Defence
Safety Authority

DSA 03.OME Part 1

Defence Code of Practice (DCOP) 105

Safety Risk Management

Version Record

Version 1.1

Version Date: Aug 2024.

Version changes: Reformatted in line with DSA accessibility requirements.

Copyright

Uncontrolled Copies

All hard copies of this document are to be regarded as uncontrolled copies. To check the latest amendment status, reference should be made to current documents which may be viewed on Gov.uk or on the Defence Intranet.

Preface

Requests for Change

1. Proposed changes, recommendations, or amendments to DOSR Regulations and Guidance can be submitted to the DOSR Regulations and Publications Team:

Email Address: dsa-dosr-prg@mod.gov.uk

Postal Address: Juniper #5004, Level 1, Wing 4, Abbey Wood North, Bristol, BS34 8QW

2. Any post and grammar change proposals can be approved or rejected by the DOSR without involvement of the associated Working Group.

3. Technical change proposals should be submitted to the associated Working Group for review and approval or rejection.

4. When incorporating changes, care is to be taken to maintain coherence across regulations.

5. Changes effecting Risk to Life will be published immediately. Other changes will be incorporated as part of routine reviews.

Review Process

6. The DOSR team will ensure OME Regulations remain fit for purpose by conducting regular reviews through the DOSR Governance Committees, consulting with MOD Stakeholders and other Defence Regulators as necessary on interfaces and where there may be overlaps of responsibility.

Further Advice and Feedback

7. For further information about any aspect of this document, or questions not answered within the subsequent sections, or to provide feedback on the content, contact the DOSR Regulations and Publications Team.

Contents

Amendment Record

No	Section	Para	Amendment Summary	Agreed	Date
1.0	all	all	Document created	Regs ATL	Dec 2023
1.1	all	all	Reformatted in line with DSA accessibility requirements	Regs ATL	Aug 2024

DSA 02.OME Regulation 105

Safety Risk Management

1. The Accountable Person shall ensure that the OME Safety Risk is assessed throughout the designated OME Manufacture to Target or Disposal Sequence (MTDS) and managed to be ALARP and Tolerable.

DSA 03.OME DCOP 105

Overview

2. The inherent Ordnance, Munitions and Explosives (OME) safety risks should be managed across all environments the OME system will experience throughout its life, according to the MTDS, thus demonstrating that the risks are As Low As is Reasonably Practicable (ALARP) and Tolerable.

3. Hazards that fall outside the definition of inherent OME safety should be managed in accordance with the overarching domain-specific safety regulations applicable to the service operating environment(s). As such, risk management activities may need to be conducted in accordance with the requirements of the domain specific safety policy, i.e., Land (DSA 02.DLSR.LSSR), Maritime (DSA 02.DMR), or Air (MRP). The Project Oriented Safety Management System (POEMS) provides good practice regarding procedures to be followed.

4. The management of environmental impacts that assess the direct effect of OME on the environment are managed through the application of JSP 418: Management of Environmental Protection in Defence, which provides the MOD policy for environmental management. The Project Oriented Environmental Management System (POEMS) provides good practice regarding procedures to be followed.

5. Risk Management is defined in DefStan 00-056 - Safety Management Requirements for Defence Systems, as ‘the systematic application of management policies, procedures and practices to the tasks of Hazard Identification, Hazard Analysis, Risk Estimation, Risk and ALARP Evaluation, Risk Reduction and Risk Acceptance.’

6. Risk management should encompass all environments that the OME may encounter throughout its life. This is the responsibility of the Senior Safety Responsible (SSR) or equivalent, or specifically delegated staff. The SSR retains this responsibility even when the task is outsourced, either via a contract or the internal tasking of another MOD body.

7. Risk management outputs should be scrutinised by the AP before being submitted for independent review by an OME Safety Review Panel (OSRP). Many of the same considerations apply to Safety and Suitability for Service (S3), where the risks being managed relate to failure of the OME to function as designed during or following exposure to a required service environment.

