Ministry of Defence

JSP 815 Volume 2

Element 7: Equipment Design, Manufacture and Maintenance

Contents

Amendment record

This element has been reviewed by the Defence Directorate of Safety (DDS) together with relevant subject matter experts and key Safety stakeholders. Any suggestions for amendments **should** be sent to COO-DDS-GroupMailbox@mod.gov.uk

Version No	Date	Text Affected	Authority
1.0	Dec 22	BETA version for consultation	Dir HS&EP
1.1	7 June 23	Final version of Volume 2	DDS

Terms and definitions

General safety terms and definitions are provided in the Master Terms and Definitions Glossary which can also be accessed via the GOV.UK page.

Must and should

Where this element says **must**, this means that the action is a compulsory requirement.

Where this element says **should**, this means that the action is not a compulsory requirement but is considered good practice to comply with the policy.

Scope

This policy applies to all those employed by Defence (military or civilian) as well as those working on behalf of Defence (for example, contractors). It applies to all Defence activities carried out in any location (UK or overseas).

Introduction

1. This element provides the direction that must be followed and the guidance and good practice that should be followed and will assist Defence organisations to comply with the expectations for equipment design, manufacture and maintenance that are set out in Element 7 of the Volume 1 to JSP 815 (this JSP).

Note: The term 'Equipment' used in this element refers to all types of equipment, vehicles, platforms, systems or services that are acquired to meet a capability requirement.

Purpose and expectations

2. This element ensures that the Defence organisation has put in place frameworks and working practices to incorporate safety considerations into the design, acquisition, manufacture, operation, modification, and maintenance of equipment, including Defence digital systems. References to 'equipment' throughout this element are considered to include its design, manufacture, import, supply, in-service use and disposal within Defence.

The CADMID/T lifecycle

3. After Defence has identified and expressed a capability requirement it uses a six-phase lifecycle approach for the acquisition of equipment to meet that capability requirement, the six phases are: Concept, Assessment, Demonstration, Manufacture, In-service and Disposal / Termination (CADMID/T). The CADMID/T lifecycle approach adheres to the HMT Green Book (which provides guidance to Government Departments on how to appraise policies, programmes and projects. Requirements should be set against key stage-gates to evaluate and consider the suitability and purpose of equipment against approved performance envelopes. Approval points across the CADMID/T lifecycle correspond to the overall ownership of the equipment and key information deliverables align to those approval points such as safety case reports where they are applicable.

Concept, Assessment and Demonstration (CAD)

4. During the initial phases of CADMID/T, there is the greatest opportunity to embed safety by design into equipment. Hazards to be managed by the equipment, as well as those caused by the equipment should be evaluated and risk assessed. The risk assessment should not be limited to operation of the equipment, but also maintenance, training and other activities. In most cases, this will include identification of critical safety controls, instrumentation and systems required for safe operation of the equipment, and the different contributions of the various Defence Lines of Development (DLOD). The safety case within the CAD phases should progressively inform how the equipment will be maintained and disposed of under current expectations and known safety risks.

5. During concept and design stages and within the safety case, the proposed operating envelope for the equipment should be determined. Any potential commission, life extension or uses outside of the planned and approved scope may also be considered. The risks of such extensions or further scope of operation should be evaluated so they are known and understood in advance.

Manufacture (M)

6. During manufacture, key decisions related to design amendments, or changes to materials or systems design may impact the safety risks in future operation and maintenance. A change management process owned by the Senior Responsible Owner (SRO) or the User should be followed to re-assess risks and evaluate the impact of the proposed changes.

In-service (I)

7. The appropriate and compliant use of equipment should be included in the relevant risk assessments and aligned with the safety case. The safety case should be proportionate to the risks being faced. Guidance on safety cases relating to equipment is below, with additional guidance provided in Element 4 of this Volume 2 and in more detail in JSP 376 - Acquisition Safety Policy.

8. Risks must be assessed if there are any shortfalls in maintenance, operator training or levels of crewing and controls put in place where necessary to ensure continued safe operation, e.g. by imposing operational limitations until the situation can be remedied. The risk assessment should also consider the hazards and risks of conducting maintenance or other remedial activity, and the cumulative effect of multiple shortfalls.

