Defence Safety Authority

DSA03 DLSR LSSR

Land System Safety and Environmental Protection Defence Codes of Practice (DCoP)

(Previously JSP 454 Part 2)

Land System Safety Regulator

Defence Land Safety Regulator

DLSR

Amendment record

DSA02 DLSR and DSA03 DLSR LSSR will be reviewed on a regular basis for accuracy (at least annually). They are live documents and amendments may be published at any time in response to changes in legislation, MOD policy and / or information.

Amendment Table			
Version Number	**Version Date**	**Author**	**Change to Previous Version**
1.0	Aug 17	DSA-LSSR-Reg	Initial issue
1.1	Sep 19	DSA-LSSR-Reg	Update due to publication of DSA02 DLSR to replace DSA02 DLSR LSSR. Additionally, some minor amendments made.

Contents

Introduction

1. The Ministry of Defence (MOD) has a duty to protect its employees, those that may be affected by its activities and the environment. Effective safety and environmental protection is crucial to force protection and maximising operational capability.

2. These Defence Codes of Practice (DCoPs) are to be read in conjunction with the Defence Regulations contained in DSA02 DLSR.

3. These DCoPs provide practical advice on how to comply with a Regulation articulated in DSA02 DLSR. If the DCoP is followed then this will be considered sufficient to demonstrate compliance, however alternative approaches may be utilised where this produces an outcome as good as required by the Regulation.

4. The Regulations are reiterated in the relevant DCoPs to aid clarity and allow the relationship between them and the text of a DCoP to be accessed more readily.

5. Adherence to a DCoP may be used as evidence during enforcement action and where alternative approaches have been implemented, the onus will be on those holding safety and environmental responsibilities to prove that this has produced an outcome as good as the Regulation requires.

6. Guidance material is also included in this document which, whilst not compulsory, may also be considered 'good practice' to further support the Regulations and DCoPs. For example, this would include Command / Top Level Budget (TLB) processes and procedures.

7. There are two key definitions that apply to the implementation of the Defence Regulations and DCoPs:

   a. **Shall**. Describes an activity that is mandatory;

   b. **Should**. Describes an activity that is considered to be good practice. If the activity is followed then this will be considered sufficient to demonstrate compliance with a Regulation.

LSSR Defence Codes of Practice

8. The LSSR Defence Code of Practice emulates the layout used by the UK National Health and Safety Executive (HSE). A Defence Code of Practice (DCoP) is provided for each Defence Regulation in the following format:

Regulation	The Defence Regulation is reiterated in the relevant DCoP to aid clarity and reinforce the relationship and precedence of the Regulation to the DCoP. Each Regulation may contain a number of Sub-Clauses that are pertinent to that Regulation. (*There may be more than one Regulation referenced*)
Rationale	The reason why the Defence Regulation is applied to the MOD, ideally with reference to national legislation, BSIs or industry codes of practice.
Defence Code of Practice	The DCoP provides practical advice on how to comply with the Defence Regulation. If the DCoP is followed then this will be considered sufficient to demonstrate compliance. However, alternative approaches may be utilised where this produces an outcome that can be demonstrated to be as good as that required by the Regulation.
Guidance Material	Provides Guidance Material, which, whilst not compulsory, may be considered 'good practice' to further support the Regulations and DCoPs.

Important Note The use of the term **should** in the DCoPs describes an activity that is considered to be good practice. If the activity is followed then this will be considered sufficient to demonstrate compliance with a Regulation. However, alternative approaches may be utilised where this produces an outcome as good as required by the Regulation.

LSSR Defence Codes of Practice (DCoP)

DCoP A - Safety and Environmental Protection

Regulation 1 – Safety and Environmental Protection

Regulation	**Those holding safety and environmental responsibilities shall ensure that land systems meet the requirements of all applicable safety and environmental MOD policy.**
Rational	The Land System Safety Regulator may audit a Safety and Environmental Case for land systems against all applicable safety and environmental MOD policy, in addition to DSA02 DLSR.
Defence Code of Practice	1. Those who are responsible for the land system **should** identify and apply all applicable MOD Policy for safety and environmental protection, in addition to DSA02 DLSR. 2. The Safety and Environmental Case **should** provide evidence that demonstrates the land system meets the requirements of the applicable safety and environmental MOD Policy (and legislative requirements – see Regulation 9).
Guidance Material	3. This regulation allows LSSR to capture compliance deficiencies with non-DSA02 DLSR policy encountered during regulatory activities, such as the LSSR audit and inspection process. For example, using Army Command TLB policy, a finding on the non-compliance with elements of MOD policy on Land Equipment User Maintenance Standards (LEUMS)[1] and / or Land Equipment Engineering Standards (LEES)[2] could be considered a non-compliance with Regulation, as this could have an impact on the safety / environmental management of the land system. Other TLBs may adopt the Army Equipment Care (EC) policies, use their own or a combination of both. For example, Air Command TLB also work to Military Air Environment policy to manage their land systems. 4. This regulation is all encompassing and applies to all levels of stakeholders with land system responsibilities throughout the lifecycle (including in service end-users) of the land systems, across all TLBs.

[1] Army Equipment Support Publication (AESP) 0200-A-093-013
[2] Army Equipment Support Publication (AESP) 0200-A-090-013

DCoP B - Safety and Environmental Management System

Regulation 2 – Establish a SEMS

Regulation	**Those holding safety and environmental responsibilities shall document, maintain and use a suitable and sufficient Safety and Environmental Management System (SEMS) for the management of safety and environmental protection throughout the lifecyle of all land systems.**
Rationale	A Safety and Environmental Management System (SEMS) is the organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet statutory requirements, MOD policy and Defence Regulations.
Defence Code of Practice	1. A hierarchical set of SEMS may be developed under each TLB to ensure suitable and sufficient detail is provided, to manage the safety and environmental protection of land systems throughout the lifecycle. For example, within DE&S there would be a SEMS at the Operating Centre and at the Project Team Level. It may be prudent to have a separate SEMS for a Level 1 Safety and Environmental Case[3] due to the level of risk, novel technology involved and / or complexity of the Land system(s). 2. The requirement for the number of SEMSs within a TLB **should** be agreed and documented. 3. Land systems may interface with a number of TLBs. The management of any boundaries and interfaces with other SEMSs (whether at the same level or higher/lower levels) **should** be detailed and recorded[4]. 4. Where a land system is considered part of a system or a platform, e.g. System of Systems[4] then the SEMS **should** ensure: a. All responsibilities related to being the prime platform / system are documented; b. Any letters of delegation include the responsibilities associated with being the prime platform / system; c. The Safety and Environmental Committee (refer to Para 29) agree and document which system / platform has primacy and recommend acceptance by the appropriate Capability Sponsor / Lead User. 5. The SEMS **should** detail the organisational structure, processes, procedures and methodologies in place to manage safety and environmental protection for the land system(s) it is managing. 6. The SEMS **should** be tailored to suit the level of risk and / or complexity of the land system(s). 7. The scope of the SEMS **should** be clearly identified so that those people involved know how it affects them.

[3] Refer to the DCoP (D) for Regulation 4 – for the definition of a Level 1 Safety and Environmental Case
[4] Refer to the DCoP(D) for Regulation 5

8. The authority under which the SEMS operates and the defined scope **should** be made clear and documented.

9. The SEMS **should** include and communicate the objectives for managing safety and environmental protection to ensure the land systems is safe to use and reduces adverse impact on the environment.

SEMS Lifecycle

10. There are four key elements to a SEMS lifecycle that **should** be included. This is illustrated in Figure 1 and described in the following sections.

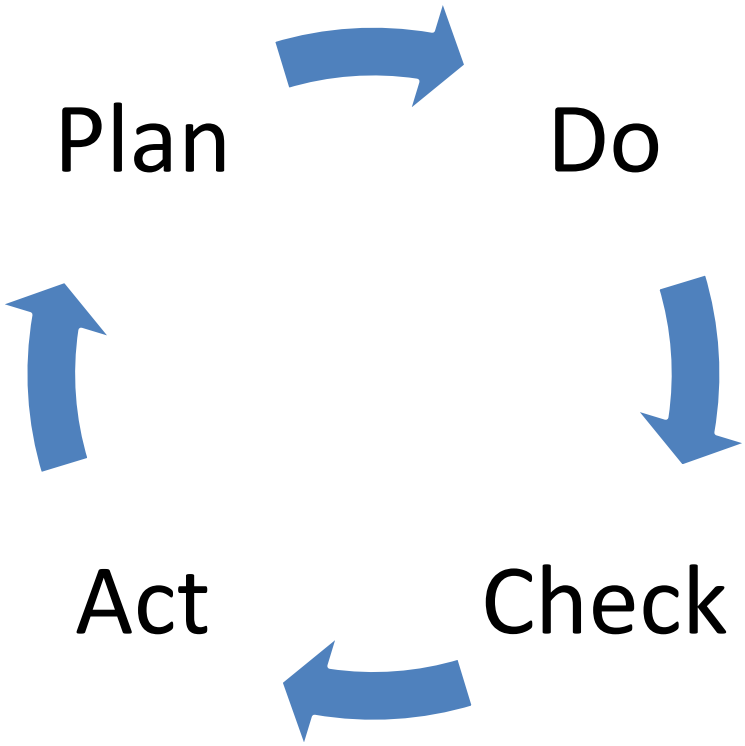


Figure 1. SEMS Lifecycle

Plan

11. The SEMS **should** establish and document what is to be achieved, activities, key roles and responsibilities and how successful implementation will be measured.

12. The SEMS **should** set out procedures for managing change.

13. The planning for an effective SEMS **should** include as a minimum the following:

a. Safety and Environmental Management Committee (SEMC) to oversee and guide the SEMS. Guidance is provided in paragraph 29;

b. Safety and Environmental Case for each land system[5];

c. Requirements for developing a Safety and Environmental Management Plan (SEMP) for each land system being managed under the SEMS. Guidance is provided in paragraph 32;

d. Hazard logs that identify hazards, assess risk and establish priorities according to risk;

e. Documented procedures;

f. Organisational structures, identifying the people involved, the resource required and allocating safety and environmental roles and responsibilities;

g. Mechanisms for ensuring competence through recruitment and training / personal development;

h. Any requirement for an Independent Safety and / or Environmental Auditor[6];

i. Leading and lagging indicators **should** be identified (these are also called active and reactive systems);

j. Establishment of measurable performance indicators and appropriate monitoring mechanisms;

k. Means of communicating the safety and environmental approach;

l. Identification of applicable legislation[7] (linked to the exemption case where appropriate).

m. Considerations for configuration management and in-service equipment care[8] issues that could potentially impact on the safety and environmental protection of the land system.

Do

14. The SEMS **should** be approved by and formally communicated to all stakeholders.

15. Adequate training and resources **should** be provided to all those holding safety and environmental responsibilities to ensure that they are able to use and implement the SEMS effectively.

[5] Refer to the DCoP (D) for Regulation 4 – on the acceptable method of compliance for a safety and environmental case
[6] Refer to the DCoP (H) for Regulation 14 – on details regarding when an Independent Auditor may be required
[7] Refer to DCoP for regulation 9 (F) – Legislation Compliance
[8] Refer to the DCoP (I) for Regulation 15 – Equipment care and configuration management.

16. A Safety and Environmental Plan (SEMP) **should** be developed for the land system(s) operating within the SEMS. For Level 1 and 2 Safety and Environmental Cases[9] a SEMP **should** be developed for each land system. For a Level 3 Safety and Environmental Case[9] a SEMP could be developed to encompass more than one land system. For a Level 4 Safety and Environmental Case a SEMP may not be required, provided that it is covered under a suitable and sufficient safe system of work. This **should** be agreed by the Safety and Environmental Committee.

17. The Safety and Environmental Case[10] **should** be established and the Safety Environmental Case Summary Reports[11] **should** be developed.

Check

18. Leading indicators (active systems) **should** be used to monitor[12] the design, development, installation, maintenance, training and operation of management arrangements, risk control systems and workplace precautions. This **should** include audit and monitoring of the SEMS and reporting through TLB processes.

19. The following **should** be the minimum that the audits and monitoring activities address:

a. Appropriateness of safety and environmental requirements;

b. Compliance against applicable Legalisation[13];

c. Compliance against applicable MOD Policy;

d. Effectiveness and the implementation of the Safety and Environmental Management Plan;

e. Operating Environment for land systems is clearly defined, documented and is being implemented;

f. Appropriateness of any Safety and Environmental Case Summary Reports;

g. All roles and responsibilities are clearly defined and documented and appropriate competency[14] in place;

h. Operational, training and maintenance policies, arrangement and associated documentation are extant, valid and being implemented;

i. Effectiveness of the safety and environmental arguments;

j. Robustness of the body of evidence supporting the safety and environmental arguments;

[9] Refer to the DCoP (D) for Regulation 4 – on the definition of the different levels of a Safety and Environmental Case
[10] Refer to the DCoP (D) for Regulation 4 – on the acceptable method of compliance for a Safety and Environmental Case
[11] Refer to the DCoP (D) for Regulation 4 – on the appropriate periodicity for the production of Safety and Environmental Case Reports
[12] Refer to the DCoP (H) for Regulation 13 – Monitoring and Reviewing Performance
[13] Refer to the DCoP (F) for Regulation 9 and 10 – on legislation Compliance Assessment and Exemption Cases
[14] Refer to the DCoP (C) for Regulation 3 – Competence

k. Quality and appropriateness of the evidence underpinning the safety and environmental argument;

l. Effectiveness of the reporting mechanisms e.g. incidents (accidents & near misses) etc.;

m. Overall effectiveness and implementation of the SEMS;

n. Lagging indicators (reactive systems) **should** be used to monitor incidents (accidents & near misses), corrective action and other evidence of deficient safety and environmental performance.

Act

20. Performance review is a key element of the SEMS lifecycle and is important because it facilitates organisational learning. These reviews **should** include formal safety and environmental management audits, reviews of Learning from Experience (LFE) and benchmarking exercises as appropriate.

21. Findings from the audits, monitoring and review activities **should** be reviewed and **should** be used to update and improve the SEMS (where appropriate).

22. Further requirements and guidance on audits is detailed in Regulation 14.

Urgent Defence Requirements / Urgent Operational Requirements

23. It is recognised that, because of the short timescales and pressures under which Urgent Defence Requirements (UDRs) and Urgent Operational Requirements (UORs) are procured, it may not be practical to apply the full requirements of a SEMS prior to a UDR / UOR coming into service. Nevertheless, those responsible **should** ensure that the MOD discharges its duty of care appropriately. Guidance is provided in paragraph 38 regarding the minimum requirements that **should** be satisfied for UDRs and UORs.

24. All those holding safety and environmental responsibilities **should** understand, and be able to demonstrate, that they can manage the main safety and environmental risks that the land system is likely to present. The possible shortfalls in a land system **should** be clearly identified and addressed if there is any planning for the future development, or extended use, of the land system.

Guidance Material

Roles and Responsibilities

25. Each TLB will have a SEMS to describe the organisational structure, processes, procedures and methodologies that enable the direction and control of the activities for which the TLB is responsible. As the land system's Safety and Environmental Case is developed through the lifecycle, the associated roles and level of responsibility for each TLB, at each stage of the cycle, will vary. For example:

a. **Capability Sponsor / Lead User / Chain of Command Representative / Duty Holder facing SMEs**. The Capability Sponsor / Lead User / Chain of Command Representative / Duty Holder facing

SMEs[15] are the joint owners of the In-Service Safety and Environmental Case (for example a Part 3 Safety and Environmental Case[16]), on behalf of the FLCs. Their responsibilities include setting safety and environmental protection requirements during the planning stages of a land system's life and ensuring that these are met throughout a land system's life. They must ensure that capability can be fielded safely, "Operated and maintained Safely" and that suitable and sufficient training exists for the capability at all times throughout its service life;

Note: It is important to ensure that the Lead User is identified at early stages of the new land system, to avoid ambiguity at in-service stage.

b. **Acquisition Team** – The Acquisition Team (for example DE&S) are responsible for the delivery of the land system to the FLCs, ensuring that it meets the capability requirements set by the Capability Sponsor. In addition, they are responsible for the development of the "safe to operate" Safety and Environmental Case (For example the Part 1 and Part 2 Safety and Environmental Case[16]).

c. **Front Line Command** – The Front Line Commands are responsible for ensuring that the land system is operated by the End User in accordance with the safe operating envelope defined within the Safety and Environmental Case.

26. Typically the in-service Safety and Environmental Case is normally developed and maintained by the Acquisition team, e.g. a Project Team within DE&S, on behalf of the Capability Sponsor.

Safety and Environmental Management System

27. The HSE publication Health and Safety Guidance (HSG) 65 provides good practice with regard to a Health and Safety Management System. The principles contained within that publication are readily transferrable to the management of safety and environmental protection.

Safety and Environmental Management Committee

28. Where a team has a number of similar land systems under its management, e.g. a cluster project team, consideration could be given to establishing a top level SEMC to set out and agree the safety and environmental management policy and strategy for those land systems. The agreed policy and strategy would be recorded in a SEMS document, similar to a SEMP. In this case the SEMC is responsible for monitoring and controlling the activities of all individual projects as shown in Figure 2.

[15] A DH Facing SME is an expert within their field who resides in the TLB HQ and will act as the conduit for TLB HQ advice to Duty Holders / the Chain of command representative
[16] Refer to DCoP (D) for Regulation 4

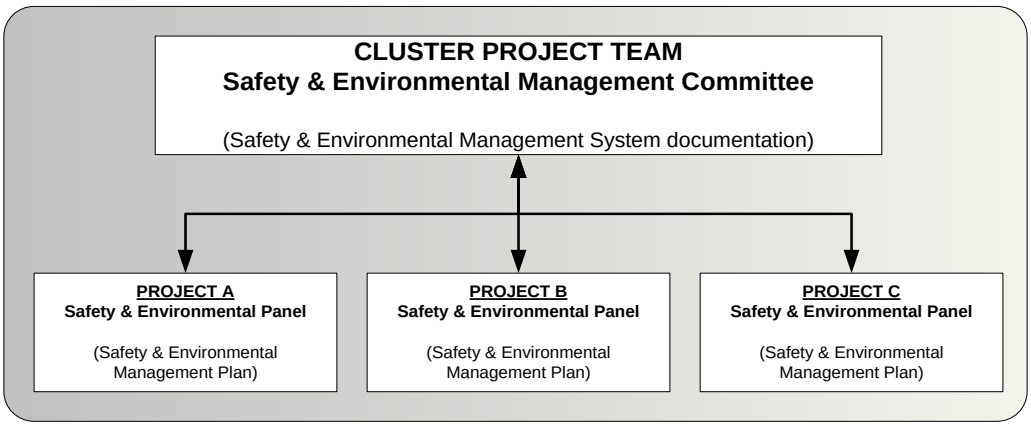


Figure 2. Safety and Environmental Management Committee

29. The SEMC is responsible for monitoring and controlling the management activities undertaken for all systems with its Area of Responsibility (AoR).

30. The purpose of the Safety & Environmental Panel (SEP), as shown in Figure 2, is to manage the safety risks and the environmental aspects through the operation of the SEMS. It provides a forum for relevant stakeholders to effectively monitor and co-ordinate all related activities.

31. Further guidance on the development of a SEMP is detailed in Defence Standard 00-056 and ASEMS.

Safety and Environmental Management Plan

32. A SEMP (it is acceptable for this to be a single, combined, document or two separate documents) should be produced to document how the SEMS is to be applied to the system(s).

33. The SEMP should be used to set out and record the safety and environmental management arrangements for the system(s), and the actions and processes to be followed to ensure safe operation and support of the system(s).

34. The SEMP should state the responsibilities of both MOD and its contractors for the management of safety and environmental protection.

35. The SEMP should typically include the following:

a. A high level description of the system(s);

b. Key safety and environmental requirements;

c. Applicable legislation;

d. Tolerability Criteria;

e. Risk management processes, including the definition of applicable methodologies e.g. hazard identification and analysis techniques;

f. The identification of tools e.g. hazard log tool, hazard analysis tools, environmental features matrix tool etc;

g. The safety and environmental programme;

h. The audit plan;

i. A list of deliverables.

36. Further guidance on the development of a SEMP is detailed in Defence Standard 00-056 and ASEMS.

UDR / UOR

37. In the case of UDRs and UORs the following basic elements of a SEMS should be established:

a. SEMC is to:

(1) Agree the extent of the Safety and Environmental Case (boundaries / interfaces);

(2) Define principal safety requirements and acceptance criteria;

(3) Provide input to safety assessment (particularly from the user and maintainer);

(4) Review and recommend acceptance of the Safety and Environmental Case and agree on the future strategy for its development should the use of the system be extended.

b. SEMP - can be brief, but needs to define:

(1) Those with the key responsibilities for safety and environmental protection (by post and responsibility);

(2) Agreed requirements and acceptance criteria:

(3) The safety and environmental assessment process;

(4) What safeguards will be adopted to give early identification of potential problems in-service, e.g. through full accident and failure reporting, additional briefings etc., recognising that there may be limitations in the safety assessment process.

c. Safety and Environmental Assessment - A top down approach concentrating on likely main hazards and risks. The SEMC should ensure that mitigation action is robust, only relying, for instance, on training as a last resort. The SEMC should also ensure that those holding safety and environmental responsibilities are aware of the limitations under which the safety assessment was carried out.