8. The domains in which the MOD equipment is used pose a wide range of threats. The policy published for each functional safety domain describes domain specific requirements. Underlying these is a risk-based approach based on the SEC, encompassing:

a. Safety and Environmental Management System.

b. Safety and Environmental Management Plan.

c. Safety and Environmental Requirements.

d. SECRs.

9. OME PT/DTs should adopt a risk-based safety management approach to system design and through-life management. They should demonstrate in their SEC and SEMS details of the system, its manner of operation, and the operating environments to which it will be subjected.

10. OME PT/DTs should begin implementation of processes that identify hazards and provide an assessment at the earliest possible stages of the project. The levels of risk presented by the OME should be assessed and reduction of risks using suitable methods to control consequence and/or probability should be considered, with the support of appropriate ITE/guidance from demonstrably SQEP OME competent body[3].

11. The justification for the use of novel approaches to risk management should be documented in the OME's SECR and SEMP. A risk-based approach does not preclude the use of traditional design standards, deviation from standards should be justified, and the resultant risk should be ALARP and Tolerable.

12. DefStan 00-056 provides requirements and guidance on the core elements, activities, and outputs of the safety management process. It is not prescriptive, and the processes and procedures contained also set a framework for compliance with DSA 02.OME Regulation 105. DE&S's standards for PT/DTs to meet the requirements of DSA 02.OME Regulation 105 are POSMS and POEMS.

13. Irrespective of the standard selected, each Duty Holder should adopt a risk-based approach, with suitable emphasis placed on the level of scrutiny that is appropriate and proportional to the level of risk presented by the equipment, system, or platform.

14. Any existing safety pedigree that can be ascertained from historical in-service data (i.e., defects, faults, and incidents), previous best-practice, or re-application of evidence from similar equipment or systems by a demonstrably OME SQEP individual or body, should be considered.

15. The OME PT/DT should demonstrate a structured, systematic approach to safety management, starting with the setting of high-level safety goals, the identification of hazards, followed by the estimation of risk levels and finally the reduction of risk to ALARP and Tolerable.

16. The evidence generated by the safety management process is the backbone of the SEC, and the AP, or appropriate Duty Holder should select common processes, regardless of the domain in which the equipment will operate, where practical.