9. During the in-service phase, many factors can change how equipment is used, such as changes in operator training, operating procedures, environment of use, or other interfacing equipment. Where equipment is planned to be used outside standard operating procedures and scope that have previously been approved, the risk assessment should be updated to reflect these situations and scenarios. Operating limits should be regularly reviewed and re-assessed so that equipment is maintained and operated within defined parameters. Mechanisms should be in place to communicate these operating limits to those who operate and maintain the equipment.

Disposal and service termination (D/T)

10. The Defence organisation should address any safety considerations during their assessment of how equipment will be taken out of service and appropriately disposed of or how any services are terminated. The Disposal and or termination phase should be considered and planned for throughout the equipment lifecycle and constantly updated and refined throughout each subsequent phase.

Compliance with legislation and regulations

11. Section 6 of the Health and Safety at Work etc Act 1974 (HSWA) requires any person who designs, manufactures, imports, or supplies equipment for use at work to:

a. ensure, so far as is reasonably practicable, that the equipment is designed and constructed to be safe and without risks to safety when it is being used, cleaned or maintained;

b. take necessary steps so that those using equipment have adequate information about its use. It also expects that the equipment is used in a safe manner, without risks to safety, including when it is being dismantled or disposed of; and

c. take necessary steps to provide all relevant and revised information to users, so they are made aware of anything which may give rise to a serious risk to safety.

12. The Provision and Use of Work Equipment Regulations (PUWER) 1998 is secondary legislation raised under HSWA, to amplify Section 6. It requires that equipment provided for use at work is:

a. suitable for the intended use;

b. safe for use, maintained in a safe condition and inspected to ensure it is correctly installed;

c. used only by people who have received adequate information, instruction and training; and

d. accompanied by suitable safety measures, such as protective devices. and controls.

13. Defence must comply with all H&S legislation, unless covered by a disapplication, exemption or derogation (DED). Defence organisations may be able to apply for a DED for certain equipment in certain circumstances but any DEDs must be clearly approved and set for a defined period and reviewed prior to their expiry date and throughout the equipment lifecycle. DEDs are covered in more detail in Element 3 of this Volume 2.

14. Safety should be considered at all stages of equipment integration and across the eight DLODs which are: training, equipment, personnel, information, logistics, doctrine & concepts, organisation and infrastructure. The DLODs are a checklist for capability deliverers to ensure all key factors relevant to the capability have been considered, and that issues that require resolution have been identified. It is generally the responsibility of the SRO / User to consider the safety risks along with all other DLOD risks and issues and their effects, however this responsibility may change as the equipment moves through the CADMID/T phases. Issues from the integration of equipment should be documented so that lessons can be learned and proactively communicated across the Defence organisation and wider Defence to help prevent future recurrence.

Equipment design and safety cases

15. As part of their strategy for demonstrating safety, the SRO for an equipment should consider whether a safety case will be required and what form it should take. Safety cases are described in Element 4, and considerations for safety as part of the acquisition process are set out in JSP 376. Considerations affecting the need for a safety case for an equipment include the following:

a. Whether a safety case approach is proportionate given the complexity of the equipment and the level of risk involved, or whether a simple risk assessment would be more appropriate;

b. Whether a standalone safety case is required for the equipment, or whether it would be better incorporated in the safety case for the activity, capability, or higher-level system that the equipment is used in;

c. Whether separate safety cases are necessary for different applications of the equipment, or different contexts of use (e.g., test and evaluation, training);

d. Whether legislation or Defence regulation mandates particular requirements for the safety case;

16. Construction of the safety case for an equipment should start as early in the acquisition lifecycle as possible and should be an integrated part of the equipment design, rather than a supplementary activity. As well as providing a justification that the equipment is (or will be) safe to use, the safety case should be an aid to its design and the planning of the acquisition programme. Planning in advance the safety argument that the SRO hopes to be able to make when a system is delivered and used in service should inform the safety requirements for the equipment, and the type of activities that will be necessary in the acquisition programme and during operation to generate the evidence to support the safety case. This information should in turn support decisions such as the choice of supplier and whether to use a bespoke, off-the-shelf or customised design.

17. Safety cases for equipment should be forward-looking and take into account activities beyond normal operation and training. They must also consider how equipment can be manufactured, tested, commissioned, transported, stored, maintained and disposed of safely. Stakeholder input will be required to validate assumptions made by the safety case about the contribution of other DLODs. Input from human factors specialists is also likely to be required to ensure these activities can be carried out safely and easily. Risk controls that cannot be put into practice easily are unlikely to be effective.

