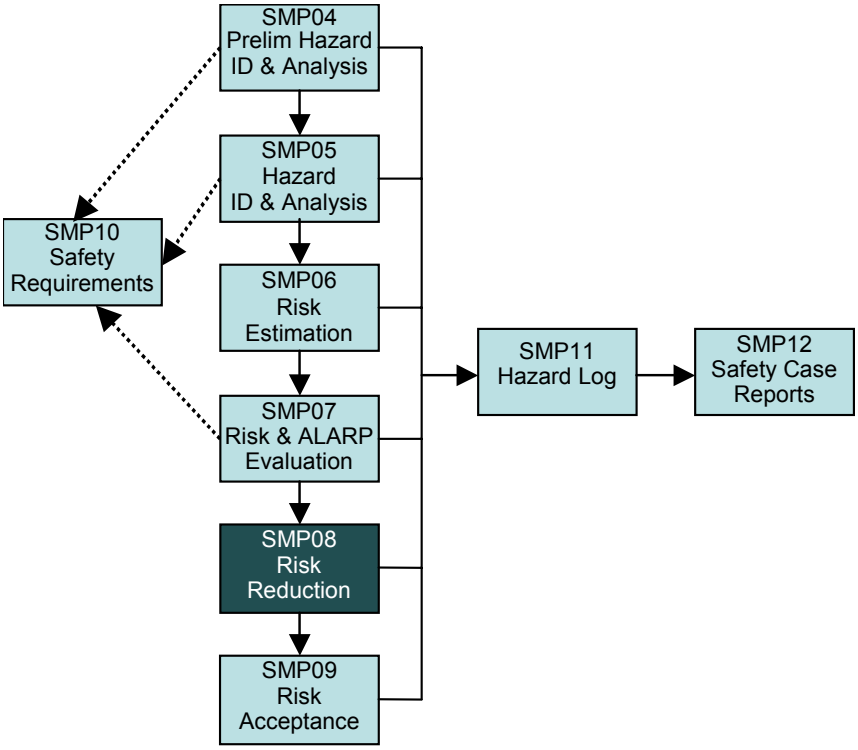
6 REQUIRED OUTPUTS

6.1.1 The primary outputs of the Risk Reduction are changes to the system or the supporting SMS which can reduce the Risk of identified Accidents.

7 DESCRIPTION

7.1.1 Where Risk Evaluation indicates that a risk does not meet tolerability criteria, measures should be put in place to reduce the probability of the hazard resulting in an accident by breaking the accident sequence or reducing the consequences by controlling the accident that occurs. These measures should be recorded in the Hazard Log and arguments justifying the claim made in the Safety Case.

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



7.2 Method

7.2.1 Where the risk from the system is assessed not to meet the tolerability criteria, the Project shall ensure that Risk Reduction is carried out by identifying and implementing a combination of mitigation strategies until the tolerability criteria are met. Mitigation strategies shall be selected according to the following precedence:

a. Eliminate the hazard.

b. Reduce the risk associated with the hazard or accident by implementing engineered mitigation strategies.

c. Reduce the risk associated with the hazard or accident by implementing mitigation strategies based on human factors.

7.2.2 The Project shall demonstrate the effectiveness of the process for identifying and selecting mitigation strategies.

7.2.3 In some cases the mitigation strategies will include new safety requirements (for example new protective functions to be designed in). The Project shall identify the safety requirements that realise the selected mitigation strategies, and ensure that where necessary these are incorporated into the overall safety requirements (see Procedure SMP10 – Safety Requirements and Contracts) and TLMP where appropriate. The Project shall ensure that records are maintained to show traceability between hazards and accidents, and the associated safety requirements.

7.2.4 If, after a risk has been reduced to a level that is ALARP, it is still unacceptable, the IPT Leader shall advise the Capability Customer and Equipment User that the Department is taking on board residual risk that is greater than should be tolerated. Procedure SMP09 defines the actions necessary for Unacceptable risks.

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 process of Risk Reduction should be recorded through the Hazard Log. This will document in detail the audit trail of what Risk Reduction measures were considered and evidence of their implementation, or record the justification of why they were considered either not practicable or not reasonable to adopt.

8.1.3 The Safety Case Report will summarise the Risk Reduction process and include evidence that the reduction has been effective in achieving the tolerability criteria. Also, the Safety Case Report should clearly identify any associated Residual Risks which are not considered to be ALARP.

9 RECOMMENDED TOOLS AND FORMS

9.1.1 The process of Risk Reduction requires review by stakeholders to identify, consider and implement, where necessary, options for reducing risk. The results of the review must be recorded in the Hazard Log.