17. Further guidance regarding each element of the risk management process is available in the (POSMS).

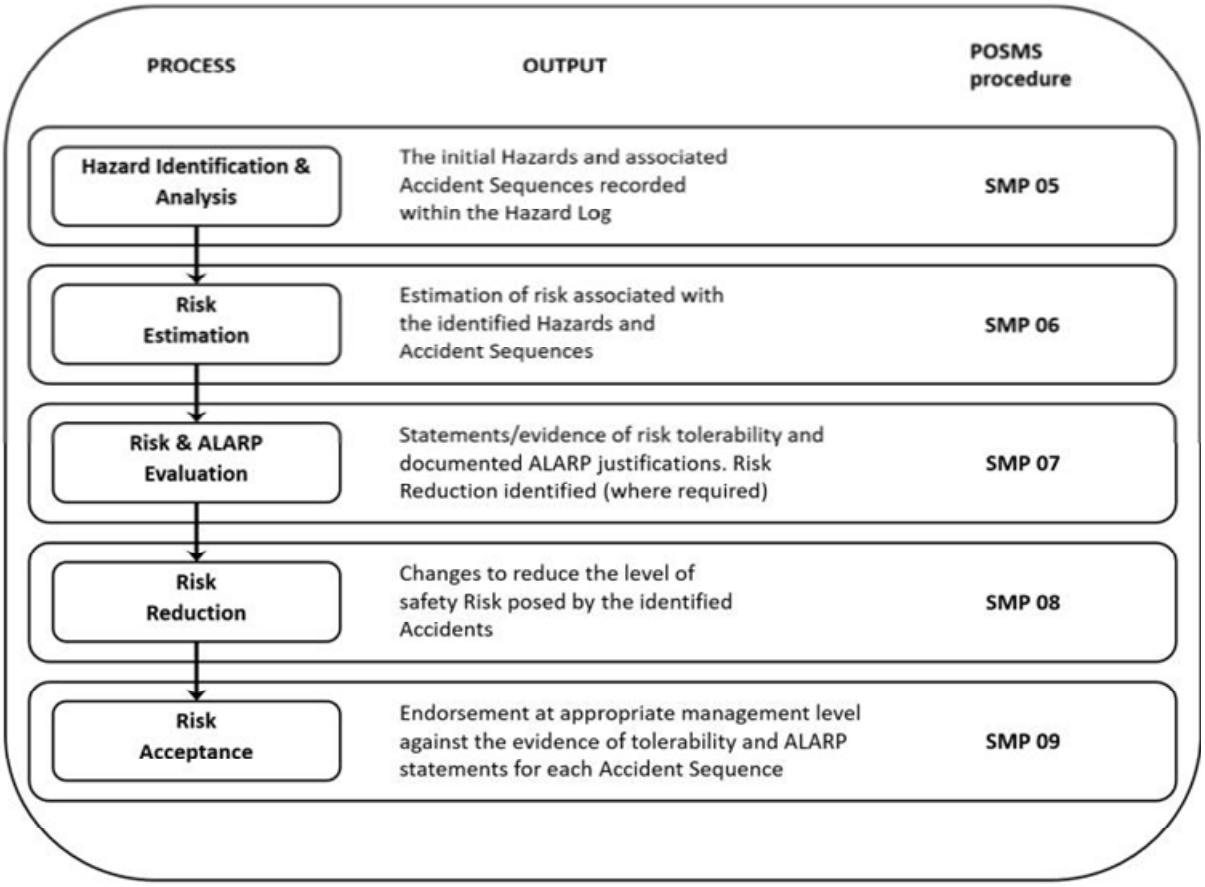

Figure 1 - Risk Management Process

Hazard Identification and Analysis

18. The techniques of Hazard Identification (HAZID) should be used to identify all potential hazards, initially to the total system Preliminary Hazard Analysis (PHA), and subsequently to all sub-systems and components. Omission of hazards at this stage can cause overall risks associated with a system to be incorrectly assessed.

19. The PHA is a qualitative study of the system design concept in its intended operating environment, allowing detection and definition of hazards. Hazard information contributes to the identification of high-risk components in the system, identifies safety critical sub-systems or components and software, and initiates controlling design criteria for safety. The result of this analysis is identification of all known design features that can impair mission capability. PHA results in developing steps that can be taken to ensure avoidance of such features.

20. The Sub-System Hazard Analysis is performed on sub-systems of the overall system to identify hazards associated with component failure modes and functional relationships of components and equipment comprising each sub-system, including software. Analysis should identify all components and equipment whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The analysis should include a determination of the modes of failure and should include all single and multiple point failures with unacceptable combined probabilities of failure arising from faults in sub-system components. This analysis should be started as soon as detailed system design information becomes available.

21. The System Hazard Analysis (SHA) is performed on the total system to identify hazards at the interface of the sub-systems (elements), including software. The assembly of individual hazard-free components does not necessarily ensure that the resulting system is also hazard-free. Multiple failures will be addressed in the SHA.

22. The Operating and Support Hazard Analysis is performed to identify and control hazards and to determine safety requirements for procedures and equipment used in production, installation, maintenance, testing, modification, transportation, storage, operation, and disposal during all phases of intended use.

23. Results of these analyses should provide the basis for:

a. Actions required to minimise risk during a hazardous period or event.

b. Design changes to eliminate and control hazards.

c. Requirements for safety devices and equipment and required maintenance procedures to detect the OME system's functional failure.

d. Warnings, cautions and, special and emergency procedures for operation, maintenance, and modification.

e. Special procedures for handling, storage, and transportation.

