Table of Contents

12. Safety Case and Safety Case Report

ASEMS Document Version:
4.1
Effective From:
Friday, 31 January, 2020 - 00:15
Summary:
This procedure provides guidance on the development of a Safety Case and Safety Case Report. The Safety Case brings together all project safety information, forming a number of arguments which are summarised in the Safety Case Report.

12.1. Introduction

12.1.1. Definitions

12.1.1.1.

A **Safety Case** is defined in Def Stan 00-056 [1] 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 environment.”

12.1.1.2.

A **Safety Case Report** is defined in Def Stan 00-056 [1] as:

“A report that summarises the arguments and evidence of the Safety Case, and documents progress against the Safety Programme.”

12.1.2. Objectives

12.1.2.1.

The purpose of the Safety Case is:

1. To document evidence that the Safety Requirements are being met, and that all identified risks are tolerable and As Low As Reasonably Practicable (ALARP);
2. To demonstrate that any activities underway at that time (including tests or trials) can be carried out safely;
3. To describe clearly the evidence and arguments used to justify the safety of the system that the processes and assessments made are appropriate and adequate, so that agreement can be reached on the validity of the claim of tolerable safety;
4. For systems requiring safety approval outside the Project (eg by a Safety Regulator, Safety Certification Authority or for integration into a higher-level system), the Safety Case contains the documentary evidence submitted for approval and will also include approval notifications or rejections.

12.1.2.2.

The Safety Case Report is the means by which the Project demonstrates that all of the safety issues relating to a project have been brought to a condition appropriate for the stage in the life cycle. It therefore provides the safety justification to support the major project milestones as identified in Section 12.4.2 of this procedure.

12.2. Procedure

12.2.1. Method

12.2.1.1.

Within MOD, the Safety Case regime has been adopted not only as the means to demonstrate that the required, tolerable, levels of safety have been achieved, but also as the basis for the management of safety. It is also used to demonstrate compliance with legislative and regulatory requirements.

12.2.1.2.

The generation of a Safety Case is an iterative process. It starts during the Concept stage of a project, with the setting of requirements, and develops through the Assessment, Development and Manufacturing stages to influence and validate the design and then finally qualifying the equipment and the Safety Management System supporting it in service.

12.2.1.3.

The Safety Case will bring together the entire project Safety information generated by the Contractor(s) and the MOD, including the outputs of all Safety Assessment and Risk Management activities described in Procedures SMP01 [2], SMP02 [3], SMP03 [4], SMP04 [5], SMP05 [6], SMP06 [7], SMP07 [8], SMP08 [9]and SMP09 [10].

12.2.1.4.

The Safety Case body of evidence can contain factual, historical, analytical, test and judgmental information. It may not all be stored together, but the Safety Case approach should ensure that important safety information is recognised as such, and preserved in a traceable way.

12.2.1.5.

The Safety Case will provide the mechanism for Safety submissions to many MOD authorities providing Safety approvals (e.g. Safety Certificates) or acting as internal MOD Safety Regulators in specific areas (e.g. Naval Authorities for Key Hazards). It is vital that Projects identify the approvals that it will be necessary for them to obtain and plan how to provide the necessary information in a timely manner.

12.2.1.6.

Where it is considered beneficial, combined Safety and Environmental Case Reports should be issued for a Project. It will be ensured that the safety and environmental programmes are aligned as far as possible and that data is shared where relevant.

12.2.2. Safety Case as Good Practice

12.2.2.1.

The Safety Case concept is considered best-practice because:

1. It has a Safety Assessment of risk at its core, which facilitates the prioritisation of effort and the judgement of what is a disproportionate use of resources;
2. Almost all highly complex industries, particularly those involving hazardous processes are now regulated through a Safety Case;
3. Common law considers written evidence (safety justifications) to have more weight than verbal testimony, making a written Safety Management System, prioritised by a Safety Assessment, essential for the discharge of legal obligations;
4. Structured, written records of safety decisions (the Safety Case) mitigate against high MOD staff turnover and the problems that large organisations historically have with corporate memory;
5. Information developed within system specific Safety Cases can be developed and reused for similar system types, facilitating feed-back of lessons learnt and economies of scale;
6. Safety Cases, efficient Safety Management Systems and a robust Safety Culture reduce whole life costs, facilitating better change management, business improvement, improved morale and efficiency by reducing accidents;
7. Risk Management allows innovative approaches and facilitates the incorporation of Engineering Judgement, which works well in the Defence industry sector where decisions are complex and value judgements are often required.