DCoP C - Competence

Regulation 3 – Competence

Regulation	**Those holding safety and environmental responsibilities shall have the competence to undertake the roles for which they are engaged.**
Rationale	Much of the safety and environmental legislation applicable to MOD has an explicit requirement for certain duties to be carried out by competent persons. This requirement has been repeated in policy where MOD has benchmarked its own arrangements to be equally as good as those required by legislation. The Management of Health and Safety at Work Regulations (1999) defines a competent person as a person who has sufficient training and experience or knowledge as to enable them to assist in securing compliance, on the part of the employee, with the necessary safety legislation and maintenance procedures. Competent persons shall be an integral part of the resources available to allow delivery of high standards of safety and environmental performance. Competence is not just about the individual but also an organisation or team who collectively ensure that land systems meet MOD policy and legislation, throughout their lifecycle.
Defence Code of Practice	1. TLBs **should** develop and maintain competence through implementation of a Competence Management System. The Competence Management System **should** identify competency requirements for all staff at all levels of responsibility within an organisation that have been identified as having safety and environmental responsibilities, including those within the supply chain. Further guidance on a Competence Management System is provided in the guidance at paragraph 16. 2. TLBs **should** identify: a. The safety and environmental roles and responsibilities applicable to land system(s) activities throughout the lifecycle. For example: operation, training, management, maintenance, etc. b. Safety and environmental competencies applicable to the various roles and responsibilities. 3. These roles, responsibilities and competencies **should** be recorded in applicable documentation[17] at the appropriate management levels. 4. A record of required safety and environmental competencies and actual competency for each individual, thereby showing any training and development requirements, **should** be kept. When assessing an individual's competency, previous training or experience **should** be considered. This **should** include work experience and on-the-job training and development.

[17] Examples of applicable documentation include the Safety and Environmental Management System, Safety and Environmental Management Plans, Land Forces Standing Orders, Safety and Environmental Case Reports, Interactive Electronic Technical Publications, Army Equipment Support Publications, ToRs, HRMS / JPA etc

5. Where the individual does not meet the competency level required for their role, a training and development plan **should** be used to demonstrate how competency is to be achieved. This individual **should** be supervised by a competent person until the training and development plan has been completed.

6. The roles, responsibilities and competencies for the land system(s) **should** be reviewed and updated throughout its lifecycle, where there is a change to the land system[18].

7. Competence is not centred only on competence of individuals, it **should** also include teams / organisations that might have an impact on the functional safety of land systems during any lifecycle phase, e.g. design, development, manufacturing, operation, maintenance, modification etc.

Individual Competency Assessment Levels

8. At an individual level safety and environmental competencies **should** be assessed against the levels of 'Awareness', 'Supervised Practitioner', 'Practitioner' and 'Expert'[19]:

a. **Awareness**. The person is able to understand key System Safety issues and their implications. They are able to ask relevant and constructive questions on the subject;

b. **Supervised Practitioner**. The person has knowledge of System Safety and can apply its principles under supervision. They are capable of applying System Safety assurance processes and safety management for a system or a group of systems, e.g. Vehicles, Communication Systems. Typically engineering staff directly performing the management of safety;

c. **Practitioner**. The person displays a detailed knowledge of System Safety and can apply its principles. They are capable of discharging responsibility for the management of safety and safety assurance requirements, or supervising system safety, within a functional domain, e.g. Land, Sea, Air or Ordnance. A Practitioner is distinguished from a Supervised Practitioner by a sufficient depth of knowledge and breadth of experience to allow them to work unsupervised, taking full responsibility for the consequences of their judgements;

d. **Expert**. The person displays extensive and substantial practical experience and applied knowledge of System Safety. They can advise on and interpret the requirements for System Safety across functional domains, e.g. Land, Sea, Air or Ordnance.

[18] Refer to the DCoP (D) for Regulation 4 on the monitoring and reviewing of the Safety and Environmental Case
[19] As defined in the System Safety Functional Competences document: http://defenceintranet.diif.r.mil.uk/libraries/corporate/PSCLearning/CompetenceFrameworks/UsefulInfo/FC_M-Z/SystemSafety_v2_Apr14-U.pdf

Competency Requirements for Safety and Environmental Management Committee (SEMC) Members

9. The SEMC will include members and representatives as appropriate from the areas set out in Table 1, who **should** meet the minimum safety / environmental competence requirements also set out in Table 1.

10. The members of the SEMC **should** be competent for their main role for which they are representing at the SEMC and hold the appropriate authority to represent their area.

Table 1. Competency Requirements for SEMC Members

Member / Representative From	Minimum Safety and Environmental Competence Level
The Project / Delivery Team Leader (or equivalent) or representative	Awareness
Project Manager / Officer	Awareness
System Safety / Environmental Manager / Officer / Safety and Environmental Case Lead	Practitioner / Expert[20]
Integrated Logistics Support Manager	Awareness
Equipment Capability Customer	Awareness
Equipment User	Awareness
Maintenance Authorities	Awareness
Training Authorities	Awareness
Design Authority	Awareness
Independent Safety Auditor, if appointed	Expert
Interfacing Project / Delivery Team Representative(s), if required	Awareness
External Safety / Environmental specialists (e.g. Safety / Environmental Engineers and Advisors)	Practitioner / Expert[21]
External technical specialists	Awareness

Independent Safety Auditor (ISA) Competence[22]

11. The competence of an ISA **should** be ascertained due to the reliance on the expert opinions that they provide. When choosing an ISA, consideration **should** be given to the qualifications / accreditations, auditor experience, and the technical knowledge in relation to the task at hand.

12. ISA Competence **should** be reviewed if any project or task requirements change. Those holding safety and environmental

[20] Refer to the DCoP (D) for Regulation 4 – to determine the minimum competency level
[21] Depending on the specific role performed within the SEMC
[22] Note: The term Independent Safety Auditor (ISA) encompasses environmental aspects as well as safety

responsibilities **should** ensure that any additional tasking is within the ISA competence.

Contractor Competence

13. The contractor has a duty to ensure that all workers are competent for the related task, and all those holding safety and environmental responsibilities **should** take all reasonable steps to ensure the competence of those carrying out work under their direct control, and those responsibilities and lines of communications **should** be properly established and clearly laid down.

14. Contracting tasks or activities outside the MOD does not discharge MOD's obligation to manage safety and environment protection. Those holding safety and environmental responsibilities **should** ensure suitable control of staff under contract in order to assure themselves that safety and environmental protection continues to meet their requirements. This assurance **should** include the ability to understand and accept the Safety and Environmental Case, and authorise the residual risks identified within it.

15. The Contractor / Supply Chain **should** be measurable against the Competence Management System which includes supplier competence requirements.

Guidance Material

Competence Management System

16. Guidance on developing an Organisational Competence Management System is available in the HSE Guidance document "*Managing Competence For Safety Related Systems Part 1: Key Guidance."*[23]

General guidance

17. The MOD authority maintains responsibility for safety and environmental management irrespective of where its resources come from.

18. There are a number of sources for detailed guidance on competence that are not reproduced within this DCoP. These documents should be referred to where appropriate:

[23] http://www.hse.gov.uk/humanfactors/topics/mancomppt1.pdf

a. MOD Single Skills Framework;

b. System Safety & Environmental Protection Role Profiles, DE&S Safety and Environmental Protection Leaflet 10/2017;

c. Guidance leaflet AAP01a/G/01 within the Acquisition Safety and Environmental Management System (ASEMS) Audit Manual provides detailed guidance on Auditor competence;

d. Project Oriented Safety Management System (POSMS) manual;

e. Project Oriented Environmental Management System (POEMS) manual;

f. Safety and Reliability Society Open Standard for Competence.

19. There are also a number of key industry documents that discuss competency assessment in more detail. These include:

a. Managing competence for safety-related systems (HSE 2007);

b. Institution of Electrical Engineers / British Computer Society (IEE / BCS) Competence Criteria for Safety-Related System Practitioners. (Guidance provided by the IET in collaboration with the HSE and BCS, 1999).

System Safety Functional Competences

20. The System Safety Functional Competence framework provides five competence areas relevant to system safety:

a. SysSaf 1 - MOD Policy;

b. SysSaf 2 - Principles of System Safety Management;

c. SysSaf 3 - Compliance with Requirements;

d. SysSaf 4 - Safety Risk Management;

e. SysSaf 5 - Domain-specific Requirements.

System Environmental Functional Competences

21. The System Environmental Functional Competence Framework provides three competence areas relevant to system environmental issues:

a. SysEnv 1 - Formulate Environmental Policy and Procedures;

b. SysEnv 2 - Implementation of policy and procedures, creation of strategies and effective plans for environmental aspects of the MOD acquisition cycle;

c. SysEnv 3 - Technical Authority, Advice and Guidance on Environmental issues in the acquisition cycle.

Training

22. Safety and Environmental training is available via the DE&S Director Safety & Environment, Quality and Technology Team (QSEP). The QSEP team sponsors a suite of courses acquisition safety and environmental protection. These courses have been produced specifically to align with the generic Safety and Environmental Protection (S&EP) role profiles and functional competences, and comprise both eLearning and workshop modules.

23. The System Safety courses are provided by the Defence Academy[24] and are free to MOD personnel at the point of delivery.

24. The environmental protection equivalents cover a similar scope. They are provided by Cranfield University and are based on the principles published in POEMS. The practitioner course forms part of a practitioner training programme comprising a teaching element followed by assessment and on the job training. It is primarily aimed at staff that will be expected to implement POEMS within their Project Team.

25. There are a number of training courses available ranging from safety and environmental awareness to practitioner courses. Planning for training should be developed in accordance with the requirements of the Project Team SEMC, individual staff roles and responsibilities and terms of reference.

ISA Competences

26. When consideration is given to the qualifications / accreditations, auditor experience, and the technical knowledge in relation to the task at hand, technical knowledge can include experience of land system projects; system / equipment being assessed; risk management principles etc.

27. A key industry document that discusses ISA competency assessment in more detail includes: ISA Working Group's Competency Framework for Independent Safety Assessors[25].

[24] http://www.da.mod.uk/
[25] http://www.theiet.org/factfiles/isa/comp-frame-page.cfm

DCoP D - Safety and Environmental Case Development

Regulation 4 Safety and Environmental Case

Regulation	**Those holding safety and environmental responsibilities shall establish, use and maintain a valid Safety Case and Environmental Case, including summary reports, for land systems.**
Rationale	A Safety Case is necessary in order to demonstrate that a system is acceptably safe in use; all risk has been reduced to a level that is As Low As Reasonably Practicable (ALARP) and that the system complies with applicable legislation. An Environmental Case is required in order to demonstrate that applicable legislation has been complied with and that all environmental impacts and risk have been reduced as far as is reasonably practicable.
Defence Code of Practice	1. The Safety Case and Environmental Case may be produced separately or as a combined, single entity. 2. A Safety and Environmental Case **should** be established to provide a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a land system is safe and is the Best Practicable Environmental Option (BPEO) [26], for a given application in a given operating environment. 3. The strategy for the creation, development and management of the Safety and Environmental Case for a land system **should** be developed at the start of the project. The safety case strategy **should** be reviewed on a regular basis and typically recorded within the land system's Safety and Environmental Management Plan (SEMP)[27]. 4. The strategy **should** define the roles, responsibilities and activities of all relevant TLBs for the creation, development and management of the Safety and Environmental Case throughout the lifecycle of the land system. This strategy **should** identify how stakeholders will be engaged through the process and set clear milestones and goals. Additionally a clear scope, boundary and interfaces **should** be determined, which is realistic and adequately captures all elements that interact with people, the environment or that could be affected by the environment. This is typically recorded within the land system SEMP[28]. 5. The detail for the Safety and Environmental Strategy **should** be proportionate to the perceived level of risk and environmental impacts. 6. The Capability Acquirer, e.g. DE&S, **should** agree with all stakeholders including the capability sponsor, the evidence necessary to define and document the application and operating environment for the land system's Safety and Environmental Case. 7. Where a land system includes sub-systems that have separate Safety and Environmental Cases, these Safety and Environmental Cases **should** be integrated,

[26] Refer to the DCoP (E) for Regulation 8
[27] Refer to the DCoP (B) for Regulation 2
[28] Refer to the DCoP (B) for Regulation 2

or reconciled, with the land system's Safety and Environmental Case, e.g. the host platform Safety and Environmental Case[29].

8. If the land system is part of a larger system, e.g. integrated onto a host platform or arranged in a "system of systems"[30], then the Delegated Authority responsible for the higher level system **should** be satisfied that the land system is safe and for environment impacts and risks the BPEO has been selected, the within the defined application and operational environment.

9. As the Safety and Environmental Case develops it **should** present the current status of the progress against the Safety and Environmental Plan. It **should** present a clear route to reducing risk to a level that is ALARP and selection of BPEO.

10. The generation of a Safety and Environmental Case is an iterative process and **should** start as early as possible in a system's lifecycle.

11. A Safety and Environmental Case **should** provide evidence that, as a minimum:

a. Safety and Environmental requirements have been met;

b. Hazards have been adequately identified and analysed and the associated risk has been assessed in an appropriate manner;

c. All hazards and potential accidents have had controls applied, to ensure all residual risk has been reduced to a level that is ALARP;

d. Environmental Impacts and risks have been adequately identified and analysed and the associated risk has been assessed in an appropriate manner;

e. BPEO has been selected for residual environmental impacts and risks;

f. The system complies with all relevant safety and environmental legislation, Defence Regulations and MOD Policy;

g. All measures have been taken to ensure that acceptable levels of safety residual risks and environmental impacts and risks can be maintained through life.

12. Proportionality is a fundamental attribute of modern risk management. The concept of proportionality will drive the level of risk / impact analysis, the level of assurance, and the competency required to deliver the Safety and Environmental Case. The structured safety and environmental arguments and supporting body of evidence within a Safety and Environmental Case **should** be proportionate.

13. The proportionality levels within Table 1 **should** be used to determine the proportionality of a Safety and Environmental Case. The definitions for the proportionality levels are provided in Table 2, and the definitions for Expert and Practitioners are presented in the DCoP (C) for Regulation 3 - Competence. Where the Safety Case and the Environmental Case are separate, the levels of proportionality **should** be determined independently.

[29] Refer to the DCoP (D) for Regulation 5 – on Ancillary Systems
[30] Refer to the DCoP (D) for Regulation 5 - on Systems of Systems

Table 1: Proportionality Levels for the Development of a Safety & Environmental Case.

Directly Involved Operator / Maintainer	Indirect Personnel / General Public	Bespoke Defence Equipment	Modified Military / Commercial Off The Shelf	Unmodified Military / Commercial Off The Shelf
Catastrophic: Multiple Deaths	Catastrophic: A single Death and / or multiple major injuries or equivalent occupational illness.	1	2	2
Critical: A single Death and / or multiple major injuries or equivalent occupational illness.	Critical: Single major injury or occupational illness and / or multiple injuries or minor occupational illness.	2	2	3 (See note 1)
Marginal: Single major injury or occupational illness and / or multiple injuries or minor occupational illness.	Marginal: At most a single minor injury or minor occupational illness.	3	3	4
Negligible: At most a single minor injury or minor occupational illness.	Negligible	4	4	4

Note 1 - SEMC to determine whether a 3 Part Safety Case should be undertaken.

The table is based on the most credible risk.

Please see the next page for Table 2: Proportionality Level Definitions.

Table 2: Proportionality Level Definitions.

Proportionality band	Safety Case led by	Safety Case undertaken by	Safety Case Strategy	Safety & Environmental Management Plan
LEVEL 1	Practitioner/ Expert	Experts and Practitioners	3 Part Safety Case	Yes
LEVEL 2	Practitioner/ Expert	Practitioners	3 Part Safety Case	Yes
LEVEL 3	Practitioner	Practitioners and Supervised Practitioners	A singular Safety Case[31]	The land system may share a Safety & Environment Plan with other land systems
LEVEL 4	Practitioner	Supervised Practitioners	Risk assessment supported by a suitable and sufficient Safe System of Work	Covered under a Safe System of Work

14. The residual risks associated with the land system **should** be demonstrated as tolerable or broadly acceptable and As Low As Reasonable Practicable (ALARP) [with the selection of the BPEO for environmental impacts and risks] within the given application and given operating environment. The requirement and guidance on demonstrating ALARP and defining tolerability are contained in the DCoP (E) for Regulation 7 - ALARP. The requirement and guidance on demonstrating selection of BPEO are contained in the DCoP (E) for Regulation 8 – BPEO.

Structured Argument and Evidence

15. A safety and / or environmental argument **should** be produced that links the available evidence to the claims made regarding the safety and / or environmental impact of the system(s).

16. The safety and / or environmental argument **should** be compelling and supported by sufficient evidence.

17. The safety and / or environmental argument **should** be articulated in a way that is proportionate to the complexity of the system and the level of risk / environmental impact. A formal, structured approach to articulating the argument **should** be used where the Safety and Environmental Case is at Level 1 or 2 (See Table 1).

18. The degree of evidence required and work involved in developing a Safety and Environmental Case **should** be commensurate with the risk (whether it is a safety

[31] Refer to Paragraphs 20 and 96

risk or an environmental impact) posed, complexity and maturity of a particular system.

Safety and Environmental Case

19. For Level 1 and Level 2 Safety and Environmental Cases (See Table 1), a Safety and Environmental Case **should** be developed in three parts as the system progresses through its lifecycle. Paragraphs 23 to 0 detail the development of a three part Safety Case.

20. A Level 3 Safety and Environmental Safety Case will have the same elements as 3 Part Safety Case but be contained in one document that still provides clarity on the residual risk. The SEMC **should** agree and document the depth of rigor and reporting required.

21. A Level 4 Safety and Environmental Case **should** be a risk assessment supported by a suitable and sufficient safe system of work.

22. Paragraphs 46 to 51 detail the development of the Environmental Case.

The Three Part Safety Case

23. The Safety Case **should** be structured in this way to give clarity to those responsible for its development. The three parts of the Safety Case are:

a. Part 1 – Requirements;

b. Part 2 – Design;

c. Part 3 - Operation & Support.

24. The relationship between each part of a Safety Case and an Environmental Case throughout a system's life is shown in Figure 1.

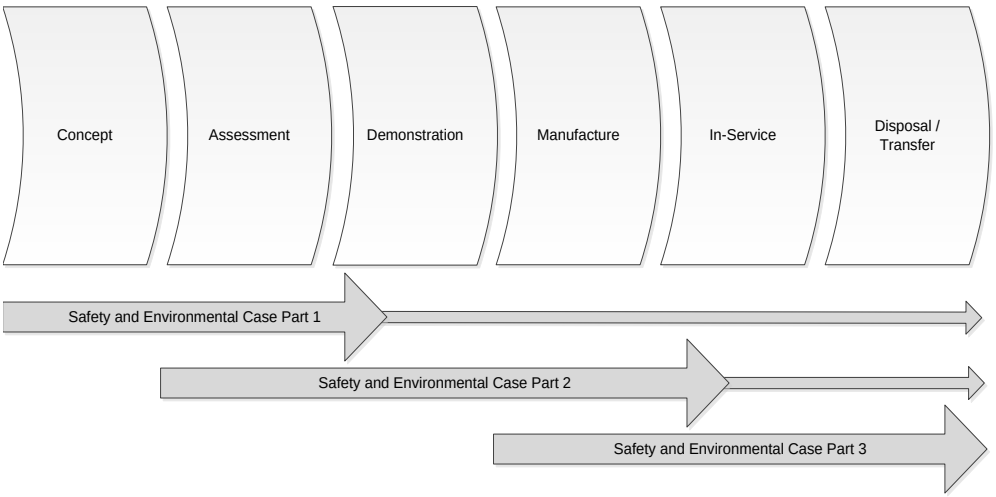


Figure 1. Relationship between the Safety and Environmental Case and the Lifecycle.

Part 1 Safety Case

25. The aim of the Part 1 Safety Case **should** be to identify safety requirements for the system.

26. The Part 1 Safety Case **should** be initiated at the Concept phase and maintained throughout the life of the system, if and when further information becomes available, although the main effort **should** be applied during the initial stages of a system(s) lifecycle.

27. The Part 1 Safety Case **should** examine the User Requirement Document (URD) in order to refine and establish the safety requirements for the system, the likely risks that meeting the User requirements may present and the criteria against which safety performance will be measured.

28. The Part 1 Safety Case **should** document whether equipment is regarded as a 'System' or a 'Systems of Systems'[32].

29. The Part 1 Safety Case **should** support the development of the System Requirement Document (SRD).

30. The Part 1 Safety Case **should** address the following:

a. The system operating context and its environment;

b. Legislative and regulatory requirements;

c. MOD Policy and Certification requirements;

d. Civil or MOD Standards to be complied with;

e. Risk targets, tolerability criteria and the application of the ALARP principle;

f. Safety Integrity requirements;

g. Derived safety requirements.

31. All requirements identified in paragraph 30 **should** be derived from a safety and compliance assessment of the capability or concept being developed.

32. The requirements identified from this part of the Safety Case, which are based on the URD, **should** be published in the SRD. As the system matures and the URD and SRD are refined, the Safety Case **should** be updated and reviewed by the SEMC.

Part 2 Safety Case

33. The aim of the Part 2 Safety Case **should** be to provide sufficient evidence and arguments that the system can meet the safety requirements established in the SRD and the Part 1 Safety Case.

[32] Further requirements for a "System of Systems" are detailed in the DCoP (D) for Regulation 5 on Safety and Environmental Case Interfaces

34. The Part 2 Safety Case **should** be established for each capability option being explored, and when a solution is identified, the Part 2 Safety Case **should** be progressively refined and updated for the chosen solution through life.

35. The Part 2 Safety Case **should** provide the justification and evidence that a system design is acceptably safe and that risk has been reduced so far as reasonably practicable. This evidence will be used to support the In-Service ALARP statements within the Part 3 Safety Case.