Risk Estimation

Purpose

24. Risk estimation is defined in DefStan 00-056 as 'the systematic use of available information to estimate risk'. It determines the consequences and estimates the frequencies of potential accident sequences.

25. The severity and probability of an accident sequence should be predicted in terms of harm to personnel, property, or the environment should an accident occur. The frequency of occurrence and severity should be estimated using previous experience and precedent, analysis such as quantified fault trees, and in some cases, professional suitable qualified and experienced personnel (SQEP) judgement.

26. Risk estimation should be conservative, endeavor to avoid optimism bias, and a suitable risk margin should be considered, with regards to accident analysis. The precautionary principle should be applied where there are reasonable grounds for

concern that an activity may cause harm, but where there is uncertainty about the probability of the risk and the degree of harm. If there is an absence of information, or if the information available is inadequate, then assessments should be based on worst case assumptions.

Tools and Techniques

27. There are techniques available to estimate risk. Techniques for identifying the consequence of individual component / sub-system failures are used across other engineering communities (logistics, human factors, reliability) and the results of assessment studies may be readily available, albeit for a slightly different context. The main techniques are outlined below, although the Acquisition Safety and Environmental Management System (ASEMS) and the Acquisition System Guidance (ASG) provides further guidance regarding Risk Estimation techniques:

a. Top-down methods such as Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) can be powerful when used on their own or in conjunction with bottom-up techniques such as Failure Modes, Effect and Criticality Analysis, Consequence Modelling Analysis, and other risk assessment techniques. These 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, may be useful supplements for the quantification of risk.

b. Useful data may come from other disciplines (e.g., Quality Assurance, Occupational Safety and Health workplace risk assessments, and/or Availability, Reliability and Maintainability Studies). Sharing information between different systems engineering domains is encouraged as it ensures that there is a mutual understanding of the system and makes best use of available resources as part of life-cycle costing.

Risk and ALARP Evaluation

28. The Health and Safety at Work Act 1974 imposes general duties on every employer to ensure the health, safety, and welfare at work of their employees, So Far As is Reasonably Practicable (SFARP). This duty extends to include the provision and maintenance of ‘plant’ (which includes any machinery, equipment, or appliance) that is, SFARP, safe and without risks to health. Note: The Health and Safety Executive (HSE) consider the two terms ‘so far as is reasonably practicable’ and ‘as low as reasonably practicable (ALARP)’ to mean the same thing, and at their core is the concept of ‘reasonably practicable.’

29. ‘Reasonably practicable’ is a narrower term than ‘physically possible’ and implies that a consideration must be made in which the quantum of risk is placed on one scale and the sacrifice (financial, time, or otherwise) involved in the measures necessary for averting the risk is placed in the other. If it is demonstrable that there is gross disproportion between them (the risk being insignificant in relation to the sacrifice) the defendants discharge on the onus for proving that compliance was not reasonably practicable.

30. Def Stan 00-056 defines ALARP as “when it has been demonstrated that the cost of any further Risk Reduction, where the cost includes the loss of defence capability as well as financial, time, or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction.” The ALARP principle is further detailed in Figure 2 and discussed below.