18. Safety cases should be updated to match the configuration of the equipment and when there is a 'material change' to the understanding, risk profile, design or operation of the equipment. Safety performance monitoring of the equipment should be maintained throughout the in-service phase for sustaining the safe performance of that equipment, any safety related issues identified must be acted upon. They should also be recorded in the safety case to demonstrate in an auditable way that the safety of the equipment is being achieved.

19. When equipment has been in service for a long time, it is particularly important to check that the assumptions made by the safety case are still valid and have not been undermined by factors such deterioration in the material state of aging equipment, obsolescence of the parts or services necessary to support them, or demographic changes in the user community.

Operational Requirement to use Equipment in line with the Parameters of its safety case.

20. The Defence organisation should implement risk control measures so that identified equipment are 'safe to operate.' Those managing other DLODs will work together so that the overall system capability will "operate safely" within the bounds of a defined Statement of Requirements (SOR) and comply with any additional requirements within Defence regulations.

21. Actions taken to make equipment safe should be able to demonstrate:

a. that equipment is safe for use within its specified parameters of application and environment through a documented and structured argument with supporting evidence;

b. how risks will be managed to levels that are ALARP and tolerable and that the required information, instruction, training and other control measures are proportionate and adequately communicated to the user;

c. that all safety related information has been collated, whether generated by contractors or Department stakeholders;

d. that all safety requirements, including relevant process and procedural requirements have been identified and complied with. If safety requirements have not been fully complied with, the residual risk and any further mitigating activity should be clearly set out;

e. that safety requirements are valid, i.e., they have been derived by thorough analysis of appropriate specifications and artefacts, and that they correspond to the equipment as designed and implemented. Safety requirements should be updated through the equipment lifecycle, to reflect any changes to operating requirements and conditions;

f. that the assessment undertaken of the equipment is proportionate to the level of safety risk;

g. suitable records of the arrangements for effective planning, organisation, control, monitoring and review of preventive and protective measures to maintain risk to ALARP are maintained;

h. that staff undertaking key roles with defined responsibilities have the appropriate competencies for those roles; and

i. that all contractual safety requirements have been discharged.

22. The receiving users should be able to demonstrate:

a. formal acceptance of ownership and "holding to account" of the supplying party for the delivery of all safety control measures, documentation and training requirements;

b. that protective devices and controls, information, instruction and training requirements were received from the delivery organisation and implemented; and

c. adequate supervision was provided and risk assessments reviewed prior to the equipment entering service.

Management of change

23. The Defence organisation should introduce mechanisms to become aware of new equipment requirements and changes when they arise. It may be possible that the change is tolerated within the existing safety case and expected equipment operation. Otherwise, a change to the safety case should be undertaken to reflect the updated means of operation.

24. Changes may occur due to adjustments to statute, technology, social, environmental or political influences, along with alterations in the way that equipment is being used.

25. Defence organisations should formally re-assess the risks they face on a continual basis through equipment lifecycle, to remain up to date with their use.

26. Where an operational requirement exists to use equipment outside of the parameters of their safety case, the Commanding Officer should be able to demonstrate evidence of possession of a formal written dispensation from their Chain of Command or the Operating Duty Holder (if one is in place).

27. The evaluation, risk assessment, approval, implementation and documentation of all physical changes should consider the following essential elements:

a. agree and evaluate the technical justification for the change at the appropriate management level;

b. risk assess the proposed change using a multi-disciplinary team of competent people, including specialists, contractors, vendors and suppliers when their particular experience and knowledge is required;

c. put in place a rigorous design approval process to ensure that the appropriate engineering standards are applied to the design, and any deviations from design are approved by a suitably qualified and competent person with sufficient knowledge and experience. If the Defence organisation does not have control of the design, it should request confirmations from the design holder on its rigour;

d. write formal procedures to implement the change, train all personnel who are directly affected by the physical change and obtain confirmation that training has been effective; and

e. confirm the change has been communicated to all relevant stakeholders, maintain records of the change and share feedback and lessons learned for the benefit of continuous improvement.