9.1.2 The identification of Risk Reduction options requires imaginative thinking which may best be conducted in "brainstorming" sessions for the stakeholders. A Risk Reduction checklist such as that provided in Guidance Sheet SMP08/G/01 (Risk Reduction Checklist) of this procedure may be used to guide the brainstorming.

10 GUIDANCE

10.1 General

10.1.1 There are two possible means of achieving Risk Reduction – a reduction in the probability of an accident occurring and/or a reduction in the severity of the consequences of an accident. Strategies to achieve either or both of these should follow the precedence set down in Section 7. Different domains and technology areas often have different detailed interpretations of this list:

a. Eliminate the Hazard, possibly by re-specification or re-design of the system.

b. Incorporation of safety features, extra functions or sub-functions to reduce the probability of occurrence of the event. These features may include redundancy, fall-back modes of operation etc.

c. Revision of operating and training procedures to reduce the probability of error by increasing manning or skill levels, by re-allocating functions or by introducing independent review/checking. Analysis of the effects of operating and training procedures carried out as part of Hazard Analysis should be updated. It should be noted that changes to operating procedures and training will be elements of many risk reduction measures.

d. Incorporation of warning devices. Where it is not possible to apply one of the above methods, warning devices may be introduced. However, when assessing the revised predicted probabilities, the likelihood of human error in a stressful or unusual situation should be carefully considered.

10.1.2 Due regard should be taken of human fallibility wherever a mitigation strategy is implemented through a human being. The failure rate apportioned to the human being in a particular situation should be based on actual experience of the same or similar tasks under the same or similar conditions where that exists. Any use of human failure rates should be supported by a demonstration of the validity of the rates being used.

10.1.3 The selection or rejection of mitigation strategies is not a trivial activity. The Project should demonstrate in the Safety Case Report that all feasible mitigation strategies have been considered in sufficient detail to be able to make meaningful judgements about what is reasonably practicable. The Project should also demonstrate that mitigation strategies have been considered sufficiently early in the design process to allow the design to be modified.

10.1.4 For any mitigation strategy that is employed, the effect on the system should be carefully considered. This should involve re-assessment to review the effect of the mitigation strategy on the system, to see if any new hazards have been introduced which require further examination, or if any existing hazards have been affected. Details of any new hazards or changes to the status of an existing hazard should be recorded in the Hazard Log.

10.1.5 Should there be no apparent way of meeting the tolerability criteria, the Contractor should immediately inform the Project Safety Manager. If there are exceptional circumstances, the risk may be accepted in consultation with the relevant regulatory/certification bodies and/or senior management. Such events should be fully documented in the Hazard Log and Safety Case and justified in terms of the maintenance or optimisation of defence capability. See also responsibilities above.

10.2 Alignment with Environment

10.2.1 The key alignment opportunity in SMP08 is to ensure wherever possible that Risk Reduction measures cover both safety and environmental control of common issues.

10.3 Domain-Specific Guidance and References

10.3.1 Additional guidance on Risk Reduction is contained in the following references:

a. Land Systems: JSP 454:

b. Ship Safety Management: JSP 430:

   i. Section 10 Risk Reduction (10.7)

c. Airworthiness: JSP 553 1st Edition:

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

e. Nuclear Propulsion: JSP 518

   i. Appendix A to Annex J (AJ09, AJ12)

   ii. Appendix A to Annex K (AK10, AK11)

10.4 Guidance for Different Acquisition Strategies

10.4.1 The requirements for Risk Reduction 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.

10.5 Warnings and Potential Project Risks

10.5.1 Risk reduction strategies relying on warning signs or signals are unlikely to be sufficient for risks associated with high consequence accidents. Design solutions are greatly preferable.

10.5.2 Once a Risk Reduction option has been identified and before it is implemented, it should be assessed to ensure that it does not introduce additional Hazards or increase the risks of existing hazards. After implementation, it should be monitored to ensure that it continues to be effective.

10.5.3 If Risk Reduction is not considered sufficiently early in the project life cycle, certain options may be closed off. The cost of implementing design changes and impact on Project timescales become more and more significant.

10.5.4 If the correct authorities are not consulted, then not all Risk Reduction options may be identified for consideration. Furthermore, the practicability and reasonableness of potential Risk Reduction options may not be judged correctly and an invalid ALARP argument or non-optimal Safety may result.

10.5.5 If potential Risk Reduction measures are not actively sought, then it will not be possible to claim ALARP, except on the basis of compliance with recognised good practice.