36. The Part 2 Safety Case **should** show how risks have been mitigated and identify the residual risks which will require mitigation during Operation and Support of the system.

37. The Part 2 Safety Case **should** be developed progressively throughout the development of a system, prior to acceptance into service.

38. The Part 2 Safety Case **should** also demonstrate compliance with applicable legislation and regulations and identify any non-compliances and the action required to address these.

Part 3 Safety Case

39. The aim of the Part 3 Safety Case **should** be to demonstrate that the residual risk is ALARP.

40. The Part 3 Safety Case **should** support System Acceptance.

41. The Part 3 Safety Case **should** confirm that all safety requirements have been met, that risks have been reduced to ALARP and that all the necessary arrangements are in place, including limitations if necessary, to ensure the proper and acceptably safe operation and support of the system on its introduction into service and throughout the system(s) lifecycle.

42. Any residual risks and their proposed, or actual, mitigations **should** be examined and a case made that all appropriate controls have been identified and are in place.

43. The Part 3 Safety Case **should** demonstrate that:

a. The Maintenance Policy and arrangements meet the requirements of the system(s)[33];

b. The Training Policy and arrangements meet any requirements stipulated by the system(s);

c. Operating documentation is available that identifies any requirements for the acceptably safe operation of the system;

d. Limitations of use are identified and any safety related restrictions have been imposed on the operation of the system, i.e. safe operating envelope;

e. Emergency and Contingency arrangements are identified and in place;

f. Arrangements are in place for monitoring safety performance and maintaining the Safety Case;

g. Resources are in place to maintain the acceptably safe operation of the system through life and these are identified in the SEMP.

Hazard Log for the Safety Case

44. A hazard log **should** be used to record the results of the hazard identification and analysis, the risk assessments and ALARP justification. Guidance regarding the content of a hazard log is provided in paragraph 90.

45. The hazard log tool selected **should** be appropriate for the complexity of the system(s). For example, for a Level 1 or 2 Safety Case a software based Hazard Log tool could be used. For Level 3 or 4 Safety Case, a simplified software solution could be adopted.

Developing the Environmental Case

46. The Environmental Case **should** be developed in accordance with Regulation 8 and JSP 418 and combined with the Safety Case at each Part. Where the Safety and Environmental Management Committee (SEMC) has decided not to combine the Environmental Case with the Safety Case, the Environmental Case Summary Reports **should** be issued at the same key milestones as the Safety Case Summary Reports (Refer to Paragraph 57).

47. The Environmental Case is an iterative process and documents making up the Environmental Case **should** be updated throughout the programme to include new information as it becomes available to provide a robust case and reported in Safety and Environmental Case Summary Reports for commercial, programme milestones as well as key activities such as trial and testing.

48. All stakeholders associated with the land system(s) **should** be identified to support the study and to help inform decisions (and those that need to be informed about decisions) on environmental protection.

[33] Refer to Paragraphs 8, 9 and 10 in the DCoP (I) for Regulation 15 on Equipment Care and Configuration Management

49. Legislation applicable to environmental aspects of land system(s) design, manufacture, operation and disposal **should** be identified. Where derogations, exemptions or disapplications apply, land systems **should** produce outcomes which are, so far as is reasonably practicable, at least as good as those required by UK legislation. Where environmental aspects exist which are not governed by applicable regulation or standards then the BPEO **should** always be demonstrated.

50. Identification and assessment of the environmental impacts and risks **should** be conducted throughout the lifecycle of the land system(s). Operational Controls and mitigations (for the land system(s) and its operations) **should** be identified that minimise environmental impact and risk across the lifecycle. BPEO Statements **should** be prepared, see Regulation 8 to justify that the solution provides the most benefits, or the least damage, to the environment at an acceptable cost in both the long term as well as in the short term. The assessment **should** be conducted proportionately to the severity of environmental impact or risk.

51. Operational Controls **should** be implemented for land systems. Objectives and Targets **should** be set, regarding reduction in environmental impact and risk, as far as reasonably practicable. These Operational Controls, Objectives and Targets **should** be monitored through life as part of the SEMC and adjusted as appropriate.

Human Factors

52. Human Factors (HF) **should** be considered during the development of the Safety and Environmental Case. Guidance is provided at paragraph 103.

Safety and Environmental Case Summary Reports

53. Where the land system has a combined Safety and Environmental Case and associated Safety and Environmental Case Summary Reports then the Environmental Case **should** be summarised in those reports as and when they are issued.

54. As a Safety and Environmental Case develops it **should** be supported by a series of Safety and Environmental Case Summary Reports. These reports **should** summarise the arguments made and the evidence provided at various stages of the land systems development. They **should** document progress against the safety and environmental programme (typically documented in the SEMP) and the arrangements for managing safety through life.

55. A Safety and Environmental Case Summary Report **should** be available to all stakeholders and **should** be produced at key points in the land system's lifecycle. The following **should** be considered to be points at which a Safety and Environmental Case Summary Report is required:

a. Prior to system(s) development commencing - to set out the strategy for achieving the safety and environmental requirements and the issues to be dealt with;

b. Prior to trials - to ensure that risks to personnel are identified, controlled and managed (particularly where safety and operating documentation is incomplete); and to ensure that risks to the environment are under control;

c. Prior to System Acceptance - to demonstrate that the agreed levels of safety performance and environmental protection have been achieved;

d. Any time that the Safety and Environmental Case is reviewed and updated – refer to paragraph 63.

56. The contents and structure of the Safety and Environmental Case summary reports **should** be proportionate to the Safety and Environmental Case Level.

57. Where a SEMC decide to have a separate Safety Case and Environmental Case then the Environmental Case Summary Reports **should** be produced at key points in the land system's lifecycle – refer to paragraphs 55 a to d.

Sign Off

58. The Safety and Environmental Case **should** be signed-off at various stages throughout land system's lifecycle[34], via the Safety and Environmental Case Summary Report. When a Safety and Environmental Case Summary Report is generated, it **should** be reviewed and agreed by the relevant stakeholders at the SEMC.

59. The authorisation of the Safety and Environmental Case Summary Report **should** be signed-off by the applicable TLB. For a Part 3 Safety and Environmental Case, the reports **should** be signed off:

a. Part 1 – by the Acquisition Organisation;

b. Part 2 – by the Acquisition Organisation;

c. Part 3 – by the Acquisition Organisation and by the Capability Sponsor (on behalf of the Front Line Command);

d. Trials – by the Acquisition Organisation and by the Capability Sponsor (on behalf of the Front Line Command).

60. Where a three part Safety and Environmental Case is not used, the Safety and Environmental Case **should** be signed off by the Acquisition Organisation and when In-Service / Trials also by the relevant Capability Sponsor (on behalf of the Front Line Command).

[34] Refer to Paragraph 55

61. The signature sheet of a Safety and Environmental Case Summary Report **should** include as a minimum:

a. The Author;

b. Technical Reviewer. Evidence that it has undergone a proportionate technical review. The competency of the reviewer **should** be proportionate to the Safety and Environmental Case Level;

c. Acquisition Organisation;

d. Capability Sponsor (on behalf of the Front Line Command) – at the In-Service / Trials stage (Refer to Paras 59 and 60).

62. At the In-Service / Trials phases the:

a. Acquisition Organisation is signing to provide assurance that the land system is "Safe to Operate" given the application and the operating envelope, as defined within the land system's Safety and Environmental Case; and the residual risks are defined in terms that enables the Front Line Command to manage those risks.

b. Capability Sponsor (on behalf of the Front Line Command) is signing to ensure that given the activity, the land system will be used within the application and operating envelope as defined within the land system's Safety and Environmental Case.

Monitoring and Review of the Safety and Environmental Case

63. The Safety and Environmental Case (all relevant parts) **should** be reviewed, as a minimum, on an annual basis and when:

a. Any of the functional requirements, constraints or assumptions change through life;

b. There is a change to an interface with other systems;

c. Incidents, accidents or failures occur;

d. Modifications to the system(s) are introduced;

e. There are changes to legislation, regulations or policy;

f. There is a change in its application or its operating environment;

g. On disposal.

64. The extent of the review **should** be proportionate to the Safety and Environmental Case Level and the residual risks of the land system. This review **should** be documented, for example, minutes of the meeting.

65. Following the review the relevant documents within the Safety and Environmental Case **should** be update with any new information, for example, Hazard Log, operating procedures, maintenance procedures etc. The SEMC **should** decide whether an updated Safety and Environmental Case Summary Report for the

land system is required. If, as part of a review, no changes are identified then this **should** be documented.

Industry

66. Where industry have been contracted to support the development of the land systems Safety and Environmental Case, the MOD **should** ensure that:

a. Adequate arrangements are in place and actioned, to control and manage any residual risks at the contracted interfaces;

b. The roles and responsibilities for Industry are clearly defined, agreed and recorded.

67. The accountability of the land system Safety and Environmental Case cannot be transferred to Industry and remains with the Capability Sponsor.

Rail System Structural Integrity

68. For rail systems the Safety Case needs to consider structural integrity. The structural integrity of trains **should** be maintained during normal operations and afford effective protection to people and goods carried in the event of an accident.

69. To help you achieve this outcome, you **should** at least consider:

a. The maximum loads foreseeably arising in normal operations;

b. The effects of a collision and the crashworthiness of a vehicle;

c. The structural compatibility of all trains using the route unless there are arrangements to reduce further the risk of collision;

d. The level of containment and containment arrangements of any goods carried and any foreseeable movement that may occur;

e. The protection from and containment of fire;

f. The integrity of attachment of equipment;

g. The range and compatibility of coupling devices and other inter-train connections;

h. Compatibility with buffer stops or similar train arrestor devices;

i. The arrangements for lifting the vehicle for both normal maintenance and emergency situations; and

j. The ability of glazing to resist impact damage and withstand aerodynamic effects.

Safety of Powered Systems for Rail

70. For rail systems the Safety Case **should** consider the safety of powered systems. These include on-board electrical, mechanical, air or hydraulic systems or equipment including electric traction current collection, main and auxiliary power systems and all electrical control systems including software.

71. To help ensure safe systems, you **should** consider:

a. Interference with other (rail) powered control systems;

b. The positioning and protection of rail equipment and electrical conductors to avoid accidental contact by people;

c. The effect of the loss of power supply and their effects;

d. The effect of the loss of safety critical systems;

e. Retention of and protection from failed mechanical components

f. The limitation of fire load and its protection, ignition sources, fire spread and smoke and fumes;

g. Unauthorised access to, or use of, equipment (including software systems) and the prevention of malicious interference;

h. The availability of rail powered systems in degraded operations or emergency situations;

i. Bonding and short-circuit protection including RCD protection of sockets available for use by passengers; and

j. Avoidance or control of electro-magnetic fields which are known to be harmful to people.

k. The safe management of any stored energy devices on the train in normal and emergency situations.

l. The arrangements for safe maintenance of rail powered systems, including de-energisation during maintenance.

m. The control of emissions; and

n. The control of noise.

Speed Control and Braking on Rail Systems

72. For rail systems, the Safety Case **should** consider speed control and braking. The speed control system may include systems other than the braking system.

73. To help ensure safe systems, the following **should** be considered:

a. The requirement for the braking system to be continuous, capable of stopping and holding a divided train, and holding a stabled train;

b. The acceleration and deceleration rates and the rate of change of those rates to avoid endangering the goods carried or damaging the vehicles and their couplings;

c. The performance of the braking system under all foreseeable conditions of adhesion;

d. The incapacity of the train driver;

e. Redundancy in the service braking;

f. The availability of the braking system on demand;

g. The overall braking performance provided by one or more braking systems;

h. The transition between different types and combinations of braking systems;

i. The gradients of the railway;

j. The compatibility with the track and, in particular, the forces imposed on the track;

k. The compatibility of the service braking performance with the train control system;

l. The compatibility with the electric traction system, including the compatibility of any regenerative braking systems and the effects of the receptivity of the traction system on braking performance;

m. Minimising the risk of 'dragging' brakes;

n. Minimising the release of toxic or other harmful substances from brake pads or blocks;

o. The provision of a reliable indication of speed; and

p. The compatibility with train control or driver advisory systems as they develop.

Rail Systems Running Gear

74. For rail systems the Safety Case **should** consider the running gear, to help achieve safe rail systems, you **should** consider:

a. The compatibility of the wheel and rail interface;

b. The range of train operating speeds;

c. The compatibility with the track geometry;

d. The foreseeable track maintenance tolerances and the risk of the track being outside the normal condition tolerances;

e. The arrangements for transfer between tracks;

f. The effects of traction and braking forces;

g. The effects of permitted forces imparted to the track or train body and within the components of the running gear;

h. The risk and effects of component failure, particularly of wheel-sets and bearings;

i. The effects of collisions with obstacles and the provision of effective obstacle deflection;

j. The risk of derailment due to wheel unloading including from the influence of offset loads and locked suspensions;

k. Transfer of noise or vibration to the track or train body;

l. The integrity of attachment of equipment to the running gear; and

m. Effective electrical bonding of the vehicle to ensure safe operation on the railway.

Guidance Material

Safety Case

75. A Safety Case is defined as *"A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment."*

76. A simple way of understanding the Safety Case is to consider the following basic questions:

a. What are you looking at? – (system description, scope and assumptions);

b. What could go wrong? – (hazard identification and analysis);

c. How bad could it be? – (risk estimation);

d. What has been or can be done about it? – (risk evaluation and risk reduction plans);

e. What if it happens? – (emergency and contingency arrangements).

77. The Safety Case should answer these questions for the whole system under consideration and for the uses defined. The Safety Case should also use plain English to make it easily understandable to all recipients.

78. The Haddon-Cave report into the Nimrod accident[35] raised a number of issues associated with the Safety Case, stating: “The current shortcomings of the Safety Cases in the military environment include: bureaucratic length; obscure language; a failure to see the woods from the trees; archaeological documentary exercises; routine outsourcing to industry; lack of vital operator input; disproportionality; ignoring of age issues; compliance-only exercises; audits of process only; and poor assumptions of safety and ‘shelf-ware’.”

79. Haddon-Cave said “Safety Case should be an aid to thinking, not an end in themselves” and should consider the following principles:

a. Succinct;

b. Home-grown;

c. Accessible;

d. Proportionate;

e. Easy to understand; and

f. Document-lite.

80. Key principles of a Safety Case are as follows:

a. Is owned by the Capability Sponsor / Lead User for the defence activity as a means of documenting the hazards to and risks from conducting the activity, and the management of the necessary controls and mitigations;

b. Is evidence to support a claim by the Capability Sponsor / Lead User that they consider that the defence activity is safe with the reasoning for that conclusion;

c. Has evidence that the boundary for the assessment of the defence activity e.g. context of use, operational environment, interfaces etc. is defined;

d. Starts with a short executive summary outlining, in plain English, the principal hazards and environmental impacts which have been identified and the reasons why the safety risks are ALARP;

e. Identifies any residual safety risks and how they should be mitigated or managed;

f. Is appropriate and proportionate in its rigour to the activity to be conducted, the consequences of failure and the needs of the Capability Sponsor / Lead User (and regulator(s) as necessary);

g. Includes evidence and analysis from each defence line of development (See Para 84) that contributes to control and mitigation of hazards;

[35] The Nimrod Review, An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, Charles Haddon-Cave QC, 28th October 2009

h. Defines the safe operating envelope of any equipment / materiel / infrastructure used in conducting the activity;

i. Addresses and defines interfaces with other related activities and their risk assessments / Safety Cases;

j. Is able to address urgent and short-term changes to hazards, consider changes to risk and the need to adjust controls and mitigations;

k. Is maintained and reviewed, being informed by feedback from conducting the activity, from any incident or accident, by the equipment / materiel state, by technological developments, by changes to appreciation of hazards and by changes to controls and mitigations (e.g. the availability of human or financial resources);

l. Documents any assumptions, dependencies and limitations that have been used or identifies and justifies the reasonableness of such assumptions;

m. Is available at appropriate milestones throughout the life of the activity, product, service or system;

n. Provides evidence that risks, outside the owning Capability Sponsor / Lead User's authority, have been referred and owned at an appropriate level of seniority;

81. Methodologies for establishing a Safety and Environmental Case are available in ASEMS Project Oriented Safety Management System (POSMS) manual and Defence Standard 00-056. Additional information on MOD Rail Safety Management can be found in JSP 790[36].

The Environmental Case

82. The Environmental Case is the complete set of documentation that is created during the project lifecycle relevant to the environmental management and assessment of the land system(s). The Environmental Case Report is a summary of the information, identifying the residual impacts and risks at a given point in time, whilst identifying the key actions taken to minimise the residual impact and risk. This can be provided as a stand-alone environmental summary report or as part of the Safety Case Report but must include an Environmental Impact Statement.

83. ASEMS POEMS provides process flowcharts to identify what activities should be carried out for each lifecycle phase.

Defence Line of Development

84. The Safety Case should consider the Defence Lines of Development (DLoD)[37] throughout the lifecycle of the land system: Training; Equipment; Personnel; Information; Concepts & Doctrine; Organisation; Infrastructure; and Logistics.

[36] JSP 790 is currently being re-written
[37] Defence Instructions and Notices, Defence Lines Of Development, 2005DIN03-012, 29 July 2005

85. There are 11 HS&EP Management Arrangements which overlay the 8 DLODs:

a. Applicable Legislation, Defence Regulations, Policy and Guidance;

b. Information Management;

c. Organisational Leadership, Culture, Capability and Change Management;

d. Personnel competence and training;

e. Risk Assessments and Safety Cases;

f. Equipment / Materiel and Infrastructure Design and Manufacture;

g. Equipment / Materiel and Infrastructure Maintenance;

h. Supervision and Control of Activities;

i. Incident Management and Learning from Experience;

j. Emergency Arrangements;

k. Self-assurance.

Structured Argument

86. Although Goal Structuring Notation (GSN)[38] is widely used in DE&S as a method for graphically representing a safety argument, the structure of the argument should be appropriate to the level of Safety and Environmental Case being produced.

87. Structured Safety Case arguments for simple land systems, i.e. level 3, can be built using linked tables of claims, supporting evidence and explanatory arguments. For more complicated systems it is often helpful to use a graphical notation such as the Claims, Arguments and Evidence (CAE) notation developed by Adelard[39].

88. Further guidance on techniques to support safety arguments can be found in the Safety Managers Toolkit in ASEMS.

Evidence

89. The degree of evidence required and work involved in developing a Safety and Environmental Case should be commensurate with the risk posed by a particular system, its complexity and maturity. There is a need to gather and manage the evidence throughout the life of project from concept to beyond disposal. Retention of evidence beyond disposal must be considered as claims can arise for some time after the equipment disposal.

[38] www.goalstructuringnotation.info
[39] http://www.adelard.com/asce/choosing-asce/cae.html

Hazard Log

90. A hazard log should contain at least the following information:

a. Hazards;

b. Controls / Mitigations;

c. Causes;

d. Accidents;

e. Risk Assessments;

f. ALARP justifications;

g. References e.g. standards, design documents, competent personnel at hazard identification and assessment meetings, Test Results, SEMC dates and decisions, etc.

91. The hazard log should clearly show the relationship between causes, hazards, accidents and mitigations and how the mitigations impact the risk assessment.

92. For Level 1 and 2 Safety and Environmental Cases it is recommended to use a Hazard Log software management tool, for example E-Cassandra. For Level 3 and 4 cases other suitable methods could be used to record and manage the Hazard Log.

93. Further guidance on the creation, development and maintenance of a Hazard Log is contained in Defence Standard 00-056.

Level 3 Safety and Environmental Case

94. A Level 3 Safety and Environmental Safety Case will have the same elements as a three part Safety Case but be contained in one document that still provides clarity on the residual risk. For example:

a. The Land system may share a SEMP with other land systems;

b. The Hazard Log may be developed within a simple spread sheet;

c. A lower competency is required to develop one;

d. No requirement for independent review / audit, unless the land system has the potential to result in death or multiple major injuries;

e. Depth of the body of evidence. Safety argument requirements will be less, unless land system has the potential to result in death or multiple major injuries.

95. The depth of the Level 3 Safety and Environmental Case will be proportionately dependent on how the land system is procured (See Figure 2 below).

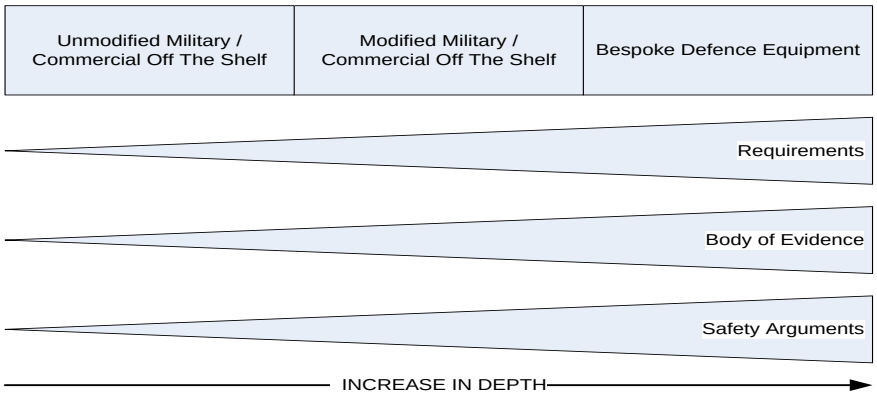


Figure 2. Level 3 Safety and Environmental Case Proportionality.

