Table of Contents

8. Risk Reduction

ASEMS Document Version:
4.3
Effective From:
Friday, 16 July, 2021 - 00:15
Summary:
This procedure provides risk reduction guidance for hazards that have not been evaluated as being either tolerable or broadly acceptable and ALARP.

8.1. Introduction

8.1.1. Definitions:

8.1.1.1.

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

“The systematic process of reducing risk.”

8.1.2. Objectives

8.1.2.1.

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 (As Low As Reasonably Practicable) and then Accepted after appropriate management review. It provides input to:

1. Risk Estimation and Evaluation;
2. Hazard Log;
3. Safety Case;
4. Risk Acceptance.

8.1.2.2.

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.

8.1.2.3.

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 [2]) has shown that risks do not meet tolerability criteria, and therefore action is required.

8.1.2.4.

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.

8.1.2.5.

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?”

8.1.2.6.

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.

8.2. Procedure

8.2.1. Method

8.2.1.1.

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 should be selected according to the following precedence:

1. Eliminate the hazard;
2. Reduce the risk associated with the hazard or accident by implementing engineered mitigation strategies;
3. Reduce the risk associated with the hazard or accident by implementing mitigation strategies based on human factors.

8.2.1.2.

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

8.2.1.3.

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 be determined. Different domains and technology areas often have different detailed interpretations of this list. There is a hierarchy of control that should be followed, provided at Annex A.

8.2.1.4.

Due regard will 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.

8.2.1.5.

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.

8.2.1.6.

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.

8.2.1.7.

Should there be no apparent way of meeting the tolerability criteria, the Project Safety Manager should immediately be informed. If there are exceptional circumstances, the risk may be accepted in consultation with the relevant regulatory/certification authorities 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.

8.2.1.8.

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 [3]) and Through Life Management Plan where appropriate. The Project shall ensure that records are maintained to show traceability between hazards and accidents, and the associated safety requirements.

8.2.1.9.

If, after a risk has been reduced to a level that is ALARP, it is still unacceptable, the Project shall formally 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 - Risk Acceptance [4] defines the actions necessary for

unacceptable risks.

8.2.2. Records and Project Documentation

8.2.2.1.

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.

8.2.2.2.

The process of Risk Reduction will 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.

8.2.2.3.

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.

8.2.3. Warnings and Potential Project Risks

8.2.3.1.

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

8.2.3.2.

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 will be monitored to ensure that it continues to be effective.

8.2.3.3.

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.

8.2.3.4.

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.

8.2.3.5.

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.

8.3. Timing

8.3.1. Initial Production

8.3.1.1.

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.

8.3.2. Review, Development and Acceptance

8.3.2.1.

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

8.4. Required Inputs

8.4.0.1.

This procedure for Risk Reduction requires inputs from:

1. Outputs from Procedure SMP03 – Safety Planning [5];
2. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [6];
3. Outputs from Procedure SMP11 – Hazard Log [7];
4. Outputs from Procedure SMP12 – Safety Case and Safety Case Report [8];
5. Outputs from Procedure SMP05 - Hazard Identification and Analysis [9];
6. Outputs from Procedure SMP06 - Risk Estimation [10];
7. Outputs from Procedure SMP07 - Risk and ALARP Evaluation [2].

8.4.0.2.

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

1. Tolerability Criteria;
2. System Requirements Document;
3. Design information;
4. Operation and Maintenance information;
5. Accident and incident history from relevant existing systems in service.

8.5. Required Outputs

8.5.0.1.

The primary outputs of the Risk Reduction are changes to the system or the supporting Safety Management System which can reduce the risk of identified accidents.

8.5.0.2.

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

8.5.0.3.

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 under Further Guidance of this procedure may be used to guide the brainstorming.

8.6. Annex A - Hierarchy of Control and Risk Reduction Checklist

8.6.0.1.

The following paragraphs present a generic checklist for use in identifying options for reducing the risks associated with hazards and accidents relating to a system. Any such 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. Checklists application in a narrow way or by those with an incomplete appreciation of the system will be very much less effective.

8.6.0.2.

The checklist may be used in considering specific hazards and accident sequences identified for the system of interest. Safety Management requires that the Project development should also be subject to overarching good practices, including:

1. Quality;
2. Configuration Management;
3. Design Reviews;
4. Independent Review;
5. Closed-loop problem reporting and resolution;
6. Use of Suitably Qualified and Experienced Personnel;
7. Focus on Safety Culture.

8.6.0.3.

Mitigation strategies should follow the HSE Hierarchy of Control. This is represented in figure 8.1. Further detailed information can be found on ISO 45001: 2018.

Figure 8.1

8.6.0.4.

1. Hazard Elimination Strategies:

1. Eliminate the hazardous substance or procedure;
2. Achieve the required capability by a different means;
3. Reduce the performance required.

8.6.0.5.