12.2.3. Arrangements for Production of Safety Case Documentation

12.2.3.1.

The Project Safety Management Plan should:

1. Identify the person responsible for overseeing the production of the safety documentation;
2. Define the process for approval of the safety documentation, both within and external to the Project;
3. Describe the arrangements in place to:
    1. Prepare, review and assess safety documentation pertaining to design, construction, manufacture, operation and disposal/decommissioning,
    2. Show how safety documentation is categorised in accordance with its safety significance,
    3. Have such documentation produced by Suitably Qualified and Experienced Persons,

4. Have the documents approved at the appropriate level and reviewed at appropriate intervals.
5. Where necessary, have the document reviewed by independent, Suitably Qualified and Experienced Persons,
6. Where necessary, submit documents to Safety Regulator(s) and/or approval Authorities external to the Project.

4. Describe the requirements for safety documentation to cover procurement, commissioning, operation, maintenance, modification and decommissioning of equipment or systems, and supporting infrastructure if appropriate.

12.2.4. Necessary Evidence in the Safety Case

12.2.4.1.

As a minimum, the Safety Case should provide evidence that:

1. All Safety Requirements, including relevant process and procedural Safety Requirements have been met, or there is adequate mitigation for failures to meet the Safety Requirements;
2. The set of Safety Requirements is valid, i.e. they have been derived by thorough analysis of appropriate specifications and artefacts, and that they correspond to the system as designed and implemented;
3. That the assessment undertaken is appropriate to the equipment and level of risk identified;
4. Derived Safety Requirements are traceable to and from their source;
5. Derived Safety Requirements are sufficient to meet Safety Requirements from which they are derived;
6. The Safety Management System has been implemented as defined;
7. The staff undertaking key roles with defined responsibilities had the appropriate competencies for those roles;
8. All applicable legislation, regulations, standards and MOD policy have been complied with;
9. All contractual safety requirements have been met.

12.2.5. Development Through the Life cycle

12.2.5.1.

There should be a seamless development of the Safety Case from one project phase to the next, building on the core of data and information. A Safety Case should begin at the formative stages of the project with high level Safety Assessment of project requirements (performance requirements, targets and criteria). Specific safety requirements arising from such assessment should be fed back into project requirements and the Project Safety Plan as part of the continuous management process.

12.2.5.2.

During system development, Safety Case Reports should show the progress in risk reduction and producing safety evidence. In operation they support the operational use of the system, and present data on the rate of occurrence of safety-relevant events and remedial action, if any, needed to preserve safety.

12.2.5.3.

During the Assessment, Development and Manufacture phases, Safety Case Reports should be produced and updated as the design and development progresses. The following are considered the minimum required (see also the guidance document SMP12/G/02 - Safety Cases during the Project Life Cycle [11]):

a. At Main Gate setting out the issues to be dealt with and the strategy to be followed to achieve the requirements;
b. Prior to System Acceptance, or as part of the assessment process – to demonstrate that the agreed levels of safety performance have been achieved or solutions have been identified;
c. Prior to User Trials – to ensure that risks to MOD personnel, others and facilities etc. are under control (particularly where safety and operating documentation is incomplete and training may be only partial);
d. Prior to production – to confirm that production has not reduced the level of safety performance achieved during the design stages;
e. Prior to Introduction to Service – to confirm that all necessary prerequisites (e.g. facilities) and management arrangements (e.g. training courses, logistic support) are in place to maintain the predicted level of safety performance throughout the In-Service phase.

12.2.6. Hierarchy of Safety Cases

12.2.6.1.

Where a system includes sub-systems that have separate Safety Cases, these Safety Cases should be integrated, or reconciled, with the system Safety Case. This will assist in demonstrating that interface and other safety issues have been managed effectively, and that assumptions and cascaded Safety

Requirements have been properly addressed.

12.2.6.2.

If the equipment is part of a larger system (e.g. integrated onto a Platform or arranged in a “system of systems”), then the Delegated Authority responsible for the higher level system should be satisfied that the safety performance of the equipment is adequate. These safety performance requirements should be taken into account in setting the requirements for the equipment (see Procedure SMP10 – Safety Requirements and Contracts [12]) and should be covered by the system acceptance process.

12.2.7. Safety Case(s) for Options

12.2.7.1.