96. Level 3 Safety and Environmental Cases are typically modified military or commercial "Off The Shelf (OTS)". They will require a programme of work that shows that any modifications undertaken do not affect the inherent safety of the system and that it is safe to use for its intended purpose. As with any other system a Safety Case is required to provide the evidence that the system is safe to use, particular attention should be given to identifying the additional risks introduced by the modifications and the way in which they are to be mitigated.

97. Level 3 Safety and Environmental Case would include the development of a Safety and Environmental Case Summary Report which should include (as a minimum):

a. Executive Summary;

b. Description, including scope and interfaces;

c. Assumptions;

d. Progress against SEMP;

(1) Summary of the organisation and arrangements in place. This should only include the specifics related to the land systems which reference to the overarching SEMS;

(2) Progress against SEMP;

(3) Summary of any safety issues since last publication, e.g. incidents, near misses, shortfalls, etc.

e. Meeting safety and environmental requirements;

(1) Summary on how the requirements have been identified and met;

(2) Detailing the risk management process undertaken with evidence to meetings;

(3) Result of the risk assessments;

(4) The residual risks that is, or is anticipated to be, posed by the land system;

(5) Declaration of ALARP.

f. Operational Information;

(1) Identify Safe Operating Envelope;

(2) Emergency / Contingency Arrangements;

(3) Summary of the Residual risks;

(4) Limitations on operational use, including info to support the End User balancing operational imperatives;

(5) Reference to key documentation, e.g. Operating and maintenance procedures.

g. Conclusions and Recommendations, including any forward action items;

h. References;

i. Appendices;

(1) Hazard Log;

(2) Legislation Compliance Matrix.

98. It may be prudent to combine a number of land systems into a single Safety and Environmental Case Summary Report, where they are similar in nature.

99. Further guidance contained in POSMS manual and Defence Standard 00-056.

Level 4 Safety and Environmental Case

100. Level 4 Safety and Environmental Cases are typically “Off The Shelf” equipment / systems which will be operated in accordance with the guidelines set by the manufacturer.

101. Commercial Off The Shelf (COTS) equipment intended for sale on the EU market will have a CE mark which shows that it has achieved a set standard for that system. COTS equipment procured from other countries which is not intended for sale in the EU market may not have a CE marking; however this does not preclude its use provided it has a robust Safety Case. CE marking does not make a system safe to use and the MOD should as a minimum build a Safety Case to ensure the faceable risks posed by the equipment are considered and that any limitation of use set by the manufacturers guidelines are adhered to. Where the MOD intends to use the system outside of the operating conditions set by the manufacturer the Safety Case must consider these differences and provide the evidence to support the safe use of the equipment.

102. Level 4 Safety and Environmental Case would simply include a documented risk assessment supported by a Safe Systems of Work. Five steps are applied to ensure effective risk assessment and management:

a. The hazards which may affect the activity and are inherent within the activity are identified;

b. Those who might be harmed, and the degree of harm, are identified;

c. The identified hazards are assessed for their severity and likelihood, risks are evaluated and controls and mitigations are developed that reduce safety risks to ALARP. If risk to life is identified in the assessment, the arrangements of the relevant DH hierarchy are to be activated;

d. The result is recorded (as necessary) and implemented: if a commanding officer or manager, at any level, considers that resources (financial, human, material) available to them do not provide for controls or mitigations which reduce the safety risk ALARP, they are to refer this to a relevant higher commanding officer or manager for consideration and action and is not to proceed / continue with the activity;

e. The assessment is reviewed: in particular controls and mitigations are monitored to determine their continuing effectiveness; corrective actions are taken as necessary.

Human Factors

103. In order to address the safety aspects of human factors, the output from ergonomic studies, Human Factors Integration (HFI) activities, output from early human factors analysis and human error rates should be used.

104. Further guidance on Human Factors may be found in:

a. JSP 912 Human Factors Integration for Defence Systems;

b. Defence Standard (Def Stan) 00-250 Human Factors for Designers of Systems;

c. MOD HFI Process Handbook;

d. HFI ASG.

Software

105. The risks associated with the failure or unintended behaviour of Programmable Elements (PE) in land systems, including its integration, must be managed. PE is defined as a land system which is implemented in software or programmable hardware, which includes any device that can be customised, e.g. Application Specific Integrated Circuit (ASIC), Programmable Logic Devices (PLD) and Field Programmable Gate Array (FPGA).

106. To enable safe operation of a land system, component PEs will need to meet the required Design Integrity and fulfil the PE integrity principles (Def Stan 00-055:

a. Principle 1. PE safety requirements shall be defined to address the PE contribution to system hazards;

b. Principle 2. The intent of the PE safety requirements shall be maintained throughout requirements decomposition;

c. Principle 3. PE safety requirements shall be satisfied;

d. Principle 4. Hazardous behaviour of the PE shall be identified and mitigated – addressed by failure modes and supported by designing for safety;

e. Principle 5. The confidence established in addressing the other PE safety principles shall be commensurate to the contribution of the PE contribution to system risk and will be addressed by Design Integrity requirements.

107. PE cannot be generally safe or unsafe in itself, only in the context of its role in a land system; however the term 'PE safety' has been adopted as global term addressing the properties of PE to consider its role in relation to the safety of land systems.

108. Lack of Design Integrity can lead to the unintended behaviour of PE. These may result in a hazard or impair mitigation of a hazard within the land system and hence the MOD considers PE Design Integrity to be a significant safety issue.

109. Further guidance on PE safety is provided in:

a. IEC 61508 - Functional Safety of Electrical / Electronic / Programmable Electronic Safety related Systems;

b. IEC 26262 - Road Vehicles - Functional Safety;

c. Defence Standard 00-055, Requirements for Safety of PE in Defence Systems Part 1: Requirements and Guidance;

Environmental Management Process

110. To ensure that environmental impacts and risks are identified and appropriately managed, information on relevant stakeholders, their needs and possible contribution to the project is also collated and documented. It is also important to identify any environmental standards that potentially apply to the project. (Note that 'standards' in this context also includes legislation, agreements, MOD policies and strategies).

111. To ensure that the environmental assessment is coherent and consistent with the objective of BPEO it is necessary to identify the scope of the assessment, determine evaluation criteria and identify where areas of tradable capability exist.

112. The approach to environmental assessment must be proportionate to the severity of environmental impact or risk. For example particular attention should be paid, if aspects include any of the following:

a. Vehicle washing – resource depletion and effluent handling;

b. Energy use – resource efficiency;

c. Movement of equipment between different environments or watercourses - transfer of species leading to ecosystem damage;

d. Hazardous material use - especially in electronic equipment;

e. Emissions – discharges to air and water;

f. Management of waste – including disposal whilst in-service.

Environmental Impact Screening and Scoping

113. It is essential to undertake screening and scoping activities from the concept of a land system project or activity. Before assessment of risk or impacts can take place, all environmental aspects need to be identified and identification of options within the capability trade space. This is to be achieved using the stakeholder's knowledge and experience, gathering data from similar land systems or those land systems operating in similar environments. The depth of study should be proportionate to the risk and therefore it can be conducted in workshops or as a desk based study.

Environmental Impact Prioritisation

114. Environmental Impacts and Risks identified during Environmental Impact Screening and Scoping (EISS) activities must be prioritised to identify those that require further action to eliminate, mitigate or manage. The 'priority based on risk' evaluation is carried out to assess the severity of the likely environmental impact or risk against the frequency / duration of that impact or risk.[40]

Regulation 5 – Safety and Environmental Case Interfaces

[40] Refer to POEMS EMP03 for the details of this process

Regulation	**Those holding safety and environmental responsibilities shall ensure that all interfaces relating to safety and environmental protection between land systems and other systems are identified, assessed and managed effectively.**
Rationale	A Safety Case is necessary in order to demonstrate that a system is acceptably safe in use; all risk has been reduced to a level that is As Low As Reasonably Practicable (ALARP) and that the system complies with applicable legislation. An Environmental Case is required in order to demonstrate that applicable legislation has been complied with and that all environmental impacts and risk have been reduced as far as is reasonably practicable.
Defence Code of Practice	115. TLBs **should** have a process in place for the effective management of risks across the interfaces between land systems and other systems. Typically this process is recorded within a land system's SEMS[41]. 116. All interfaces between land systems and other systems **should** be identified, recorded and assessed for safety and environmental protection. 117. The roles and responsibilities for controlling and managing the residual risks across interfaces **should** be identified and recorded in a land system's SEMP. 118. Review and monitoring of the interfaces **should** be undertaken in accordance with Regulation 13, Monitoring and Reviewing Performance. **Ancillary Systems** 119. Where a hazard is identified on an ancillary system but the risk does not manifest itself until the ancillary system is attached to the host platform i.e. the risk does not exist in either system until they are interfaced with each other, a formally documented risk assessment of the hazard **should** be undertaken, so that relevant safety and environmental protection information can be communicated to the appropriate responsible persons. 120. A risk assessment **should** be conducted and recorded at the integrated system level and not at the ancillary system level, to demonstrate that the residual risks are tolerable / broadly acceptable and ALARP[42]. 121. The host platform **should** ensure that there is a valid Safety Case in place for the intrinsic safety of the ancillary system, before being attached to the host platform. This Safety Case **should** demonstrate that the residual risks associated with the intrinsic safety of the ancillary system have been assessed and are deemed to be tolerable / broadly acceptable and ALARP. The responsibility for the ancillary system's intrinsic Safety Case may not lie with the host platform. Where this is the case, the host platform **should** ensure that arrangements are in place to manage the interfaces with those who are responsible for the Safety Case of the ancillary system.

[41] Refer to the DCoP (B) for Regulation 2
[42] Refer to the DCoP (E) for Regulation 7

System of Systems

122. A System of Systems approach **should** be used for Safety and Environmental Case development where appropriate i.e. where a collection of component systems are grouped in order to provide an enhancement of functionality and performance compared to the sum of its constituent elements. Guidance is provided from paragraph 131 onwards.

123. A responsible person for the System of Systems **should** be identified and documented. This person **should** hold an appropriate level of authority, such as a Letter of Delegation.

124. In a System of Systems environment, the component systems' boundary conditions and assumptions may not be valid, so these **should** be assessed because additional hazards may exist where the different systems interact.

125. System of Systems hazards can be categorised by the nature of this interaction and **should** be assessed as part of the hazard identification and analysis process that **should** consider:

a. Cumulative hazards resulting from the additive effect of multiple systems operating in unison;

b. Interaction hazards generated as a result of interaction between systems;

c. Hazards arising from external influences (environment, people, other equipment etc.).

126. Through a System of Systems approach, the safety and environmental responsibilities do not change however there is greater emphasis upon the operational objective and the interdependent persons with safety and environmental responsibilities. Hazard mitigation and management should be implemented at the appropriate level to ensure safe performance of the overall System of Systems.

Guidance Material

Interface Management

127. Failure to successfully communicate maintenance activities, abnormal conditions, emergency response procedures, residual hazards, and hundreds of other items of safety critical information can lead to an incident. Therefore, a well-functioning SEMS depends on maintaining successful communication interfaces between each involved employee or stakeholder and the many other employees or stakeholders that person must interact with.

128. An interface management process is to facilitate agreements with other stakeholders regarding roles and responsibilities, timing for the provision of safety information and identification of safety critical interfaces. The key steps in the process are:

a. Identify that you have an interface;

b. Define the type of interface;

c. Identify the stakeholders involved;

d. Identify roles and responsibilities;

e. Identify how the interface is to be managed and controlled to ensure the validity of each side of the interface is managed;

f. Identify information to be exchanged;

g. Consider other factors: bounding information, what if things go wrong, do they know? when does the interface finish?

h. Undertake a review and update.

129. An interface is a point / boundary where two independent organisations, systems, hardware or software, etc. meet and act on or communicate with one another. At an organisational level this could relate to safety and environmental management systems. There can be external interfaces between the MOD and Industry or internal interfaces between different MOD land organisations; for example, Army Command and DE&S Platform teams. At a system level this could relate to hardware; the wires, plugs and sockets that hardware devices use to communicate with each other or software; the languages and codes that the applications use to communicate with each other and with hardware.

<u>Interface Management Further reading</u>

130. See Interface Management Effective information exchange through improved communication by Josh Caglar, P.E. and Mike Connolly, ABB Inc., Houston 2007.

System of Systems

131. System of Systems can be defined as an interoperating collection of component systems that produce results unachievable by the individual systems alone.

132. The phases of system development, integration, operation (and potentially disposal) should be undertaken in the context of a broader System of Systems capability.

133. Through considering the shared objective and role within it, interfacing issues may be considered.

134. Emergent Properties may impact safety as a result of the interaction of systems operating together. For example:

a. Information transmitted from a communication system which provides additional mitigation measures in an interdependent system;

b. Weight from Soldiers carrying multiple pieces of equipment in order to enhance capability, each increasing the overall weight to be carried by the individual;

c. Troops all working together to achieve a shared objective;

d. Interference between two independent systems that when operated together prevent the other from performing as designed.

135. Hazards may emerge as a direct result of systems operating together e.g. friendly fire; detection of Infrared footprint, thermal loading etc. This should be assessed and managed appropriately.

136. The following diagram (Figure 3) illustrates the potential for new hazards emerging as a result of interaction between systems.

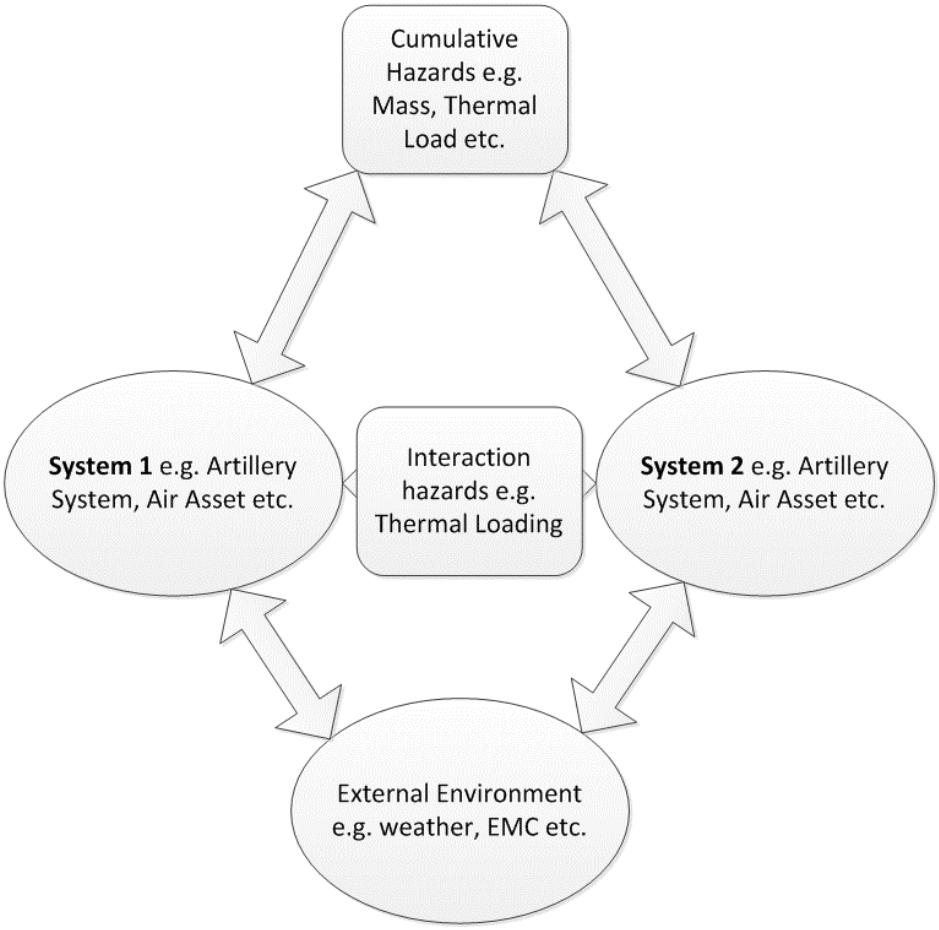


Figure 3. Interaction Hazards

137. Hazard identification and analysis should be conducted in the standard manner but focussing on the interactions between systems.

138. Table 3 provides some examples of the keywords and hazards that may emerge as a result of the interactions.

Table 3. Examples of Interaction Keywords and Hazards

Hazard Group	Hazard Keywords	Example Hazards
Physical	Contact Transmission of solids Transmission of liquids Transmission of gases Transmission of nuclear isotopes Transmission of biological organisms	Excessive weight of equipment - total load exceeds maximum safe carry load Ejected component (e.g. shell casing) impacts adjacent equipment Sharp edge of equipment contacts and punctures adjacent equipment casing Emission of exhaust gases from equipment enters intake of adjacent equipment
Energy	Thermal Chemical Electrical Radiant (EMC) Nuclear Magnetic Elastic Sound Potential Kinetic Luminous	Excessive thermal emission from electrical equipment – excessive heating Excessive electro-magnetic emissions – EMC signature too large Excessive sound emissions – noise signature too large Thermal emission from equipment heats adjacent equipment above maximum operating temperature Equipment contacts adjacent live equipment causing short circuit Electro-magnetic emission from equipment causes interference
Information	Omission - the interaction does not occur Commission - the interaction occurs when not expected Early - the interaction occurs too early Late - the interaction occurs too late Too much –a parameter associated with the interaction is increased Too little - a parameter associated with the interaction is decreased Conflicting -the interaction conflicts with another interaction on the channel	Interference causes degradation of transmitted / received signal quality Interference prevents transmission / receipt of signal Processing delays signal being transmitted / received

139. Systems are a combination of interacting elements organised to achieve one or more stated purposes.

140. Some larger and / or more complicated systems may be made up of other systems, but may not be defined as a ‘System of Systems’.

141. Systems of Systems:

a. Share, or are likely to share, an overall objective;

b. Are interdependent and contribute different functions to achieve a shared objective;

c. Consist of systems which have been developed in their own right;

d. Individual systems may communicate directly with one another;

e. Reduce capability if a system was removed but may still operate.

142. The benefits with a System of Systems approach are that:

a. An interdependent environment is created;

(1) On the smaller scale, it enables platforms to manage changes to their role and configuration;

(2) On the larger scale, it facilitates a change in operational need and so the utilised capability can be adapted in use and operation easily (i.e. Peacekeeping to Focused Intervention).

b. Greater understanding of how systems interact to deliver Defence Capability is achieved, improving effectiveness on operations without creating additional risks;

c. Training requirements for Users can be streamlined;

d. Costs and resources can be saved in the longer term, removing the need to procure multiple variations of similar equipment.

143. Risks can materialise if evolution does not occur with:

a. The method of compiling a Safety Case, causing one or more systems to be taken outside their intended operational envelope because the interface relationships have not been considered appropriately. This increases risk either unnecessarily and / or in an uncontrolled manner;

b. Different risk tolerability criteria have been used for the component systems within a System of Systems;

c. Incident reporting systems to ensure information is disseminated appropriately through the System of System User community, and remove the reliance on Military knowledge and training to prevent hazardous instances escalating.

144. Information made readily available within the Systems of Systems scope should include, but not be limited to:

a. Scope / boundary;

b. Assumptions;

c. Limitations of use;

d. Recommendations;

e. Risk matrix used;

f. Definitions;

g. Operational parameters;

h. Operational scenarios considered;

i. Emergent properties;

j. Where appropriate, assurance of the integrity of the information supplied.

Regulation 6 – Transferring a Safety and Environmental Case

Regulation	**Those holding safety and environmental responsibilities shall ensure that due diligence is exercised when responsibility for a safety and environmental case is transferred.**
Rationale	A Safety Case is necessary in order to demonstrate that a system is acceptably safe in use; all risk has been reduced to a level that is As Low As Reasonably Practicable (ALARP) and that the system complies with applicable legislation. An Environmental Case is required in order to demonstrate that applicable legislation has been complied with and that all environmental impacts and risk have been reduced as far as is reasonably practicable.
Defence Code of Practice	145. Where a Safety and Environmental Case is to be handed over, the receiver who is taking over the responsibility for the Safety and Environmental Case **should** be identified together with those elements of the Safety and Environmental Case that are being transferred. 146. The receiver **should** be competent to undertake the role and hold the appropriate delegated responsibility, e.g. a formal letter of safety delegation. The donor **should** be satisfied that the receiver has the competence to undertake the role. 147. The instance when the Safety and Environmental Case will be transferred **should** be identified at the earliest opportunity, to allow timely engagement with appropriate stakeholders involved in the transfer. 148. An assessment of the proposed transfer **should** be undertaken and documented by the receiver. This assessment **should** consider whether the proposed transfer would adversely affect the existing arrangements for conducting safety and environmental protection activities. As a minimum, the following actions **should** be undertaken by the donor: a. A review and update of the Safety and Environmental Management Plan and any incomplete or outstanding risk management activities identified; b. Review and update (where deemed necessary) of the extant Safety and Environmental Case Report and any incomplete or outstanding risk management activities identified. 149. If the receiver rejects the transfer as a result of their assessment, the receiver **should** inform the donor and document the reasons why. If the donor and the receiver cannot mitigate the issues then this **should** be resolved by a higher authority. 150. A plan for transferring the Safety and Environmental Case **should** be developed, taking into consideration the assessment made for the transfer. The plan **should** be proportionate to the complexity of the transfer process and magnitude of risks. The plan **should** describe how the transfer will be executed and identify specific actions, time limits, and responsibilities for

addressing any safety / environmental protection issues or any negative impact prior to the change being implemented.

151. The plan **should** be approved prior to handover by the receiver and donor. If any risks associated with the change were required to be referred to a higher authority, then the plan **should** be authorised by the higher authority.

152. When the Safety and Environmental Case is transferred, all relevant documentation **should** be updated to reflect the transfer, and the transfer **should** be communicated to all relevant personnel.