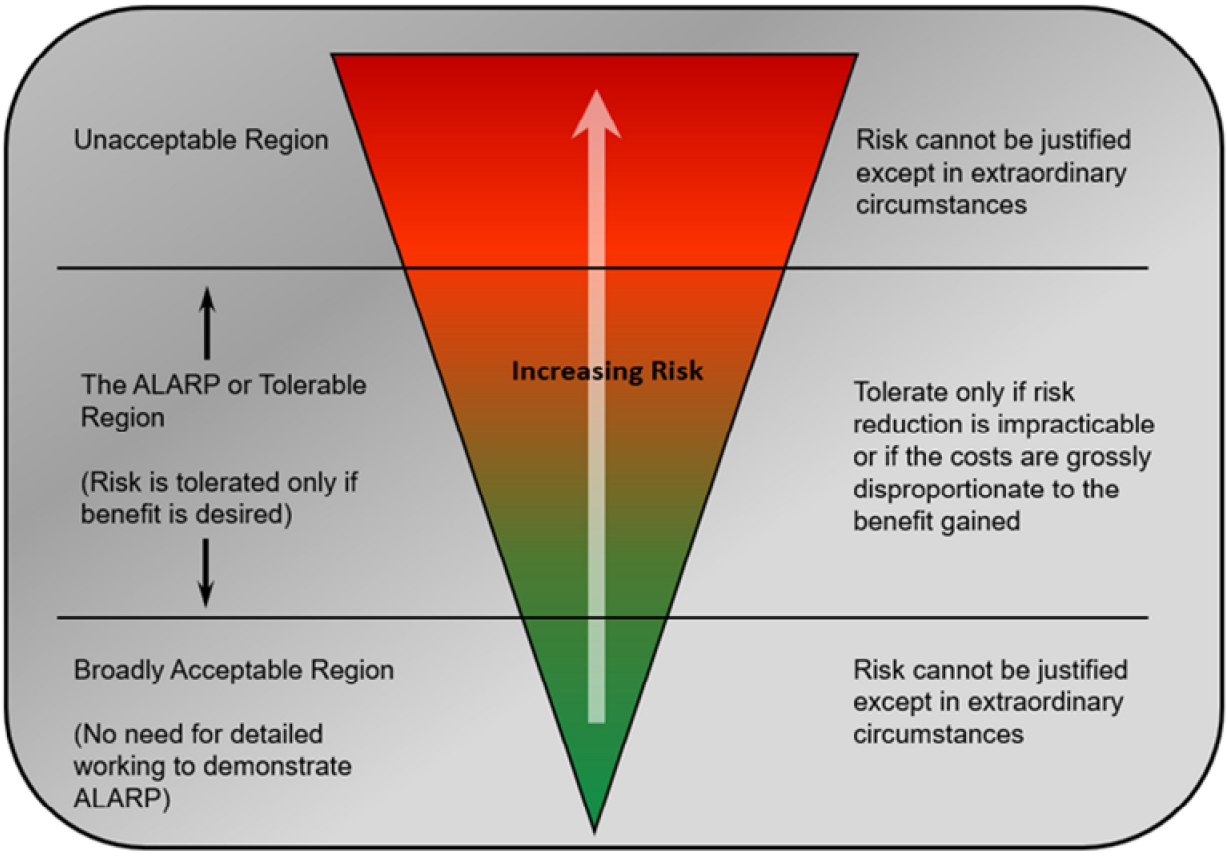

Figure 2 - Risk Tolerability Framework

31. Above a certain level, a risk is regarded as intolerable and cannot be justified except in extraordinary circumstances. Below such levels, an activity can occur providing that the associated risks have been made ALARP and Tolerable.

Risk Tolerability

32. 'Tolerability' does not mean 'acceptability'. Tolerability refers to a willingness to tolerate an acceptable level of risk, to secure certain benefits in the confidence that the risk is being properly controlled. To tolerate a risk means that the risk is not regarded as negligible or something to be ignored, but rather as something to keep under review and reduce to ALARP if possible. When controlling risks, it is necessary to determine the following:

33. Whether a given risk is so great, or the outcome so unacceptable, that it will be refused altogether.

34. Whether the risk is, or has been made, so small that no further precaution is necessary. Any mitigations that have reduced this risk should remain in place and continue to be considered.

35. Whether the risk falls between the two levels stated above, and has been reduced to ALARP and Tolerable, bearing in mind the benefits gained from its tolerance and considering the costs of any further reduction.

36. The tolerability framework described in Figure 2 can be applied to all accident sequences. When determining reasonably practicable measures for any accident, whether the decisions taken to control the risk are good enough depends on where the boundaries are set between the unacceptable, tolerable, or broadly acceptable regions. The choice will be the outcome of deliberation reflecting the preferences of stakeholders and the practicability of practical solutions.