2(a). Incorporate Safety Features Strategies (Hazard Controls):

1. Passive control – process inherently cannot run-away (laws of physics etc.);
2. Hazard detection and automatic shutdown (e.g. trip systems, circuit breakers);
3. “Friendly design” such as:
    1. Smooth control system response;
    2. Tolerance of mal-operation (design for recovery);
    3. Inability to mis-assemble;
    4. Design for disposal/dismantling;
    5. Clear status visible on system components (e.g. valves).
4. Increased Integrity of Safety functions, through:
    1. Redundancy;
    2. Diversity (different technology to achieve same function);
    3. Failsafe design;
    4. System monitoring (including Health and Usage Monitoring);
    5. Reallocate function to a different technology;
    6. Increased Safety factors or margins;
    7. Increased Reliability through stress de-rating;
    8. Increased Reliability through improved component quality (including stress screening)
    9. Increased Reliability through improved maintenance;
    10. Improved design for Human Factors for human Safety functions.
5. Increased integrity of Safety functions realised in software, through:
    1. Error detecting/correcting codes (e.g. parity or CRC check, hamming codes);
    2. Full diversity (different software language running on different technology processor);
    3. Software diversity3 (not full diversity as same processor is used);
    4. Defensive programming (ensure that variables cannot go out of range);
    5. Graceful degradation (if there are insufficient resources, prioritise functions and perform high priority ones);
    6. Exception handling/error trapping. Trap run-time errors, then fail safe or reset;
    7. Watchdog.
6. Physical protection measures such as barriers, shields, firewalls, blastwalls, guards, enclosures, interlocks, lock-off systems, exclusion zones, special atmosphere;
7. Remove people from Hazardous area (include making system remotely operated);
8. Reduce number of people exposed to Hazard;
9. Relocate Hazard away from other activities;
10. Controlled entry to Hazardous areas;
11. Automate certain functions or procedures;
12. Reduce Hazard in scale, e.g:
    1. Substitute with a less Hazardous replacement (e.g. alternative substance, alternative technology);
    2. Reduce inventory of Hazardous material;
    3. Reduce Hazardous aspect (e.g. energy, pressure, voltage, temperature, height, speed, toxicity);
13. Attenuation – use material in least Hazardous form (e.g. slurry not dust);
14. Reduce usage rate of Hazardous aspect or frequency of Hazardous activity;
15. Special handling/support equipment or facilities;
16. Weak points/relief systems (e.g. fuses, Pressure Relief Valves, bursting discs);
17. Design for preferential lower severity failure mode (e.g. pressure vessel “leak before break”);
18. Special coatings and treatments (e.g. fire-retardant, slip resistant, anti-bacterial);

19. Personal Protective Equipment (including harnesses);
20. Defence in depth (including physical measures such as containment or bunds for leakage).

8.6.0.6.

2(b). Incorporate Safety Features Strategies (Accident Controls):

1. Emergency plans;
2. Evacuation plans;
3. Safe refuge;
4. Post-accident response;
5. Personal Protective Equipment (including harnesses);
6. First aid provision;
7. Fire-fighting arrangements;
8. Deluge/fire suppression;
9. Survival equipment;
10. Life-saving equipment.

8.6.0.7.

3. Incorporate Warning Devices Strategies:

1. Alarm systems (including failsafe alarms which are normally active);
2. Warning buzzers, beacons and lights;
3. Stop lights.

8.6.0.8.

4. Procedural Strategies:

1. Permit to work system;
2. Additional manpower to support operator during hazardous operations (e.g. safety man, banksman, banksman/slinger etc.);
3. Independent review/checking of Safety-related tasks;
4. Inspection or functional test for dormant failures of Safety functions;
5. Inspection for incipient failures of Safety functions;
6. Human monitoring of Hazard areas;
7. Hazard control procedures in specific circumstances (e.g. de-icing);
8. Increased competence of personnel (e.g. through selection, training);
9. Refresher training to retain competence;
10. Emergency exercises/drills to examine competence.

8.6.0.9.

5. Warning Information Strategies (not suitable as sole strategy for accident sequences with high severity consequences):

1. Warning signs and notices;
2. Warnings in manuals and written instructions.
3. Marked Hazard areas.

8.6.0.10.

Additional considerations:

1. Vulnerability to dependent failures;
2. Failure modes and wartime operation if relevant;
3. Implementing the same function in the software two or more times on the same processor and using voting;
4. Often switched off because code runs too slowly;
5. A process dedicated to monitoring the critical process resets the critical process if it fails;
6. Should be aware of loss of skills;
7. Vulnerability to dependent failures;
8. Use standardised symbols, implemented to minimise probability of incorrect reaction;
9. Use standard notation and language for documented warnings.

8.7. Version Control

8.7.1. Version 2.3 to 3.0 Uplift

8.7.1.1.

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

8.7.2. Version 3.0 to 3.1 Uplift

8.7.2.1.

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

8.7.3. Version 3.1 to 4.0 uplift

8.7.3.1.

Major reorganisation of all SMPs:

- Restructure into a consistent format.
- Responsibilities, Alignment with Environment and guidance for different acquisition strategies have been removed and included in the POSMS summary.
- All further guidance has been placed into the Procedure section, and duplicated text has been removed
- Annex A has been created for the Risk Reduction Checklist and Order of precedence for the Risk Reduction Strategy.

8.7.4. Version 4.0 to 4.1 Uplift

8.7.4.1.

Minor text changes to align with ASP taxonomy.

8.7.5. Version 4.1 to 4.2 Uplift

8.7.5.1.

Text change replacing Project Team with Delivery Team.

8.7.6. Version 4.2 to 4.3 Uplift

8.7.6.1.

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://test.asems.mod.uk/ExtReferences [2] https://www.asems.mod.uk/guidance/posms/smp07 [3] https://www.asems.mod.uk/guidance/posms/smp10 [4] https://www.asems.mod.uk/guidance/posms/smp09 [5] https://www.asems.mod.uk/guidance/posms/smp03 [6] https://www.asems.mod.uk/guidance/posms/smp04 [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/smp05 [10] https://www.asems.mod.uk/guidance/posms/smp06