153. Written acceptance of the Safety and Environmental Case **should** be provided by the receiver to the donor after the transfer has taken place.

154. There will always be a degree of uncertainty as to the impact of change. Therefore, the Safety and Environmental Case **should** be reviewed following transfer to demonstrate that the arrangements for conducting activities safely and for providing environmental protection have not been degraded.

Guidance Material

Examples

155. Examples of when a Safety and Environmental Case may be transferred include:

a. Transfer to a different area of the organisation;

b. An individual leaves their post;

c. Disposal of equipment / systems.

Assessment

156. When the receiver is undertaking the assessment of the proposed transfer, the following factors should be considered:

a. **Responsibility** - Have you or will you have the appropriate delegated responsibility?

b. **Competency** - Are you and your team competent to undertake the role? Do you or your team require additional training? And if so do you have sufficient resource to support the supervision of untrained personnel?

c. **Resources –** Do you have suitable and sufficient resources to manage and maintain the Safety and Environmental Case? For example, resources could be manpower or budget;

d. **Documentation –** Consider how much effort and time would be required to update your existing Safety and Environmental Management System. In addition, consider the time and effort for updating the documentation associated with the Safety and Environmental Case being transferred;

e. **Communication** – Are you aware of all stakeholders who would need to be informed and what interfaces[43] need to be reviewed?

f. **Timescales** – Are the timescales for transfer realistic? Will the transfer overlap with a key milestone on the land system's Acquisition system, for example In-Service Date? If so, then time of transfer may need to be reconsidered.

Review following transfer

157. When reviewing the Safety and Environmental Case following transfer, the following questions may be useful to consider:

a. Have actions identified within the plan been completed?

b. Are the revised roles and responsibilities clear and relevant are stakeholders documented?

c. Have any additional / unexpected issues or training needs been identified?

d. Have there been impacts from interactions with other changes, and how have they been managed?

e. Have there been impacts on performance indicators?

f. Has there been any impact on morale that could adversely affect the safety culture or the Safety and Environmental Case?

Safety and Environmental Case sign-off

158. Guidance for the Safety and Environmental Case sign-off is provided in the DCoP (D) for Regulation 4 - Safety and Environmental Cases.

Further Guidance

159. The transfer of a Safety and Environmental Case is a type of organisational change. Further guidance on organisational change can be found in JSP 375 Management of Health and Safety in Defence, Part 2 Volume 1: Guidance, Chapter 35, Organisational Change, Version 1, January 2016.

[43] Refer to the DCoP (D) for Regulation 5

DCoP E - Safety and Environmental Risk Management

Regulation 7 – As Low As Reasonably Practicable (ALARP)

Regulation	**Those holding safety responsibilities shall ensure that the residual risk posed by the land system(s) has been reduced to a level that is ALARP.**
Rationale	The Management of Health and Safety at Work Regulations (1999[44]) (MHSWR) require that employers assess the risk created by their undertaking and that all employers assess risk to the health and safety of anyone that may be affected by their activities. This includes employers, employees and members of the public and the Health and Safety and Work etc. Act 1974 (HSWA) imposes general duties on every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all their employees. MOD must fulfil its statutory obligations and its common-law duty of care whilst maintaining Defence capability. Requirements have been placed on those holding safety and environmental responsibilities to demonstrate that residual risk is at a level that is As Low As Reasonably Practicable (ALARP)[45] and is adequately controlled. The Secretary of State for Defence demands that we protect the environment. Potential risks to the environment must be reduced or managed as far as reasonably practicable in order to comply with the Environmental Protection Act 1990[46].
Defence Code of Practice	1. The residual risks associated with land systems **should** be tolerable or broadly acceptable, and ALARP. In order to demonstrate that the residual risks are tolerable or broadly acceptable, and ALARP a risk management process **should** be followed. This process **should** be documented and the Safety and Environmental Case[47] **should** demonstrate that a suitable and sufficient risk management process has been followed which is proportionate to the perceived level of risk.

[44] As amended 2003
[45] SFAIRP is a legal term that is incorporated in the MHSWR. ALARP is the term used in safety engineering and is commonly considered to be analogous to SFAIRP. Ultimately, if a prosecution was brought under the MHSWR, a court of law would decide if a safety argument made on the basis of ALARP satisfies the demands of SFAIRP
[46] Individual environmental protection legislation refers to terms such as 'As Low As Reasonably Achievable', 'Best Available Techniques', 'Best Practicable Environmental Option (BPEO)' which have subtle variations of meaning. For brevity in this JSP, 'selection of BPEO' is used to describe the acceptable reduction of environmental risk
[47] Refer to the DCoP (D) for Regulation 4

Risk Management Process

2. A Risk Management Process **should** be led and undertaken by competent[48] people.

3. Risk Management is about identifying sensible measures to control the residual risk. Risk management has four key stages as illustrated in Figure 1.

4. Further guidance on the approaches and techniques that may be applied to these four stages, including the ALARP judgement, is discussed in the remainder of this document.

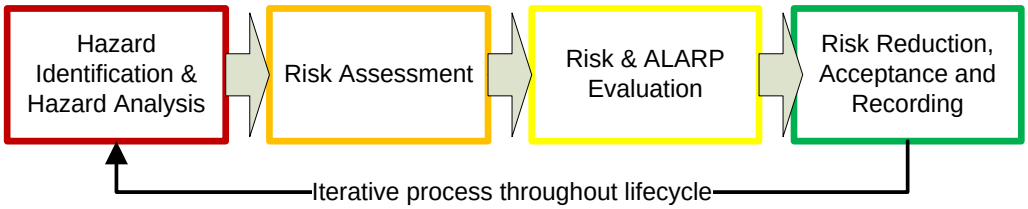


Figure 1. Four Stage Risk Management Process

STAGE 1

Hazard Identification

5. All hazards associated with a land system, given its application and operating environment **should** be identified and recorded, using a suitable and sufficient technique.

6. It is important to use exploratory methods to identify possible hazards, but a safety study must consider hazards identified by any means: previous incidents, checklists, design reviews etc. Whatever techniques are used, good hazard identification will benefit from experience and imagination. When conducting a Hazard Identification exercise for a safety study, various techniques are available.

Hazard Analysis

7. Each credible Hazard **should** be analysed and documented. The hazard analysis **should** be appropriate to the technology (cause), and the potential accident. The analysis **should** include as appropriate zonal and particular risk analysis.

8. Hazard Analysis is the process of investigating and describing the hazards, accidents and accident sequences for a system or activity of interest. It results in an understanding of the possible accident sequences, from causes to outcomes. This understanding then allows the subsequent Risk Reduction process to determine what risk control measures are possible and necessary.

[48] Refer to the DCoP (C) for Regulation 3

STAGE 2

Risk Assessment

9. A suitable and sufficient risk assessment **should** be undertaken for each credible accident scenario identified, to determine its level of risk.

10. The level of risk is determined by combining the frequency (likelihood of occurrence) of an accident and the consequence (severity of harm) of that accident. The qualitative judgement can be informed by quantitative data to determine the appropriate risk classification. It is likely that a more quantitative approach will be required where a system poses significant risk.

11. The risk assessment **should** be based upon a risk tolerability matrix which will be tailored to the system and have justification supporting its structure. This matrix provides the framework for the prioritisation of risk and accident according to its tolerability.

12. It is important to ensure the matrix has been compiled in a way that can be understood by those needing to use it throughout the entire life of the system. To do this it is vital that clear definitions are given for all the terminology used to identify the different criteria (e.g. non-numerical descriptors of probability, units of likelihood, fleet or single equipment, etc.).

13. It is important to note that when setting tolerability criteria, consideration **should** be given to different groups of people who may be harmed by the equipment. This can be achieved by defining different severity categories for the general public, indirectly involved personnel and Users of other equipment which are more stringent than those for trained personnel who are directly involved with the system and understand the hazards it poses.

14. In a qualitative assessment, likelihood and severity are estimated using subjective terms such as ‘Frequently’, ‘Sometimes’ and ‘Rarely’. These are combined to give a qualitative estimate of risk, such as ‘High’, ‘Medium’ and ‘Low’. In a quantitative assessment, likelihood and severity are estimated using numeric terms, e.g. ‘1 x 10-6 hazardous events per operating hour’, or ‘weekly’. They are combined to give a numeric estimate of risk, e.g. ‘0.001 equivalent fatalities per person per year’.

15. Risk matrices can be purely qualitative, but are often described as semi-quantitative. This refers to when numeric measures are used to group levels of likelihood and severity into categories. The level of risk is given as a category, rather than a numeric value.

16. Safety targets **should** be set, whichever assessment methodology is used. Targets must use the same measure as the level of risk. They may be based on historic information from similar systems, accident statistics from comparable industries, industry good practice, engineering judgement, etc. For some specific hazards, targets are set in law. Safety targets **should** be reviewed by senior management, as they record the risk appetite of the organisation. Guidance on setting appropriate targets is provided by the HSE in their document R2P2.

17. It must be remembered that whichever method is used, qualitative or quantitative, 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.

STAGE 3

Application of the ALARP Principle and Tolerability of Risk

18. Once a hazard has been identified that has the potential to cause harm and the risk of that harm quantified, the MOD (to meet its duty of care) **should** reduce the risk posed to its staff and other people who may be affected. With any risk, there will come a point where the safety benefit of reducing it further is negligible compared to the costs of doing so. It requires a balance to be made between costs and benefits. This balance is biased towards safety: risk reduction may only cease when the cost is grossly disproportionate to the benefit. The overall aim **should** be to provide land systems where all residual risk has been reduced to a level that is ALARP.

19. Tolerability of risk relates to the willingness to accept a particular level of risk. The level of risk which will be tolerated is ultimately the decision those holding delegated safety responsibilities. There **should** be in place a mechanism to decide on what level of risk is tolerable and what level of risk is unacceptable. Those holding delegated safety responsibilities **should** never tolerate an unacceptable risk (by definition); the definition of what is acceptable can change according to the circumstances. There may be operational situations where a higher level of risk may be tolerated for a defined period[49].

20. Figure 2 indicates the application of the ALARP principle and levels of tolerability.

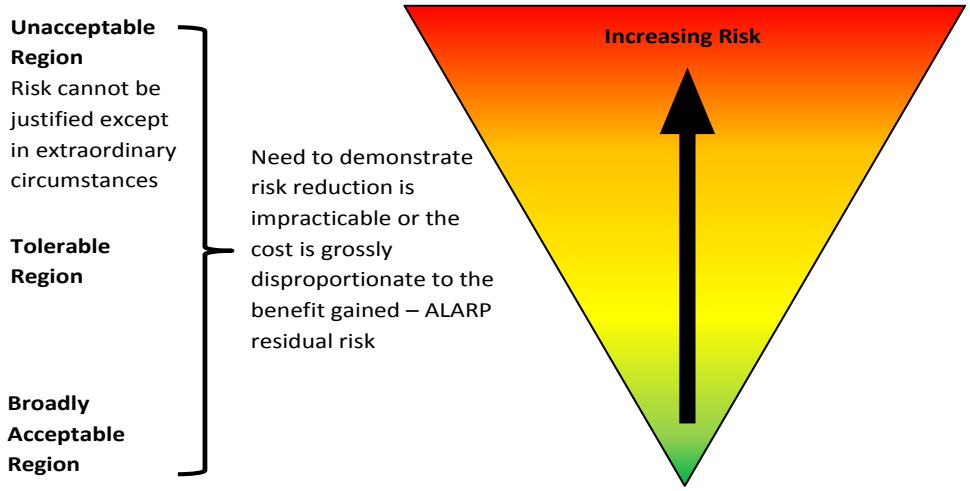


Figure 2. ALARP and Levels of Tolerability

21. The ALARP principle **should** be applied to all Land systems. Above a certain level, risk is unacceptable and **should** not be tolerated in normal operating conditions. Below this level, the risk associated with systems may be considered tolerable or broadly acceptable provided that risk has been reduced to a level that is ALARP.

[49] Refer to the DCoP (G) for Regulation 11

22. Account **should** be taken of cost of any further safety improvements. When risk is assessed as close or at the tolerability limit[50], a formal cost-benefit technique[51] **should** be used. The interpretation of further safety improvements may vary between systems, but **should** be justified and recorded in the Safety and Environmental Management System[52].

23. Determining reasonably practicable measures whether the decisions taken to control the risk are suitable and sufficient, depends in part on where the boundaries are set between the unacceptable, tolerable or broadly acceptable regions shown in Figure 2. The choice **should** be based on sound assumptions and the judgment of those holding safety responsibilities on the practicability of possible solutions.

24. Implementation of good practice **should** be considered a starting point when implementing risk reduction measures. The ALARP principle recognises that further risk reduction may cease when no further risk reduction measures exist that are reasonably practicable. This provides the basis for the majority of ALARP decisions, although it is not the only factor that **should** be considered. The ALARP principle requires a comparison to be made which balances the level of risk involved in an undertaking against the sacrifice involved in avoiding the risk in terms of money, time or trouble. If this shows that the sacrifice of reducing the risk further would be grossly disproportionate to the safety benefit, then the risk can be declared ALARP.

25. It is necessary to maintain assurance that risk remains ALARP throughout the life of the system(s). Therefore, the ALARP status **should** be routinely reviewed to ensure that the assumptions supporting the ALARP justification remains valid and that emerging approaches / technologies that may offer further risk reduction are appropriately considered.

26. Whenever there are changes to a system(s) design, role, operating environment, users and / or changes in legislation, defence regulation or standards there **should** be a re-assessment of all risks that fall within the scope of the changes.

STAGE 4

Risk Reduction

27. The risk reductions / mitigations / controls identified **should** be applied to achieve ALARP status.

Risk Acceptance

28. Once the hazard and risk analysis process has been completed, risk reductions applied and the risk judged to be at least tolerable and ALARP by the risk owner, the formal acceptance of that risk **should** be recorded.

[50] When using a Risk Classification Matrix (RCM), risks deemed close to the tolerability limit are typically classified as class B risks
[51] Refer to Para 36 to 42
[52] Refer to the DCoP (B) for Regulation 2

Recording of Risk Management Decisions

29. The results of the hazard identification and analysis, the risk assessments and ALARP justification **should** be recorded in the Hazard Log. Further requirements and guidance on the Hazard Log is provided in the DCoP (D) for Regulations 4 – Safety and Environmental Cases.

Rail System Safety by Design

30. Those who are responsible for Rail System Safety by Design **should**;

a. Assess the impact of introducing new or altered works, plant or equipment on the whole railway system throughout the project's lifecycle (i.e. manufacture, installation, commissioning, operation, maintenance, de-commissioning and disposal);

b. Design out the risks and impacts so far as is reasonably practicable;

c. Ensure residual risks can be effectively controlled, where elimination is not reasonably practicable, and explain how this is communicated to those who will control the risks in the future;

d. Regularly evaluate the impact of design decisions on all aspects of the lifecycle of the plant or equipment, beginning at the earliest stages of a project and continuing as options are selected and changes are made.

31. Those responsible **should** at least consider:

a. How the particular plant and equipment will interact with other new, altered or existing plant or equipment on the railway;

b. How the particular plant and equipment will interact with those of other railways and other guided transport systems;

c. What the plant and equipment will be used for, how it will be operated and how this affects the safety management system it is employed under;

d. New approaches used by the industry arising from information available following an investigation into an accident;

e. Management of occupational health issues for workers such as manual handling, hand / arm vibration, COSHH and noise;

f. The impact of human factors including how people will interact with the plant and equipment;

g. Trespass, vandalism and wilful acts;

h. How the railway interacts with its adjacent environment including physical interfaces, noise, vibration, and electrical and magnetic interference;

i. The reliability and durability of the plant and equipment, and the level of maintenance required;

j. How the plant and equipment will be inspected and maintained throughout their life, including their disposal;

k. The control of risk posed when degradation occurs;

l. The integrity of safety critical plant and equipment;

m. The foreseeable climatic conditions in which the plant and equipment will be used including risks, where relevant, arising from climate change;

n. Environmental legislation on pollution, such as noise, fumes etc where this may affect worker safety (other bodies may be responsible for enforcing breaches of environmental pollution duties);

o. Limiting fire load, ignition sources and fire spread.

Guidance Material

Hazard identification Techniques

32. When conducting a Hazard identification a number of techniques are available, such as:

a. The **Hazard and Operability (HAZOP)** procedure involves a multi-disciplinary team who has substantial experience of the system to be studied. The team consider taking a full description of a process and systematically question every part of it to establish how deviations from the design intent can arise. For each credible deviation the group considers possible causes and consequences and decides if additional safeguards should be recommended when consequences are found to have a negative effect upon the safe and efficient operation of the system. This examination of the design is structured around a specific set of guidewords, which ensure complete coverage of all possible problems whilst allowing sufficient flexibility for an imaginative approach;

b. The **Structured What-If Checklist (SWIFT)** study technique is a technique that combines the use of checklists with a brainstorming ‘What if?’ approach. It was initially developed for hazard identification in the chemical process industry. The technique was developed as an efficient alternative to HAZOP for providing highly effective hazard identification in situations and systems where HAZOP is not appropriate. SWIFT can also be used in conjunction with or complementary to a HAZOP;

c. The **Failure Mode and Effects Analysis (FMEA)** involves systematically reviewing components, assemblies and subsystems to identify failure modes, their causes and effects. The objective of FMEA is to identify those single failures that contribute to known hazards and those that give rise to additional hazards. FMEA does not consider combinations of failures. It is a ‘bottom-up’ method which can be applied at all levels in a system;

d. The **Zonal Hazard Analysis (ZHA)** considers the physical disposition of the system and its components in its installed or operating domain including, for example, clearances from moving parts, thermal heating and cooling, vibration and ease of access to components for installation and removal. It may be used to determine the consequences of interactions with adjacent systems, areas where maintenance or installation errors may cause or contribute to a hazard, and sources of common cause failure (such as environmental factors).

33. Further guidance on hazard identification techniques can be found in the Safety Managers Toolkit in Acquisition Safety and Environmental Management System (ASEMS) and Defence Standard 00-056.

Hazard Analysis

34. When conducting a hazard analysis a number of techniques are available, such as:

a. **Functional Safety Analysis (FSA)** involves systematically reviewing the function performed by a system and identifying what could go wrong if the function was not performed, was performed incorrectly, or was performed when not required;

b. **Fault Trees Analysis (FTA)** is a 'top-down' method used to analyse the events or failures within a system that can lead to a hazardous situation. A Fault Tree starts from an identified hazardous situation and goes on to identify the combinations of causes which could result in the hazardous situation. This can help identify common causes that affect different parts of a system;

c. **Event Trees Analysis (ETA)** is used to analyse the events or failures once a hazardous situation has arisen that cause it to escalate to an accident. Event Trees are useful for identifying safeguards that limit the potential consequences from a hazardous situation. Each safeguard acts as a barrier and the Event Tree branches out with two possibilities (that the safeguard prevents the accident or that the safeguard does not prevent the accident);

d. **Bow Tie Diagrams** are very useful in illustrating Causes, Hazards and Consequences of accidents, and the measures that are in place to control them. It can be considered as a combination of a Fault Tree (on the left of the hazardous situation) and an Event Tree (on the right of the hazardous situation). The Bow Tie technique is best applied at the operating level (with PT technical involvement) and used in a qualitative manner.

35. Further guidance on hazard analysis techniques and risk assessment can be found in:

a. ASEMS;

b. The Safety Managers Toolkit (ASEMS);

c. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment – ARP4761 (1996).

Demonstrating ALARP

36. As with other safety requirements, the Safety Case must set out and justify the criteria, approach and methodology that will be applied for making ALARP decisions.

37. For many ALARP decisions a detailed Cost Benefit Analysis (CBA) is not required and a simple comparison of costs and benefits may suffice. In other more complex situations, the benefits of reducing risk may need to be valued explicitly using CBA. The latter is far from easy because the safety of people are not things that are bought and sold, and yet a monetary value has to be attributed to matters such as the prevention of death, personal injury, pain and suffering.

38. Where the benefit is the prevention of death, the current convention used by HSE and Treasury[53], when conducting a CBA is to adopt a benchmark value of approximately £1.58M (2009 prices) for the Value of Preventing a Fatality (VPF). VPF is not the value that society, or the courts, might put on the life of a real person or the compensation appropriate to its loss.

39. When taking account of cost in the pursuance of any further safety improvements for a system that is closer to the unacceptable region than the broadly acceptable region, costs might be grossly disproportionate if they were greater than 5 – 10 times the value of the improvement.

40. For a system that is already closer to the broadly acceptable region, costs might be grossly disproportionate if they were greater than 3 – 5 times the value of the improvement.

41. If CBA is used it must be remembered that CBA cannot form the sole argument of an ALARP decision nor can it be used to undermine existing standards and good practice.

42. Further guidance on the requirements and application of ALARP and CBA is available in:

a. Management of Health and Safety at Work Regulations (1999);

b. HSE Reducing Risks, Protecting People (R2P2), HSE's Decision-making Process (2001).

Risk Tolerability

43. It is important to note that 'tolerable' does not mean 'acceptable'. It refers to a willingness to carry risk in order to secure certain benefits with the confidence that it is being appropriately controlled. Tolerable risk still requires review and further reduction if and when practicable. For risk to be acceptable, those holding delegated safety and environmental responsibilities must be prepared to carry it without committing significant resources to reduce it further, although this does not preclude further risk reduction.