37. The ALARP principle recognises that risk reduction may cease when the cost of further work becomes grossly disproportionate to the benefits gained; this forms the basis for the majority of ALARP decisions. Factors that may have a bearing on a decision and associated costs include loss or damage to assets, reputation, overall capability, cost, and whether people fully understand and undertake the risk as part of their duty, or if they are involuntarily subjected to a risk by a third party.

38. Any claims that all reasonable steps have been taken to ensure that a risk is ALARP and Tolerable, and that the common law ‘duty of care’ has been exercised shall be demonstrable, proportional to the level of risk. This should involve demonstrating that further risk reduction methods have been actively sought and considered in a systematic way. Procedures and further guidance regarding risk and ALARP evaluation, and how to conduct Cost Benefit Analysis (CBA) is contained in POSMS.

Tolerability Criteria

39. The Safety Case should define and justify the tolerability criteria that is applied for making ALARP decisions. Tolerability criteria allows prioritisation of risks and appropriate allocation of resource to reduce the risk to ALARP and Tolerable. The level of risk is determined by bringing together the consequence and the likelihood of an accident. A qualitative or quantitative approach can be used to determine the appropriate risk classification. It is likely that a quantitative approach will be required, in support of a qualitative analysis, when a system poses significant risk. This describes the qualitative approach which is the minimum standard required by the Health and Safety Executive (HSE).

40. The tolerability criteria should be agreed by the SSR or Equivalent in UK MOD projects. The tolerability criteria should be agreed by all Partner Nations in multi-national projects which may lead to a different approach to the MOD’s recognised good practice. The SSR or equivalent will need to demonstrate how any identified deviations will be managed.

41. Either approach should be based upon a risk classification matrix which will be tailored to the system and have justification supporting its structure. The matrix provides

the framework for quantifying risk level according to its tolerability, typically defined by four levels, A to D.

		SEVERITY			
		Catastrophic	Critical	Marginal	Negligible
Frequency of Occurrence	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

Figure 3 – Example of a Risk Classification Matrix

42. Risk Class Definitions are provided in

Risk Class	Definition
A	Intolerable unless there are exceptional reasons for the activity to take place.
B	Undesirable, and should only be accepted when risk reduction is impracticable.
C	Tolerable with the endorsement of the Project Safety and Environmental Committee.
D	Tolerable with the endorsement of the normal project reviews.

43. Figure 4.

Risk Class	Definition
A	Intolerable unless there are exceptional reasons for the activity to take place.
B	Undesirable, and should only be accepted when risk reduction is impracticable.
C	Tolerable with the endorsement of the Project Safety and Environmental Committee.
D	Tolerable with the endorsement of the normal project reviews.

Figure 4 - Risk Class Definitions

44. The matrix must be compiled in a way that can be understood by those using it throughout the entire life of the system. Clear definitions must be given for the terminology used to identify the different criteria. An example of the terminology for the

criteria used in severity and frequency are shown in Figure 5 and Figure 6. Persons Directly involved include personnel having a fair and reasonable understanding of the risks associated with the OME or activity. Persons Indirectly involved include personnel not associated with the OME or activity being undertaken.

Category	**Associated Personnel (Persons directly involved)**	**Non-Associated Personnel (Persons indirectly involved)**
Catastrophic	Multiple deaths.	A single death and / or multiple severe injuries or equivalent occupational illness.
Critical	A single death and / or multiple severe injuries or equivalent occupational illness.	A single severe injury or occupational illness and / or multiple minor injuries or minor occupational illness. A Work-Related Over-7-day Incapacitation Injury.
Marginal	A single severe injury or occupational illness and / or multiple minor injuries or minor occupational illness. A Work-Related Over-7-day Incapacitation Injury.	At most a single minor injury or minor occupational illness. A Work Related 3-day Work Incapacitation Injury.
Negligible	At most a single minor injury or minor occupational illness. A non-sporting injury requiring professional medical attention (may include a Medical Orderly or Military Medical Personnel). A Work Related 3-day Work Incapacitation Injury.	Any injury or occupational illness, however minor.