28. Prior to implementing the physical changes of any item of equipment, a pre-start up safety review should be conducted to:

a. ensure that all actions from the risk assessment process have been incorporated into the design and any deviations from established standards or practices have been approved at the appropriate level;

b. confirm that all necessary testing has been successfully completed;

c. confirm that procedures for operating the equipment are in place and personnel are trained in the use of these procedures; and

d. confirm the change has been communicated to all stakeholders.

29. Once the physical changes to the item of equipment have been completed, these changes should be monitored closely. Feedback and lessons learned should be recorded for the benefit of continuous improvement and future projects.

Equipment and supply chain

30. Additional equipment safety risks can be generated in the supply chain. Selection of suppliers should take into account their competence and capability to meet safety requirements, and the availability of information to support their safety assessment. Access to safety information can be impacted by issues such as commercial confidentiality, national regulation, and the necessary information may not exist for previously developed equipment. Such issues should be addressed before the supplier is selected.

31. In accordance with JSP 940 MOD Policy for Quality, robust and rigorous processes should be put in place to assure the quality of equipment supplied to MOD. These should include processes to assist the MOD to get the product “right first time”, as well as to provide appropriate feedback to supply chain and suppliers when defects in equipment are discovered on acceptance or later in the equipment lifecycle.

32. Defence organisations should proactively manage risk within the supply chain of equipment they use or rely on, ensuring that ownership of risks is clear.

33. Change of supplier or provider requires consideration and increased quality assurance to verify equipment is suitable for purpose and of the required quality.

Lessons learned

34. Defence organisations should undertake regular, lessons learned reviews relating to any incidents or occurrences. These reviews should focus on informing and updating their Safety Management System (SMS) and capturing new understanding in a learning from experience (LfE) log. Lessons learned should also provide updated feedback into relevant safety cases and equipment users. Lessons learned should be documented and communicated as widely as possible across the organisation. Where available Defence organisations are to consider lessons learned from previous equipment design, acquisition, manufacture, operation, modification, and maintenance activities.

35. When a safety concern is raised (faults, safety occurrences, near-misses in-service or other concerns at any point in the equipment's life cycle) an assessment or re-assessment of related safety controls should be undertaken and formally documented. Assessments (including any necessary investigations) should seek to:

a. understand what contributed to the specific safety concern;

b. understand the potential consequences, what prevented the outcome from being worse, and the reliability of those controls;

c. identify related safety concerns (similar procedures or equipment such as vehicles with turrets or same type of weapon system; and more generically such as vehicle blind-spots and so on);

d. address any systemic weaknesses identified in the overall SMS for example a lack of certification or suitable quality checks;

e. update the safety case and communicate these changes as necessary;

f. present recommendations to the appropriate stakeholders to address the above; and

g. use the outcome of the assessment to review the effectiveness of the occurrence management process.

36. All concerns and required actions should be communicated to the relevant stakeholders in a timely manner as identified in the Defence organisation's communications plan. Raising safety concerns is set out in Element 11 of this Volume 2 and reporting safety occurrences is set out in Element 10 of this Volume 2.

37. Defence organisations should set out recall and urgent safety advice procedures to manage all equipment determined to be defective or inappropriate for specific uses.

38. Processes and controls to manage safety risks should be regularly updated, following identification of new risks and re-assessment of existing risks. Any changes to risk management should be revised in the Defence organisation's SMS and communicated to key stakeholders.

Element summary

39. Defence organisation leaders are to make sure that their organisation has:

a. Mechanisms in place to identify and assess safety risks and requirements associated with equipment throughout its CADMID/T lifecycle.

b. Mechanisms in place to ensure risks associated with equipment are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate level within the chain of command.

c. Mechanisms in place to ensure equipment is compliant with statute or DEDs in place where compliance is not achievable.

d. Processes in place to ensure equipment is always maintained and operated within defined design and operating limits and has mechanisms in place to communicate these operating limits to those who operate and maintain equipment.

e. Mechanisms in place to ensure physical changes to equipment, (including major software changes), materials and associated specifications are evaluated, risk assessed, approved, and documented.

f. Mechanisms in place to accurately identify and manage the safety risks and dependencies in their equipment supply chain.

g. Processes in place to share lessons learned from previous equipment design, acquisition, manufacture, operation, modification and maintenance activities.

h. Mechanisms in place to assess the risk from system integration into equipment and the effects this has on equipment safety.