[53] NERA Economic Consulting. Updating the VPF and VPIs: Phase 1: Final Report Department for Transport. 18 Mar 2011

44. When controlling risk it is necessary to determine the following:

a. Whether the risk is so great or the outcome so unacceptable that it must be refused altogether;

b. Whether the risk has been reduced to the lowest level reasonably practicable, with consideration of the benefits resulting from tolerating it and accounting for the costs of any further reduction (ALARP);

c. Whether the risk is, or is not, acceptable.

Regulation 8 – Best Practicable Environmental Option (BPEO)

Regulation	**Those holding environmental responsibilities shall ensure that the environmental risk posed by the system(s) has been reduced or managed as far as reasonably practicable by selection of the BPEO.**
Rationale	The Management of Health and Safety at Work Regulations (1999[54]) (MHSWR) require that employers assess the risk created by their undertaking and that all employers assess risk to the health and safety of anyone that may be affected by their activities. This includes employers, employees and members of the public and the Health and Safety and Work etc. Act 1974 (HSWA) imposes general duties on every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all their employees. MOD must fulfil its statutory obligations and its common-law duty of care whilst maintaining Defence capability. Requirements have been placed on those holding safety and environmental responsibilities to demonstrate that residual risk is at a level that is As Low As Reasonably Practicable (ALARP)[55] and is adequately controlled. The Secretary of State for Defence demands that we protect the environment. Potential risks to the environment must be reduced or managed as far as reasonably practicable in order to comply with the Environmental Protection Act 1990[56].
Defence Code of Practice	45. To meet its duty of care, a land system must minimise the residual impact and risk[57] posed by its operations upon the environment. In order to fulfil this obligation the requirements under DSA01.1 – Defence Policy for Health, Safety and Environmental Protection[58] and JSP 418[59] **should** be applied to land systems. These provide requirements and guidance on environmental management and **should** be followed, where applicable. The output of these processes make up the Environmental Case required in Regulation 4 of DSA02 DLSR. 46. Through fulfilling these requirements land systems **should** identify that the residual impacts and risks are managed and the Best Practicable Environmental Option (BPEO) has been selected. 47. The BPEO is a term used to demonstrate that the environmental impacts and risks associated with the land system(s) have the least environmental damage as well as meeting legislative and practicability constraints, at acceptable cost, in the long-term as well as the short-term. It is the mechanism by which due regard to the protection of the environment **should**

[54] As amended 2003
[55] SFAIRP is a legal term that is incorporated in the MHSWR. ALARP is the term used in safety engineering and is commonly considered to be analogous to SFAIRP. Ultimately, if a prosecution was brought under the MHSWR, a court of law would decide if a safety argument made on the basis of ALARP satisfies the demands of SFAIRP
[56] Individual environmental protection legislation refers to terms such as 'As Low As Reasonably Achievable', 'Best Available Techniques', 'Best Practicable Environmental Option (BPEO)' which have subtle variations of meaning. For brevity in this JSP, 'selection of BPEO' is used to describe the acceptable reduction of environmental risk
[57] Including steady-state environmental impacts and potential risks arising throughout the lifecycle
[58] DSA01.1 – Defence Policy for Health, Safety and Environmental Protection
[59] JSP 418 Management of Environmental Protection in Defence

be demonstrated for land systems, including those not governed by applicable regulation or standards.

48. Environmental Management **should** be considered from the concept of land systems or activity and be reassessed throughout. Early opportunities to investigate options and adequately scope requirements can provide many cost effective options for environmental protection.

Identification of Environmental Impacts and Risks

49. Environmental Aspects Impacts and Risks **should** be identified using stakeholder's knowledge and experience and recorded. This **should** take account of all lifecycle phases and activities within them such as trials and testing.

Assessment of Environmental Impacts and Risks

50. The assessment of the environmental impact and risk **should** be conducted throughout the lifecycle of the land system(s). The assessment **should** identify the significance of each impact and risk and thus prioritise accordingly for further management. Prioritisation methods **should** be developed for each project in order to show a spread of significance, in order to prioritise any actions accordingly.

51. Assessments **should** consider the controls and mitigation measures currently in place to manage the environmental impacts and risks. These **should** be recorded.

52. The assessment and prioritisation of environmental impacts and risks **should** be conducted with the reputation of the MOD in mind. Where the potential outcomes from an event or operational activity could reflect badly on the social acceptability of MOD operations in the UK or overseas, this **should** be incorporated into the assessment.

BPEO

53. In undertaking environmental assessments any additional controls or mitigation measures (for the land system(s) and its operations) **should** be identified that further minimise environmental impact and risk across the lifecycle, thus finding a solution that provides the most benefits, or the least damage, to the environment at an acceptable cost in both the long term as well as in the short term.

54. The BPEO is therefore the solution where any additional environmental benefit can only be obtained through expenditure of disproportionate cost, in terms of financial or other resource costs. There must be no detrimental impact to safety or defence capability when identifying a BPEO solution.

55. Ultimately BPEO assessments **should** be carried out at two levels:

a. To identify the difference in overall environmental impact and risk between solutions or options during the Concept and Assessment phases;

b. To justify each impact and risk identified is acceptably managed and understood.

56. BPEO assessments **should** consider the following criteria:

a. Cost of controls and mitigation;

b. The long and short term environmental, social and economic implications and benefits (thus considering sustainability);

c. Additional consequences of mitigations e.g. safety or operational implications;

d. Adequacy of training, technical publications and use of common sense;

e. Level of technology available.

57. The BPEO assessment **should** be supported with robust BPEO statements, for each impact and risk, which outlines controls and mitigations assigned that minimise the damage to the environment or provide the most environmental benefit. The assessment **should** be conducted proportionately to the severity of environmental impact or risk.

Continuous Management

58. Operational Controls **should** be implemented for land systems as identified by the BPEO assessment. Objectives and targets **should** be set, regarding reduction in environmental impact and risk, as far as reasonably practicable to continuously achieve BPEO. These Operational Controls, Objectives and Targets **should** be monitored through life and adjusted as appropriate.

59. There **should** be a periodic re-assessment of all environmental impact and risk to identify changes and opportunities for improvement. The BPEO Statement **should** be reviewed in accordance with the land system's Safety and Environmental Management System (SEMS)[60] or, where there are changes to a land system(s) design, role, operating environment, users and / or changes in legislation, MOD regulation or standards.

Guidance Material

General

60. The Environmental Protection Act 1990 is enacted through the Secretary of State for Defence who requires due regard to be paid to the protection of the environment. Further guidance on environmental management for Land systems is available in:

a. DSA01.1 – Defence Policy for Health, Safety and Environmental Protection

[60] Refer to the DCoP (B) for Regulation 2

b. Acquisition Safety and Environmental Management System (ASEMS) Project-Oriented Environmental Management System (POEMS);

c. JSP 418 MOD Corporate Environmental Protection Manual.

61. Guidance on Environmental Management within Defence is provided in Acquisition System Guidance (ASG) ASEMS POEMS. This provides guidance on full lifecycle environmental management, and includes templates and forms that can be utilised for the study. Complying with the POEMS framework provides the evidence required for an Environmental Case for land systems.

62. ASEMS POEMS provides a structure and guidance for an environmental case, giving flexibility to the author to adapt and apply proportionality. POEMS also provides process flowcharts to identify what activities should be carried out for each lifecycle phase.

63. The term 'best practicable environmental option' was first used by the Royal Commission on Environmental Protection in their Fifth Report, 'Air Pollution Control: an integrated approach', which was published in 1976. The term is further defined in their Twelfth report of February 1988 titled Best Practicable Environmental Option. This has been adapted for use by the MOD to justify that environmental impacts and risks are adequately managed.

BPEO Statement

64. The BPEO Statement is a mechanism to demonstrate that options have been considered through environmental assessment and that those selected minimise the residual environmental impact and risks across the system lifecycle and are therefore defined as the BPEO for the land system(s).

65. BPEO, in terms of risk to the environment caused by land systems, is the option which produces acceptable residual impact and risks upon the environment. This may mean compliant with applicable standards and legislation but that does not preclude further minimisation if it is feasible to improve mitigation or controls without further reduction in operational capability or grossly disproportionate cost.

66. The BPEO Statement is an output from the environmental assessment in addition to the ASEMS POEMS forms, though it may form part of the Environmental Impact Statement required of POEMS EMP05.

Other Environmental Techniques

67. Techniques used to reduce impact on the Environment are not limited to BPEO. Best Available Technology Not Entailing Excessive Costs (BATNEEC) is a technique used to reduce emissions from activities. More information on BATNEEC is available in the Environmental Protection Agency's Guidance Note, Class 12.1.

DCoP F - Legislation Compliance

Regulation 9 – Legislation Compliance Assessment

Regulation

Those holding safety and environmental responsibilities shall undertake a suitable and sufficient legislation compliance assessment for each land system prior to use.

Rationale

The Secretary of State for Defence requires that within the UK land systems, both in construction and use, are compliant with all applicable Health, Safety and Environmental Protection (HS&EP) legislation. Overseas, MOD UK arrangements will apply where reasonably practicable, and in addition, MOD will respond to host nation's relevant HS&EP expectations.

The MOD can rely on exemptions, derogations or disapplications from legislation and where this is the case, the Secretary of State requires the maintenance of Departmental arrangements that produce outcomes that are, so far as reasonably practicable, at least as good as those required by UK legislation. Where exemptions are required, approval will only be granted on the grounds of national security and where it is essential to maintain operational capability.

Defence Code of Practice

Legislation Compliance Assessment

1. All applicable legislation for the construction and use of system(s) **should** be identified, assessed, recorded and monitored. The requirement to conduct a Legislation Compliance Assessment (LCA) **should** be read in conjunction with the Defence Code of Practice on Safety and Environmental Case Development. A LCA **should** commence during the development of Part 1 of a Safety Case with the setting of requirements. It **should** be developed throughout the early stages of the project up to Main Gate and may require updating at various stages in the lifecycle of the system(s).

2. The purpose of the LCA is to:

   a. Identify and record all relevant legislation deemed applicable to the system at point of intended use, and this includes:

      (1) Directly applicable legislation for which the MOD has no available exemption, derogation or disapplication; or

      (2) Directly applicable legislation for which the MOD has an exemption, derogation or disapplication.

   b. Apply scrutiny to its construction and intended use features to ensure compliance;

   c. Ascertain the system complies with the Secretary of State for Defence HS&EP Policy. Where there is no relevant legislation, internal standards **should** optimise the balance between risks and benefits.

3. The User Requirement Document (URD) for the system(s) is to be examined and used to conduct the LCA which **should** include a selection of individual items of legislation applicable to the construction and intended use of the system(s). The findings of the LCA **should** be recorded in a table format which captures the headings listed below:

a. Name of the system;

b. Relevant legislation and requirements, based on the chosen Type Approval category, if the system is a vehicle;

c. Compliance Status [OK, Not OK (NOK), To Be Confirmed (TBC)] with reasons, including applicability [directly applicable, exemption, derogation or disapplication] and evidence to support the compliance status;

d. Technical and operational justification for the non-compliance(s).

4. The LCA **should** be completed prior to Main Gate and contract award to inform procurement decisions and any application for exemption(s). Applications for exemptions **should** only be considered when all practicable means of making a system compliant have been exhausted and applying for exemptions is the only remaining option. Once the need for exemptions has been established, potential applicants **should** engage with the Land Exemptions Committee (LEC) Secretariat and provide a copy of the LCA.

5. LCAs **should** subsequently be reviewed at the following stages:

a. Prior to first use, e.g. test and trials;

b. During the mid-year review of systems;

c. When modifications and / or changes are made to the construction and / or use of system(s);

d. When there are new or changes to legislation which apply retrospectively;

e. When systems used for Urgent Operational Requirements are being transferred into Core;

f. When the system is returning to service after a period of storage.

Business Cases

6. Where a non-compliance has been identified and no exemptions are available to the MOD, a legislation business case **should** be submitted to the LEC to endorse the request for change in the law. The UK Government department responsible for the legislation from which an exemption is sought will then consider the business case. The business case template on

which exemption requests **should** be submitted, is available from the LSSR web page[61].

Guidance Material	7. More information on the exemption process can be found within the exemption process Standing Instruction in the related documents section on the LSSR webpage.

Regulation 10 – Exemption Cases

Regulation	**Those holding safety and environmental responsibilities shall present a formal exemption case to the Land Exemption Committee for each**

[61] http://authdefenceintranet.diif.r.mil.uk/Organisations/Orgs/HOCS/Organisations/Orgs/DSEA/Pages/LandSystemsSafetyRegulator.aspx

land system, where a legal exemption is necessary and permitted, prior to use.

Rationale

The Secretary of State for Defence requires that within the UK land systems, both in construction and use, are compliant with all applicable Health, Safety and Environmental Protection (HS&EP) legislation. Overseas, MOD UK arrangements will apply where reasonably practicable, and in addition, MOD will respond to host nation's relevant HS&EP expectations.

The MOD can rely on exemptions, derogations or disapplications from legislation and where this is the case, the Secretary of State requires the maintenance of Departmental arrangements that produce outcomes that are, so far as reasonably practicable, at least as good as those required by UK legislation. Where exemptions are required, approval will only be granted on the grounds of national security and where it is essential to maintain operational capability.

Defence Code of Practice

Exemption Cases

8. Where non-compliances have been identified and Disapplications, Exemptions or Derogations (DEDS) are available to the MOD, an application in the form of an exemption case **should** be submitted to the LEC. The Exemption Case template, on which exemption requests **should** be submitted, is available from the LSSR web page.

9. The purpose of the exemption case is to justify, with evidence, the need to invoke an exemption and to demonstrate that all mitigations for each non-compliance have been identified and reduce the associated risks to levels that are considered to be As Low As Reasonably Practicable (ALARP). The exemption case **should** also capture the reasoning behind the arguments which justify the request for any exemption.

10. A single exemption case **should** be submitted for each system for which exemption is being sought prior to use. The information used to build the exemption case **should** be drawn from the Safety Case and the LCA.

11. The exemption case **should** include a brief description of the System; its operational role; the programme and key milestones, including Out of Service Date; and a reasoned argument for the exemption to cover the following issues:

a. The item of legislation from which exemption is being sought;

b. Applicability of legislation (i.e. directly applicable to the system or annotated as duty of care, if a disapplication is available);

c. The description of the non-compliance;

d. The technical reasons for non-compliance;

e. The operational requirement which justifies the non-compliance;

f. The risks posed by the non-compliance;

g. The mitigating measures to be implemented to ensure that any residual risks are reduced to ALARP and demonstrate that procedures and standards in place of those required by legislation still offer equal protection as if the letter of the law was followed;

h. The perceived operational and financial impact of meeting the legislative requirements.

12. Exemption cases **should** be supported with evidence and co-signed by the Delivery Team Leader and Duty Holder / Chain of Command Representative or Capability Sponsor. When presenting the submitted case to the LEC, the team **should** comprise representatives from both teams and be led by a person at least of OF4 / C1 or grade.

13. In the event that any exemption is granted, a copy of the certificate **should** be retained for future reference. In the case of a vehicle exemption, a copy of the certificate **should** be carried in the vehicle for presentation as required. All stakeholders **should** be informed of any exemption, exemption certificate and all mitigation(s) required to manage the residual risk. A lack of implementation / maintenance in regards to the exemption case mitigations, will render the exemption case invalid.

14. Exemption certificates have specified expiry dates and are assigned by system asset code; they **should** be closely monitored to ensure that any land system(s) is not operated without a valid exemption or exemption certificate.

15. Exemption cases **should** subsequently be reviewed and presented at the following stages:

a. Where non-compliances are first identified through the LCA prior to trials and / or testing;

b. Following Trials and / or testing for any exemptions required throughout the systems service life;

c. When modifications and / or changes are made to the construction and / or use of system(s);

d. When there are new or changes to legislation which apply retrospectively;

e. When systems used for Urgent Operational Requirements are being transferred into Core;

f. When systems holding exemptions change asset codes;

g. When existing exemptions are due to expire and exemption is still required.

16. The LEC **should** be notified when the following circumstances arise:

a. The system is taken into long term storage;

b. The asset code(s) of systems are changed;

c. The mitigation(s) upon which the exemption was granted is changed;

d. A change to the Out of Service Date (OSD) of the system is being considered;

e. The system is being considered for disposal.

Guidance Material

17. More information on the exemption process can be found within the exemption process Standing Instruction in the related documents section on the LSSR webpage.

DCoP G - Operational Dispensation

Regulation 11 – Operational Dispensation

Regulation	**Those holding safety and environmental responsibilities shall ensure that an Operational Dispensation is in place if an operational imperative arises that necessitates the use of the land system(s) outside its safe operating envelope.**
Rationale	Commanders must be provided with land systems that are safe for the intended military role and with adequate information to enable them to make sound risk based decisions when on operations. The systems should be acceptably safe in training, during peacetime and on operations. However, there will be occasions when the systems may need to be used outside of the safe operating envelope due to the operational imperative, therefore Commanders will need to make risk based decisions if equipment is used outside of the bounds set within the Safety and Environmental Case. Where land systems are being used in this way for an enduring period of time, an Operational Dispensation will be required.
Defence Code of Practice	1. TLBs **should** have an Operational Dispensation process in place for land systems under their responsibility, if they need to implement an operational dispensation. 2. A land system **should** be used in accordance with its safe operating envelope defined within the Safety and Environmental Case. The operating envelope **should** be recorded within the Safety and Environmental Case Report[62], the operating and maintenance procedures and training manuals. **Initial Operational Dispensation** 3. If a land system is to be used outside the safe operating envelope for an enduring period of time[63], then a request for an Initial Operational Dispensation **should** be made. The request **should** outline the operational imperative, the change of use required of the system, the risks associated with this change and the in-theatre mitigation measures to be implemented in the short term until a more enduring solution is identified. The period of the Initial Operational Dispensation **should** not exceed 28 days. **Urgent Statement of User Requirement** 4. On authorisation of the Initial Operational Dispensation an Urgent Statement of User Requirement (USUR) **should** be submitted defining the new requirement(s) and seeking an urgent review of the Safety and Environmental Case to assess the impact of incorporating these requirements. 5. The review of the safety arguments and risks within the existing Safety and Environmental Case **should** consider an operational assessment of the impact of the dispensation not being approved, expressed in terms of risk of death or injury balanced against the continued used of the land system(s)

[62] Or other appropriate form of delivery as per the DCoP (D) for Regulation 4
[63] Where capability will be used outside of the safety case for an operational tour

outside its existing safe operating envelope, taking into account in-theatre risk mitigation measures detailed in the Initial Operational Dispensation.

Safety and Environmental Management Committee

6. A Safety and Environmental Management Committee (SEMC) **should** be convened to consider the implications of the USUR. The SEMC **should** assess the risks associated with the requested change of use of the land system and identify any further mitigation measures, with the aim of demonstrating that the change of use is tolerable / broadly acceptable and ALARP, in accordance with the defined tolerability criteria defined in the existing Safety and Environmental Case.

7. The SEMC **should** consider risks in the operational context and the extent to which practical solutions can be implemented to mitigate them.

8. If the risk can be appropriately mitigated and controlled within the Initial Operational Dispensation period, then the SEMC **should** recommend acceptance of the risk. This acceptance **should** be documented through a variety of means, for example the SEMC minutes, a risk assessment, etc. In this case, the Initial Operational Dispensation **should** be closed and superseded with a revised Safety and Environmental Case Report[64] and Hazard Log, once the mitigation measures have been implemented.

Operational Dispensation Report

9. If it has not been possible to immediately identify or implement appropriate mitigation measures for the risks identified, or the risk associated with the proposed change of use of the land system cannot be mitigated the SEMC **should** produce an Operational Dispensation Report. This report **should** be completed within the Initial Operational Dispensation period.

10. The risk associated with the proposed change of use of the land system **should** be referred through the chain of command to a more senior level, and if necessary, up to ministerial level for acceptance. On acceptance of the risk, a further Operational Dispensation **should** be authorised.

Management of an Operational Dispensation

11. All active operational dispensations **should** be subject to regular monitoring and on-going management in accordance with the land system's Safety and Environmental Management System, particularly during the initial period. This monitoring **should** be proportionate to the residual risks associated with the Operational Dispensation.

[64] Or other appropriate form of delivery, as per the DCoP (D) for Regulation 4

Guidance Material

Operational Dispensation Process

12. The regulation requires the TLBs to plan for and put an appropriate process in place before a change occurs, to control the safety risks of the changes which are considered outside the safe operating envelope of the Safety and Environmental Case. The aim of an Operational Dispensation Process is to effectively control changes to ensure that they are considered, well planned and carefully executed so that the operation benefits to service personnel outweigh the potential risks to their safety.

DCoP H - Safety and Environmental Performance Monitoring, Review and Audit

Regulation 12 – Incident Reporting

Regulation	**Those holding safety and environmental responsibilities shall ensure that all incidents involving land systems are reported, recorded and appropriately investigated.**
Rationale	DSA01.1 – Defence Policy for Health, Safety and Environmental Protection requires a commanding officer or manager to conduct an appropriate investigation into a Health, Safety and Environmental Protection incident or accident occurring during a Defence activity in their area of responsibility. In the MOD, those holding safety and environmental responsibilities need to measure, review and audit the overall effectiveness of their safety and environmental management system to understand how well it is operating.

Defence Code of Practice	1. TLBs **should** have procedures in place to enable effective reporting, investigation and management of incidents involving land systems.
	
	2. All Incidents involving land systems **should** be reported, recorded and appropriately investigated to:
	
	a. Determine underlying, or root cause(s);
	
	b. Determine immediate cause(s);
	
	c. Conduct trend analysis;
	
	d. Identify appropriate additional control measures;
	
	e. Identify any lessons that can be learnt;
	
	f. Share information and lessons with stakeholders.
	