Figure 5 – Example of Severity Category Definitions

45. An example of the statements/values of qualitative and quantitative probabilities are provided in Figure 6. The units applied to frequency criteria need to be appropriate to the system being considered. For storage, transport, handling, and carriage, per individual per system per year units can be used, however, for launch or operation, per firing event units should be used.

46. Accident frequency descriptors and their associated quantitative or qualitative probabilities will be included in the system's Hazard Log. All identified system hazards will be classified using the accident severity and accident frequency descriptors, together with appropriate risk class definitions.

Descriptor	Qualitative Frequency Categories	Quantitative Frequency Categories
Frequent	Likely to be continually experienced during the life of the system.	> 10^{-3}
Probable	Likely to occur often during the life of the system.	10^{-3} to 10^{-4}
Occasional	Likely to occur several times during the life of the system.	10^{-4} to 10^{-5}
Remote	Likely to occur at some time during the life of the system.	10^{-5} to 10^{-6}
Improbable	Unlikely, but may exceptionally occur during the life of the system.	10^{-6} to 10^{-7}
Incredible	Extremely unlikely that the event will occur during the life of the system.	<10^{-7}

Figure 6 – Example of Qualitative and Quantitative Frequency Categories

47. All identified accident sequences should be categorised according to the severity of the worst credible repercussion to personnel, capability, and the environment because of that accident occurring.

48. For all identified hazards, the frequency of an accident arising from the hazard should be assessed. This may be done qualitatively or quantitatively. The decision on which approach should be taken will be based upon the complexity and risk of the system under consideration, and the level of information available:

a. Quantitative Assessment involves the use of a range of techniques such as FTA, ETA, and Reliability Analysis.

b. Qualitative Assessment may be derived from research, analysis, review of historical safety data and judgement.

49. The criteria in Figure 5 and Figure 6 are illustrative. The criteria used for any specific OME system will be derived from an appropriate comparator. Where this information is not available, HSE guidelines should be considered. Safety targets can be set by using information from internal sources (historic information on comparable systems) or external sources (HSE, industry best practice, engineering judgement) and may be as simple as a series of verbal statements providing a boundary of what is acceptable.

50. It should be remembered that whichever method is used, demonstration that a target has been achieved, or bettered, may not always be practicable. It should be used to indicate the level of performance/integrity expected from the system, and as a baseline against which to argue the Safety Case.

Risk Reduction and Acceptance

51. Risk management activities have no effect on risk until the process of risk control is implemented. Safety is best achieved when it is inherent in the features of the design;

it is recommended that all hazards be eliminated or controlled in accordance with the following order of precedence which is consistent with Def-Stan 00-056:

a. Aim to avoid hazards in the design concept phase.

b. Design to eliminate hazards.

c. Design to control hazards that cannot be eliminated through design.

d. Use safety devices when elimination or design control is not possible.

e. Use warning devices to advise of a hazardous condition that cannot otherwise be eliminated or controlled.

f. Use procedures and training when it is impossible to eliminate or adequately control a hazard through design selection or use of safety and warning devices.

52. Where risks cannot be eliminated through design, the Safety and Environmental Management Plan (SEMP) will identify the management activities necessary to ensure that residual risks will remain ALARP and Tolerable throughout the Acquisition cycle.

53. The authority necessary to accept a risk varies depending on the risk level.

Risk Class	Definition
A	Intolerable unless there are exceptional reasons for the activity to take place.
B	Undesirable, and should only be accepted when risk reduction is impracticable.
C	Tolerable with the endorsement of the Project Safety and Environmental Committee.
D	Tolerable with the endorsement of the normal project reviews.

54. Figure 4 and shows an example of the authority that is required to accept the risk. The Safety and Environmental Management System (SEMS) should articulate which roles have the authority to accept Class A to Class D risks.