	3. Incident(s) **should** be reviewed:
	
	a. To promulgate lessons identified to other domains where applicable;
	
	b. Against the relevant Safety and Environmental Case to ensure that residual risk remains ALARP.
	
	4. TLBs **should** have a Learning From Experience (LFE) process in place to enable effective communication of lessons learnt to all relevant personnel.
	
	5. All safety related fatalities, serious injuries and significant loss of major capability[65] [with a land system dimension] **should** be reported to the

[65] This includes: a) land system events formerly referred to as a Serious Equipment Failure (SEF) which is an event where a land system(s) has physically failed; relating to a resulting loss of life, personal injury and / or has compromised safety to

Defence Accident Investigation Branch (DAIB). Additionally, all TLBs are to report these events (and all other land system accidents and incidents) to the Army Incident Notification Cell (AINC). This does not change the requirement for all TLBs to notify their own Incident Cells. It **should** be noted that unless there are urgent and justifiable imperatives, the suspect system(s) must be quarantined immediately pending investigation.

6. Those holding safety and environmental responsibilities **should** ensure that all reported incidents are appropriately documented and retained.

Guidance Material

7. An incident is defined as an accident (an unintended event, or sequence of events, that causes unintended harm) or a near miss (an unintended event, or sequence of events that had the potential to cause unintended harm, but did not).

8. TLBs, Trading Fund Agencies (TFAs) and Bespoke Trading Entities (BTEs) will include their requirements for incident investigations in their Safety and Environmental Management System (SEMS).

9. Further guidance on incident reporting and investigation can be found in Part 2 Volume 1 of JSP 375: Management of Health and Safety in Defence. The Health and Safety Executive provides guidance in HSG 245, Investigating accidents and incidents, a workbook for employers, unions, safety representatives and safety professionals.

10. DE&S have a process for Project Team reporting and monitoring significant equipment safety failures or environmental incidents – leaflet 01/2010 which found be found on the ASG site.

11. In the event of a fatality the DSA need to be informed using the template contained within in DSA01.1 – Defence Policy for Health, Safety and Environmental Protection.

personnel or to the general public; and b) Serious Incident (SI) which is an event where the functional engineering integrity of a land system(s) is placed in question; relating to a resulting loss of life, personal injury and / or has compromised safety to personnel or the general public

Regulation 13 – Monitoring and Reviewing Performance

Regulation

Those holding safety and environmental responsibilities shall have in place an effective means of monitoring, reviewing and reporting safety and environmental performance.

Rationale

DSA01.1 – Defence Policy for Health, Safety and Environmental Protection requires a commanding officer or manager to conduct an appropriate investigation into a Health, Safety and Environmental Protection incident or accident occurring during a Defence activity in their area of responsibility.

In the MOD, those holding safety and environmental responsibilities need to measure, review and audit the overall effectiveness of their safety and environmental management system to understand how well it is operating.

Defence Code of Practice (DCoP)

12. TLB's **should** have in place a process for monitoring, reviewing, inspecting and reporting safety and environmental performance for land systems under their responsibility.

13. Those holding safety and environmental responsibilities **should** ensure that legislation and policy compliance, risk control and continuous improvement demonstrate that performance is adequate and fulfills corporate reporting requirements. Guidance material is at paragraph 20.

Monitoring

14. Accident, defect and deficiency data, both direct or through corporate reporting processes **should** be recorded and monitored.

15. Measuring progress against objectives **should** use evidence of performance, using a combination of:

a. **Active Systems.** Leading indicators **should** be used to measure the effectiveness of design, development, installation and operation of management arrangements, risk control systems and workplace precautions. Systems **should** be inspected iaw JSP 930 (Generic Maintenance, Inspection, Certification and Testing);

b. **Reactive Systems**. Lagging indicators **should** be used to monitor incidents (accidents & near misses) and corrective action and to monitor evidence of deficient safety and environmental performance.

16. The range of indicators **should** be regularly reviewed to ensure that areas of vulnerability and organisational change are being addressed.

17. Where a land system(s) interfaces with another MOD Duty Holder / Chain of Command Representative or organisation, e.g. contractors, then appropriate leading and lagging indicators **should** be identified and agreed by both parties. This is to ensure adequate arrangements are in place to monitor the "control and management" of residual risks at the interface.

Reviewing

18. Data gathered through monitoring **should** be reviewed to make judgements about whether performance is adequate and fulfils corporate reporting requirements. Performance **should** ensure adequate:

a. Legislation and policy compliance;

b. Risk control;

c. Continuous improvement.

Reporting

19. Reporting is a crucial part of the safety and environmental regime. It is the mechanism that promotes continual improvement in safety and environmental performance. It encourages learning from and acting on experience, whether this comes from within a project team, the Operating Authority, another organisation or from a contractor. Safety and environmental performance **should** be regularly reported in accordance with the TLBs Procedures.

Guidance Material

Monitoring and Review

20. Measuring performance to assess how effectively risks are being controlled is an essential part of a safety and environmental management system. Used effectively, safety indicators can provide an early warning, before failure, that risk controls systems have deteriorated to an unacceptable level.

21. Monitoring aims to identify strengths and weaknesses in safety and environmental protection in order to measure progress against objectives.

22. Review is the process of analysing data gathered through monitoring techniques to make judgements about whether performance is adequate. It facilitates organisational learning and the opportunity to communicate good practice.

23. Over-reliance on failure data to monitor performance (lagging indicators) can mean that improvements or changes are only determined after something has gone wrong. A range of indicators should be employed. In addition to lagging indicators, these should include performance data (leading indicators) to provide assurance that policies and processes are being implemented and are operating effectively. This will provide early warning of deterioration within capability or processes and can provide an opportunity to avoid major incidents.

24. Both success and failure should be recorded and utilised as learning experiences on which the drive for continual improvement can be sustained, and a culture that encourages upward reporting of “bad news” should be pursued.

Regulation 14 – Audit Requirements

Regulation	**Those holding safety and environmental responsibilities shall undertake suitable and sufficient safety and environmental protection audits.**
Rationale	DSA01.1 – Defence Policy for Health, Safety and Environmental Protection requires a commanding officer or manager to conduct an appropriate investigation into a Health, Safety and Environmental Protection incident or accident occurring during a Defence activity in their area of responsibility. In the MOD, those holding safety and environmental responsibilities need to measure, review and audit the overall effectiveness of their safety and environmental management system to understand how well it is operating.
Defence Code of Practice (DCoP)	**Requirements** 25. TLBs should have a process in place to enable safety and environmental protection audits of land systems. Typically this process is recorded within the Land System's Safety and Environmental Management System[66]. The audit programme should be recorded in the SEMP. 26. Organisations with land systems **should** be subject to regular audits of their SEMS. The audits provide a level of assurance that both; a. The SEMS and its activities / outputs meet MOD policy; b. The SEMS is being implemented effectively. 27. The arrangements between MOD and contractors for safety and environmental protection **should** be subject to regular reviews and audit. 28. Where non-compliances are identified against MOD Policy and / or legislation then these **should** be reported in a timely manner. 29. Arrangements **should** be in place for completion of corrective actions arising from audits within an agreed timescale. The timescales **should** be proportionate to the level of risk. The Auditor would agree the corrective actions and any further remedial actions that **should** be in place.

[66] Refer to the DCoP (B) for Regulation 2

Purpose

30. The audits **should** seek to:

a. Provide assurance that activities are being performed in accordance with the SEMS;

b. Ensure the SEMS is correctly understood and operating effectively;

c. Identify opportunities to improve the management system;

d. Identify opportunities to raise awareness of safety and environmental protection issues;

e. Identify any training needs and competency requirements;

f. Provide assurance of compliance with applicable safety standards, both statutory and non-statutory;

g. Recognise good practice;

h. Inform the management review process;

i. Inform policy development;

j. Improve procedures for the management of safety and environmental processes.

Implementation

31. The periodicity and type[67] of audits **should** depend on the level of residual risk perceived or assessed, the complexity of the system, and the value that could be added by the audit process or as required by management.

32. Audits **should** be programmed and undertaken prior to the completion of a significant phase of work, when major milestones are reached or annually.

Competence

33. Only personnel with the appropriate competence **should** conduct internal audits. If this is not possible within the immediate team, a person with appropriate competence **should** be seconded; either from elsewhere in the organisation, or from an external source (e.g. Independent Safety Auditor (ISA)). Managers **should** undertake regular assessments to ensure the audit team have the competence required to undertake an audit.

[67] Paragraph 39 provides a description of audit types

Using an Independent Auditor

34. For Level 1 and Level 2 Safety and Environmental Cases[68] an ISA **should** be appointed to carry out audits of the Safety and Environmental Case. For Level 3 Safety and Environmental Case[68] the Safety and Environmental Committee (SEMC)[69] **should** decide whether an ISA **should** be used.

35. An ISA, when appointed, **should** sit as a full member of the SEMC or other relevant body that provides management and / or oversight of the SEMS, such as sub committees or working groups. Their role and function **should** be defined in the SEMP.

Guidance Material

Audit

36. Audit can be described as any formal examination that assesses and reports upon the adequacy and effectiveness of a process and its ability to meet required outcomes and objectives. Most often an audit is carried out by comparing a process against a standard. Audits have traditionally been used as the primary means of providing assurance of the safety of the land systems within the MOD.

37. Periodic audit assists in maintaining the continued effectiveness of a management system, and enables any deficiencies to be addressed.

Audit Process

38. The process for conducting an audit, both internally and externally, should be based on the following steps, and is summarised in Figure 1:

a. The publication of an audit programme;

b. Notification to the Auditee of the intention to carry out an audit. The Auditor will ensure that personnel involved are notified in good time;

c. Issue an audit questionnaire to the Auditee[70]. Sufficient time must be allowed for completion, citing evidence and returning the questionnaire to the Auditor prior to the audit. Agree a suitable date for the audit;

d. On receipt of the completed questionnaire, the Auditor will arrange a suitable date for the audit;

e. During the audit the Auditor will also meet the key personnel and progress through the questionnaire in a logical order, entering any comments as supplied;

f. Following completion of the audit the Auditor will discuss their findings with the Auditee. Opportunities for improvement that have been identified will be discussed with the Auditee and agreed;

[68] Refer to the DCoP (D) for Regulation 4 – on the level definitions of a Safety and Environmental Case
[69] Refer to the DCoP (B) for Regulation 2 – on the requirements of a SEMC
[70] An audit questionnaire is not required for most process audits

g. The Auditor will draft an audit report recording observations made, degree of compliance and, if applicable, agreed areas of improvement. The report will be issued to the Auditee and should be jointly signed by both parties as a record of the work and actions agreed;

h. Follow-up audits may be required to monitor the progress of recommendations made for improvement, or rectification actions. On completion of the follow-up audit, the Auditor will send a revised audit report to the Auditees for agreement and signature.

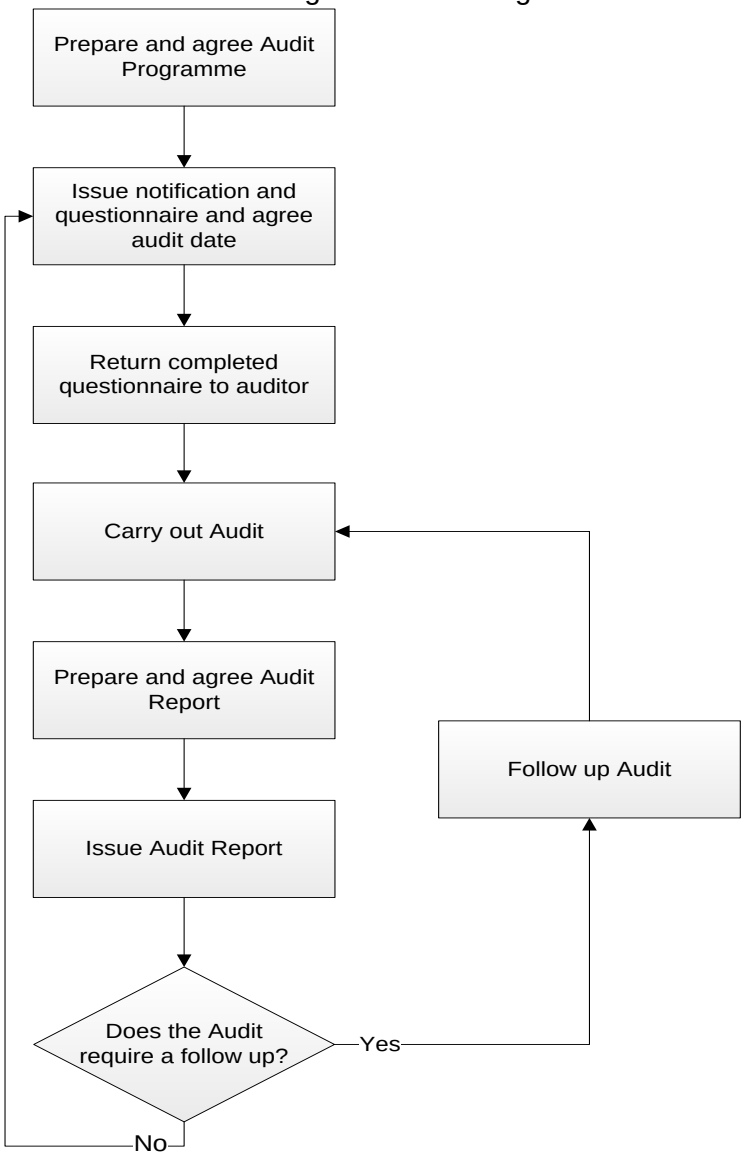


Figure 1. Audit Process

39. The various types of audits are:

a. **First Party (Internal)**. Conducting self-audit can be a valuable means of evaluating whether objectives are being met, and whether internal processes and procedures are being adhered to. Self-audit

helps to identify and gather evidence that may be required during external audits and will ensure familiarity with the audit process;

b. A peer review of the Safety and Environmental Management System may be sought to ensure good practice;

c. Commands carry out their own internal audit processes based on command levels, where a higher command level will audit the level below, i.e. Division will audit Brigade level;

d. **Second Party (External)**. An audit carried out by one part of the organisation on another, for example by a functional area, e.g. Army Inspector, on an implementer;

e. **Third Party (External)**. An audit carried out by an organisation independent to the Auditees, e.g. the Land Systems Safety Regulator.

Independent Safety Auditor

40. The ISA should have a well-defined role that is clearly understood by all parties. This role should include providing assurance by auditing the Safety and Environmental processes being followed, or by undertaking some assessment independently to check the primary assessment. The role may evolve through the lifecycle, but the ISA independence must not be compromised by involving them in activities such as setting requirements, tender assessment or providing specific advice on engineering changes.

41. The ISA should be independent of the organisation being supported and have a good understanding of issues related to systems under review.

42. The primary role of an ISA is to provide an independent opinion or assurance through assessment and validation of the Safety and Environmental Case work. This is usually achieved through audit of the following:

a. The safety and environmental management arrangements set out in the SEMP, Safety Case Part 1 (Requirements) and Safety Case Part 3 (Operation & Support);

b. The safety and environmental activities set out in the contractor's Safety and Environmental Programme Plan and the Part 2 Safety Case (Design), in response to the SEMP.

43. Information on MOD's approach to Conflicts of Interest (COI) is available on the Acquisition System Guidance (ASG) to help in understanding potential or actual COIs with an ISA in respect of their current or previous work for MOD or the Contractor.

DCoP I - Equipment Care and Configuration Management

Regulation 15 – Equipment Care and Configuration Management

Regulation	**Those holding safety and environmental responsibilities shall ensure effective processes and procedures are in place for equipment care[71] and configuration management for land systems.**
Rational	Equipment care and configuration management affects everyone within the MOD in some way, whether as a user, maintainer or service provider seeking to ensure the cost-effective delivery of land systems support. The pace of change has increased dramatically in recent times causing an increased use of contractors, and changes to legislation have resulted in significant amendments to policy, especially in areas involving safety. It is the responsibility of commanders and managers to ensure that those responsible for equipment care and configuration management of land systems are made aware of their safety and environmental obligations.
Defence Code of Practice (DCoP)	**Equipment Care** 1. Equipment care includes the cleaning, maintenance, forecasting, test and inspection that may be necessary to ensure that equipment achieves the highest levels of availability and is kept in an operational state. Regular maintenance[72] of in-service land systems **should** be undertaken and has an important role in minimising hazards and providing safer and healthier working conditions. Insufficient maintenance can lead to an increased risk of harm to MOD personnel, other parties and the environment; and undermine the safety arguments and assumptions within the Safety and Environmental Case for land systems. 2. Equipment care is the means of ensuring that the people, systems, processes and resources that deliver the integrity[73] of land systems are in place, in use and will perform when required throughout its lifecycle. 3. All commanders & managers **should** have organisation & arrangements documented and in place to ensure the effective management of land systems under their responsibility. These arrangements **should** include: a. Maintenance schedules and procedures which are properly managed to maintain the designed material state of the land system including the control of ageing / obsolescent materiel; b. Roles, responsibilities, training and competencies required; c. Procedures for ensuring shortfalls in maintenance are identified and assessed for safety and environmental impact;

[71] For Land System vehicles: TLBs **shall** also ensure compliance with the requirements of JSP 930 [Generic Maintenance, Inspection, Certification and Testing (MICaT)].
[72] Maintenance is the action taken to retain materiel in, or to restore it to, a specified condition. It includes inspection, testing, servicing, classification as to serviceability, repair, rebuilding and reclamation
[73] Land systems perform their function effectively and efficiently whilst ensuring the health and safety of personnel and minimising impact on the environment

d. Procedures for ensuring changes to maintenance requirements or scheduling are analysed for impact on Safety and Environmental Case;

e. Processes for defect reporting that are properly implemented;

f. Processes for the provision of spares to support maintenance of material state;

g. Processes to manage design changes and to maintain the material state;

h. Where appropriate, recovery procedures for ensuring the extrication of an abandoned, disabled or immobilised land system;

i. Regular review and audit of the arrangements[74].

Configuration Management

4. Land systems **should** be managed throughout their lifecycle and their configurations controlled / managed and documented accordingly to ensure they are designed, brought into service, operated and maintained in-service and finally disposed of in accordance with legislation and MOD policy.

5. TLBs **should** ensure that suitable processes and tools are used, such as the Joint Asset Management and Engineering Solution (JAMES), to ensure that up-to-date data is available to enable effective configuration management.

Retention of Records

6. A process should be established and applied to ensure all significant land system safety and environmental related documents are retained, tracked and preserved in an auditable manner.

7. Before destruction of a significant land system safety or environmental document, a thorough review should be carried out by SQEP personnel to ascertain whether the information in the document must be retained. Refer to paragraphs 23 to 25 for guidance.

Safety and Environmental Case

8. The Safety and Environmental Case[75] for the land system **should** demonstrate that changes to the material state through either modification or ageing are assessed for Safety and Environmental impact.

9. The assessment of risks arising from the maintenance and operation of equipment and systems **should** not only consider the preventive or proactive maintenance (periodic checks and repairs) but also the corrective or reactive maintenance (carrying out unforeseen repairs on equipment / systems after failure).

Industry

[74] Refer to the DCoP (H) – Safety and Environmental Performance Monitoring, Review and Audit
[75] Refer to the DCoP (D) for Regulation 4

10. Where Industry is used to support equipment care and configuration management, the TLBs **should** ensure that suitable and sufficient arrangements are in place to manage contractors and that these contractors are deemed competent[76].

Guidance Material

Equipment Care

11. Equipment Care is defined as the process employed by commanders and equipment users to ensure that their equipment achieves the highest levels of availability in the most cost effective manner. Equipment care is the sum of the physical actions taken by FLC end-users to ensure that their equipment is kept in an operational state. It includes all the routine cleaning, maintenance, forecasting, test and inspection that may be necessary and is the responsibility of the FLC users, assisted by the engineering function. Equipment care is a function of command and enhances operational effectiveness.

12. Policy on the in-service maintenance of vehicles throughout the lifecycle is detailed within JSP 930 (Generic Maintenance, Inspection Certification and Testing (MICaT) of Vehicles). The TLBs undertaking maintenance on land systems will have their own processes in place to provide guidance and assurance for their organisations carrying out equipment care. For example, TLB sponsored policies / standards on equipment care, include:

a. Land Equipment Engineering Standards (LEES)[77];

b. Land Equipment User Maintenance Standards (LEUMS)[78].

c. Military Air Environment policy used by Air Command TLB to manage their land systems.

13. It is noted that other TLBs may adopt the Army equipment care policies as good practice.

Ageing Material

14. Ageing is not about how old your equipment is; it is about its condition, and how that is changing over time. Ageing is the effect whereby a component suffers some form of material deterioration and damage (usually, but not necessarily, associated with time in service) with an increasing likelihood of failure over the lifetime.

15. Ageing equipment is equipment for which there is evidence or likelihood of significant deterioration and damage taking place since new, or for which there is insufficient information and knowledge available to know the extent to which this possibility exists. The significance of deterioration and damage relates to the potential effect on the equipment's functionality, availability, reliability and safety.

[76] Refer to the DCoP (C) for Regulation 3
[77] Army Equipment Support Publication (AESP) 0200-A-090-013
[78] Army Equipment Support Publication (AESP) 0200-A-093-013

16. Just because an item of equipment is old does not necessarily mean that it is significantly deteriorating and damaged. All types of equipment can be susceptible to ageing mechanisms.

Configuration Management

17. Configuration management anchors the technical and operational requirements in documentation that is standard for both the Authority and its Contractors. Application of configuration management principles / practices enables the maintenance and consistency of a product's requirements, design, functional and physical attributes performance and operational information.

18. Effective configuration management ensures that the internal and external interfaces and the various parts of a complete product or system remain compatible, including spares, test equipment, tools, ancillaries and support documentation.

19. Configuration baselines are established by defining materiel both functionally and physically by means of drawings, specifications and other relevant data and documentation. These are prepared at the level of detail necessary to satisfy project needs and are used to assess the potential effects of any proposed changes and to manage the implementation of approved changes.

20. Materiel is constantly verified against the defined product baseline to ensure conformance.

21. JSP 945 contains the policy and direction on Configuration Management across the MOD. The guidance on the application of this policy is currently published under the Configuration Management topic contained within the Engineering Section on the MOD Acquisition System Guidance. Configuration management is a key engineering function and its application is a critical enabler for safety and supportability. Configuration management is a through life activity and must be considered at the earliest stages in the capability lifecycle, from pre-Concept through to Disposal / Termination.

22. Defence Standard 05-57:

a. This Standard provides the Joint Service discipline for the configuration management of defence materiel. This discipline applies to both the Contractor and the Authority to ensure effective control from concept to disposal. It is based on the requirements of NATO STANAG 4159, 'NATO Materiel Configuration Management, Policy and Procedures for Multinational Joint Projects' and NATO STANAG 4427 'Introduction of Allied Configuration Management Publications (ACMPs)'

b. Defence Standard 05-57 sets out the process and requirements for configuration management and the process is represented in Figure 1;

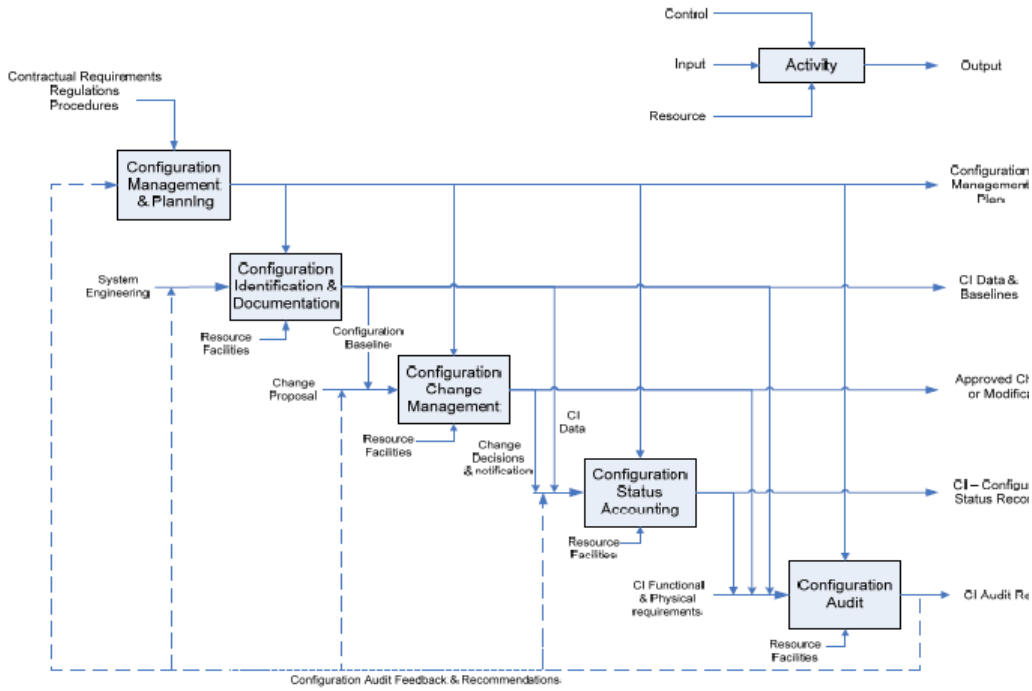


Figure 1: Configuration Management Process

c. Specific land systems configuration management is covered in Annex H of the Def Stan 05-57. This annex provides additional information concerning the application of configuration management for land systems equipment, which were previously covered by the procedures contain within Land Systems Procedure No 123 (LSP 123);

d. The additional information in the annex highlights activities of configuration management, which are necessary for the approval and implementation of in-service modifications for land systems equipment. It is concerned with the control of modifications after design documents have been brought Under Ministry Control through the formal committee structure detailed in the configuration management plan;

e. Annex H details procedures for processing the Modification Proposal Forms, agreeing or otherwise prices for the work and obtaining subsequent authority for the work to proceed.

Retention of Records

23. Poor and inadequate records management creates risk to MOD, including the risk to current or future operations, the risk that MOD does not comply with legislation and / or regulations and the risk that MOD is unable to support legal proceedings. For these reasons it is important that records are correctly retained.

24. It is not possible to provide standard instructions for what, how and how long safety and environmental records should be maintained as the policy and procedures are complex.

25. Guidance on record management and retention throughout the lifecycle can be found in a number of documents, including:

a. JSP 375 Part 2, Volume 1, Chapter 39 provides the procedures and guidance for the management and retention of health and safety records in defence, including the length of time records need to be kept and where;

b. JSP 441: Defence Records Management Policy and Procedures provides comprehensive guidance on record retention policies across Defence, and are to be consulted in conjunction with JSP 375.

Asset Management

26. Asset management for land systems is managed on an equipment by equipment basis rather than a standardised basis across the whole of MOD. Individual Delivery Teams manage assets throughout their life utilising the Through Life Management Plan for each individual new equipment as it proceeds through the lifecycle. The nominated Desk Officer, usually the Equipment Support Manager within the Delivery Teams is charged with maintaining the TLMP and keeping it updated as the equipment evolves and goes through its service life, until eventually it is disposed of, in accordance with the TLMP.

27. In order to manage an asset efficiently the MOD are to record appropriate information relating to an item to provide it with an identity and a through-life record and item level history. This could be achieved by utilising the Joint Asset Management and Engineering Solutions (JAMES).

28. JAMES is an enterprise resource planning system that provides a comprehensive Engineering and Asset Management information management capability for users operating throughout the Land environment.

29. Equipment on JAMES is known as JAMES Managed Equipment (JME), this currently includes Vehicles, Ground Support Equipment (GSE), Communications and some of the Weapon systems. JME is explained in JAMES SOP 20. JME does not normally represent the totality of a unit's equipment which is recorded on the Establishment (AF C8005) and Army Equipment Table (AET), for example, GS tables, chairs, hand and powered tools and minor electrical items.

30. JAMES provides the information architecture to support wider exploitation of equipment data, with an extensive Library of Reports, available within the application and a reports repository and data mining tool for specific reporting requirements.

31. JAMES will facilitate:

a. Management of modifications;

b. Management of key assemblies;

c. Management of spares and repairs;

d. Management of warranty;

e. Management of safety issues;

f. Monitoring of quantity and location;

g. Monitoring of availability, reliability and maintainability;

h. Monitoring of equipment husbandry and care.

32. Equipment is sentenced following inspection or maintenance in accordance with the standard JAMES criteria which are defined as follows:

a. Fully Fit (FF): This is the lowest fault state. It will be used against a fault that has no impact on the functionality or role capability of the equipment. If only faults of this state are recorded against the equipment, the equipment's overall state will remain Fully Fit;

b. Limited Role (LR): Equipment has faults recorded against it that affect the role capability of the equipment. This fault state will over-ride the Fully Fit fault to make the equipment state Limited Role overall. It will be over-ridden only by a Non Taskworthy fault;

c. Non Taskworthy (NT): Equipment has faults recorded against it that mean the equipment cannot be used. This fault covers safety and legislative requirements as well as capability for operational role. This is the highest level fault. It will over-ride all other fault states. Equipment with one fault of this state recorded against it, regardless of any other faults, will make the equipment's overall state Non Taskworthy.

33. The management of assets throughout the lifecycle can be found in a number of key regulatory publications, JSPs and standards associated with asset integrity including:

a. Defence Logistics Framework (DLF) (JSP 886 content was moved into the DLF);

b. JSP 790: MOD Rail Safety Management;

c. JSP 930 specifies the Generic Maintenance, Inspection, Certification and Testing (MICaT) for vehicles;

d. Land Equipment Engineering Standards (LEES);

e. Land Equipment User Maintenance Standards (LEUMS);

f. Defence Standard 00-600: Integrated Logistics Support for MOD projects.

34. The above publications are briefly explained below:

a. The DLF covers the Support Chain and in particular the in-service operation of Support Solutions, including the physical flow of materiel, people, services and information. An element of the Support Chain is the Joint Supply Chain, which are differentiated as follows:

(1) The Joint Supply Chain. The JSC is that element of the Support Chain that covers the policies, end-to-end processes and activities associated with receipt of stocks from trade to their

delivery to the demanding unit and the return loop for all 3 Services;

(2) The Support Chain. The Support Chain is the in-service operation of Support Solutions, including the physical flow of materiel, people, services and information.

b. JSP 945 – This JSP contains the policy on Configuration Management (CM) across MOD. CM is an enterprise wide management activity that applies technical and administrative direction, focusing upon the product's physical and functional characteristics to ensure conformance with requirements and to control the change of formally approved Configuration Baselines. Configuration management is a key engineering function and its application is a critical enabler for safety and supportability. Configuration management is a through life activity and must be considered at the earliest stages in the capability lifecycle, from pre-Concept through to Disposal / Termination;

c. JSP 790 sets out the guidance and criteria for the safe operation and management of all MOD rail activities. It is to be made available to all members of the MOD and associated contractors conducting any aspect of MOD rail activity;

d. JSP 930 specifies the Generic Maintenance, Inspection Certification and Testing (MICaT) of Vehicles. The aim of this maintenance and inspection policy is to maintain vehicles to a standard that:

(1) Satisfies the requirements of statutory legislation by applying periodic and annual mandatory testing to the standards laid down by the Department for Transport (DfT);

(2) Ensures vehicles are maintained in a safe & roadworthy condition;

(3) Ensures operational, engineering and administrative tasks are adequately supported;

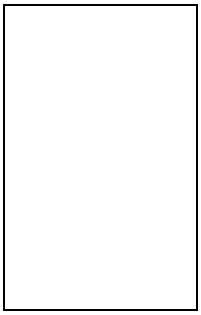
(4) Ensures vehicles complete their planned lives;

(5) Ensures economical use of maintenance resources.

e. Land Equipment Engineering Standards (LEES). LEES provides Equipment Support Commanders with a framework for running a unit by standardising engineering procedures and focusing on the key activities required for the delivery of effective engineering capability, both in barracks and on operations;

f. Land Equipment User Maintenance Standards (LEUMS). LEUMS defines equipment care and Level 1 Maintenance policy. It sets out a framework by which the minimum demonstrable equipment care systems that a unit is mandated to implement can be achieved;

g. Def Stan 00-600 is the Defence approach to Integrated Logistic Support (ILS) for MOD Project Teams. It is MOD policy that ILS will be applied to all product procurement. ILS is a disciplined approach that



influences the product design and develops the Support Solution to optimize supportability and Through Life Finance; it delivers the Initial Support Package and ensures continued optimization of the Support Solution in light of product modifications and changes in operational use and requirements. When the Authority is contracting for support, it needs to manage the risks associated with its contracts and this is enabled by access to and confidence in the results of ILS analysis. This management will apply throughout the lifecycle and will respond to any updates and change of Contractor or support solution.

Glossary: Definitions

The following terms are used throughout this publication:

Term	Definition	Source
Accident	An event, or sequence of events, that causes unintended harm.	Def Stan 00-056
Active Systems	These management systems monitor performance in order to reduce the probability of undesirable events occurring.	
ALARP	As Low As Reasonably Practicable – A risk is ALARP 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 or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction.	Adapted from Def Stan 00-056
Ancillary	Providing necessary support to the primary activities or operation of a system.	
Aspect (Environmental)	Elements of an organisation's activities, products or services that interact or can interact with the environment.	ISO 14001:2015
Assurance	Adequate confidence and evidence, through due process, that safety and environmental requirements have been met.	Adapted from Def Stan 00-056
Audit	A systematic and independent examination to determine whether safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.	Adapted from Def Stan 00-056
Best Practicable Environmental Option	The outcome of a systematic consultative and decision making procedure which emphasises the protection and conservation of the environment.	The Royal Commission on Environmental Pollution
Competent	Describes a person who has sufficient training, qualifications and experience to carry out their role to an appropriate standard.	The Management of Health & Safety at Work Regs 1999
Derogation	A relaxation of a legal requirement to allow the law be applied differently with caveats that are specified within the legislation itself, or not at all.	

Term	Definition	Source
Dis-application	Where specific legislation or a part thereof does not apply to the Military or Ministry of Defence and is expressly stated as such within the piece of legislation.	
Environment	Surroundings which a system or organisation affects, including air, water, land, natural resources, flora, fauna, and their interrelation with humans (third-parties).	Adapted BS EN ISO 14001
Environmental Hazard	A threat to the environment posed by an environmental aspect.	ASEMS POEMS
Environmental Impact	Change to the environment, whether adverse or beneficial, wholly or partially resulting from an organisation's environmental aspects	ISO 14001:2015
Environmental Management System	An Environmental Management System (EMS) is a formal, structured approach to managing the aspects of a sites activities, products or services that have, or could have an impact upon the environment.	JSP 418 Leaflet 1 Environmental Management Systems
Environmental Protection	Prevention of harm to the natural environment.	JSP 430 Part 1 Issue 4
Environmental Risk	A rating of the severity of an environmental hazard against the likelihood of its occurrence.	ASEMS POEMS
Exemption	Where legislation allows SofS to authorise an exemption from all, or part of that legislation. Exemption is conditional on SofS granting a certificate, in writing.	
Exemption Case	A demonstrable justification for exemption(s) from legal requirements on the basis of its expected operational and national security benefits.	
Failure	Failure (of an item) is the loss of ability to perform as required.	(Def Stan 00-49 issue 3)
Hazard	Potential to cause harm, e.g. A physical situation or state of a system, often following from some initiating event that may lead to an accident.	Def Stan 00-056
Hazard Log	The continually updated record of the hazards and accidents associated with a system. It includes information documenting risk management for each hazard and accident.	Def Stan 00-056

Term	Definition	Source
Incident	An accident or a near miss.	
Independent Safety Auditor	An individual or team, from an independent organisation, that undertakes audits and other assessment activities on behalf of MOD to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.	Def Stan 00-056
Inspection	Examination of the Land System, process and policy to determine conformity with regulatory requirements, or on the basis of professional judgement. An inspection is a quality control activity to determine that any work has been performed appropriately. The aim of the inspection is to determine if the land system and its operation is compliant with DSA02, DSA03 and relevant legislation and conforms to the applicable specified safety and environmental requirements	
Land environment	Refers to the physical environment in which a land-based system operates, not the part of the organisation that provides the system. Land systems may operate in the littoral zone; this straddles air, maritime and land environments	
Land systems	Refer to paragraph 8	
Legislation Compliance Assessment	A systematic process that enables the identification and assessment of legislative requirements.	
Near Miss	An unintended event or sequence of events that had the potential to cause unintended harm, but did not.	Def Stan 00-056
Operating Environment	The total set of all external natural and induced conditions to which a system is exposed at any given moment.	Def Stan 00-056
Platform	A series of integrated systems or components designed to carry out a function. (For example a vehicle, a radio system - communications network etc).	
Reactive Systems	These management systems monitor and investigate occurrences of undesirable events in order to reduce the probability of recurrence.	
Residual Risk	The risk remaining after risk reduction.	Def Stan 00-056

Term	Definition	Source
Risk	Combination of the likelihood of harm and the severity of that harm.	Def Stan 00-056
Risk Management	The systematic identification, evaluation and reduction of risk.	Def Stan 00-056
Risk Tolerability	A level of risk that may be tolerated when it has been demonstrated to be ALARP.	Adapted from Def Stan 00-056
Safety	The freedom from unacceptable risks to personnel.	
Safety Assessment	A term used to refer to the whole assessment used to identify hazards, analyse those hazards, estimate risk, validate and verify compliance with requirements.	
Safety Case	A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.	Def Stan 00-056
Safety and Environmental Case Report	A report that summarises the arguments and evidence of the Safety and Environmental Case, and documents progress against the safety and environmental programme. This can be separated into two documents – Safety Case Report and Environmental Case Report.	Adapted from Def Stan 00-056
Safety and Environmental Management Committee	A group of stakeholders that exercises, oversees, reviews and endorses Safety management and Safety engineering activities.	Def Stan 00-056
Safety and Environmental Management Plan	A document that defines the strategy for addressing safety and environmental protection and documents the Safety and Environmental Management System for a specific project.	Adapted from Def Stan 00-056
Safety and Environmental Management System	The organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet safety and environmental requirements and policy objectives.	Def Stan 00-056
Safety Integrity	Properties of the system that contribute to resistance to dangerous failure, including (but not limited to) reliability, availability, robustness, timeliness and use of resources.	Adapted from Def Stan 00-056

Term	Definition	Source
Safety Management System	The organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet safety requirements and safety policy objectives.	Def Stan 00-056
Serious Equipment Failure	An incident that results in, or has the potential to result in, serious personal injury, loss of life or serious damage to property or the environment, in which the failure of equipment is a proximate causal factor.	
SFAIRP	So far as is reasonably practicable (SFAIRP) is the term most often used in the Health and Safety at Work etc. Act and in Statutory Regulations. Broadly equivalent to ALARP.	Health and Safety at Work etc. Act 1974
Shall	Describes an activity that is mandatory.	
Should	Describes an activity that is considered to be best practice. If the activity is followed then this will be considered sufficient to demonstrate compliance with a Regulation. However, alternative approaches may be utilised where this produces an outcome as good as required by the Regulation.	
System	A combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and / or data as appropriate.	Def Stan 00-056
System of Systems	A system that includes more than one element that are themselves systems, and which are interdependent but are not necessarily controlled by the same authority or mechanism.	Def Stan 00-056
Theatre	A specific geographical area of conduct of armed conflict.	
Those holding safety and environmental responsibilities	This describes personnel (responsible persons) that have a duty of care for safety and environmental protection. This includes the three levels of Duty Holder defined in DSA01.1 – Senior Duty Holder, Operating Duty Holder and Delivery Duty Holder.	DSA01.1

Term	Definition	Source
UDR / UOR	The Urgent Defence Requirements / Urgent Operational Requirements process enables rapid procurement to address equipment capability shortfalls that have arisen as a result of current or imminent operations. The funding arrangements determine whether such procurement is a UOR or UDR.	DIN 2010DIN04-195: UOR SI V6

Annex B

Glossary: Acronyms

The following acronyms are used throughout this publication:

ACSO	Army Command Standing Order
AINC	Army Incident Notification Cell
ALARP	As Low As Reasonably Practicable
AoR	Area of Responsibility
ASEMS	Acquisition Safety and Environmental Management System
BPEO	Best Practicable Environmental Option
BTE	Bespoke Trading Entities
CAE	Claims, Arguments and Evidence
CBA	Cost Benefit Analysis
COI	Conflicts of Interest
DG DSA	Director General Defence Safety Authority
DAIB	Defence Accident Investigation Branch
DCoP	Defence Code of Practice
DDH	Delivery Duty Holder
DE&S	Defence Equipment and Support
DEDs	Disapplications, Exemptions or Derogations
Def Stan	Defence Standard
DfT	Department for Transport
DG DSA	Director General Defence Safety Authority
DH	Duty Holder
DINs	Defence Instructions and Notices
DLSR	Defence Land Safety Regulator
DLIMS	Defence Lessons Identified Management System
DMR	Defence Maritime Regulator
DNSR	Defence Nuclear Safety Regulator
DOSR	Defence Ordnance Safety Regulator
DSA	Defence Safety Authority
DSeC	Defence Safety Committee
DSRP	Defence Safety Regulatory Publication
EA	Environment Agency
EISS	Environmental Impact Screening and Scoping
EMS	Environmental Management System
EPA	Environmental Protection Act
FGSR	Fuel and Gases Safety Regulator
FLC	Front Line Command
HF	Human Factors
HS&EP	Health Safety & Environmental Protection
HSE	Health and Safety Executive
HSG	Health and Safety Guidance
HSWA	Health and Safety at Work Act 1974
IET	Institution of Engineering and Technology
ILS	Integrated Logistic Support
ISA	Independent Safety Auditor
JAMES	Joint Asset Management and Engineering Solutions
JSP	Joint Service Publication
KiD	Knowledge in Defence
LCA	Legislation Compliance Assessment
LEC	Land Exemptions Committee
LEES	Land Equipment Engineering Standards

LEUMS	Land Equipment User Maintenance Standards
LFE	Learning From Experience
LSSR	Land Systems Safety Regulator
LSSR SWG	Land Systems Safety Regulator Stakeholder Working Group
MAA	Military Aviation Authority
MOD	Ministry of Defence
MRP	MAA Regulatory Publications
ODH	Operating Duty Holder
POEMS	Project Oriented Environmental Management System
POSMS	Project Oriented Safety Management System
PS	Permanent Secretary
R2P2	Reducing Risks Protecting People
S&EP	Safety and Environmental Protection
SD	Sustainable Development
SDH	Senior Duty Holder
SEF	Serious Equipment Failure
SEMP	Safety and Environmental Management Plan
SEMS	Safety and Environmental Management System
SFAIRP	So Far As Is Reasonably Practicable
SofS	Secretary of State for Defence
TFA	Trading Fund Agency
TLB	Top Level Budget
ToRs	Terms of Reference
UDR	Urgent Defence Requirements
UOR	Urgent Operational Requirements
USUR	Urgent Statement of User Requirement
VPF	Value of Preventing a Fatality