Where a Project is considering more than one option for a given capability, a generic Safety Case should be initiated pre Initial Gate which should be developed for each proposed option during the Assessment Phase. As potential options are eliminated, the respective Safety Case may be closed off, but retained for future reference.

12.2.8. Safety Cases for Systems with Variants etc.

12.2.8.1.

A single Safety Case Report may be written to cover several minor variations of a system, through the use of appendices for each variant or by using compatibility matrices.

12.2.9. Safety Case Caveats and their Removal

12.2.9.1.

It may be necessary for a Project to proceed through a key milestone with incomplete information on some Safety issues. For stages of the project where people are exposed to the equipment (e.g. trials, training and in-service usage), the Delegated Authority should carefully consider how this information shortfall can be addressed.

12.2.9.2.

If it is decided to proceed with “caveats” on the Safety Case, then the delegated authority should consider carefully factors such as:

1. How are the caveats or limitations on usage to be promulgated to those who need to know?
2. How is compliance with the caveats or limitations to be enforced?
3. Do the caveats or limitations introduce additional Hazards or increase the Risks associated with any known hazards?
4. If there are multiple caveats or limitations, might they interact in some way that degrades safety?

12.2.9.3.

It is important that the need for caveats or temporary limitations is considered in a systematic way and not hurried due to Project pressures to achieve the milestone.

12.2.10. Retention of Safety Information

12.2.10.1.

MOD policy for retaining safety related information is to comply fully with the requirements of civil statute. Where personnel are exposed to a hazard to health, the latest information available to the FSMOs is that specific legal requirements for keeping records are for:

1. exposure to hazardous materials or related occupational disease health surveillance records, (eg including asbestos and lead) are to be kept for forty years after any incident or exposure;
2. exposure to biological agents for ten years after any incident;
3. health surveillance records on ionising radiation for fifty years after any incident;
4. compartment air monitoring for exposure to hazardous substances must be kept for forty years after the incident;
5. personnel breathing apparatus records (including compressed gases) are to be kept for forty years after any incident;
6. general work place monitoring, test or maintenance records of control equipment to be kept for five years after any incident;

7. respiratory protective equipment records for two years after any incident;
8. personal accident records (medical) for three years after any incident;
9. general health and safety records (eg noise assessments and work-place Risk Evaluations), where the process of assessment is on-going, remain valid until a new assessment is made;
10. monitoring and documentation retention of nuclear plant safety and munitions disposal are specified by the Naval Authority;
11. where there is no statute stipulating information retention times for specific hazards, the MOD Legal Advisor advises that safety related documentation (eg Safety Cases and safety certification) should be kept for ten years after equipment disposal. When equipment is sold, all such pertinent documentation should be handed to the new Delegated Authority.

12.2.10.2.

Departmental Safety Management Systems should ensure that records are retained and instruct Delegated Authorities and others to comply with the departmental regulations, forwarding any data collected in their respective areas.

12.2.11. Disclosure of Safety Information

12.2.11.1.

The Public Interests Disclosure Act permits the exemption of MOD establishments and operational training areas from disclosing sensitive information. However the Secretary of State for Defence is unlikely to seek a dis-application unless there is strong evidence that the release of information required by civil statutory regulations would seriously compromise national security or the achievement of operational goals.

12.2.11.2.

In general, all unclassified safety documentation should be readily retrievable and made available for inspection by other government departments, safety regulators and authorised public representatives.

12.2.12. Use of Existing Safety Information

12.2.12.1.

In some instances, the Project may wish to base the Safety Case on data that already exists; for example from civilian certification authorities or other Nations' approval regimes. If this data is to well-known standards, it may be possible to provide, in the Safety Case, a reasoned argument which justifies the Project's decision to dispense with or reduce the scope of other safety analyses and independent tests and trials.

12.2.12.2.

The value that may be attached to data about previous experience and use of the system should be discussed with the all relevant stakeholders including certification authorities and Defence Regulators where appropriate. For such data, any Contractor should demonstrate its applicability to the updated system.

12.2.13. Retrospective Application

12.2.13.1.

For legacy equipment where the design has already been accepted by MOD, or equipment is already in-service, and no Safety Case exists, a Safety Appraisal should be undertaken. A Safety Appraisal is aimed at ensuring that all the hazards presented by a Product, System or Service are understood and that adequate measures are in place to manage those hazards.

12.2.13.2.

For projects that have reached this stage in their life-cycle, the majority, and most likely all, of the hazards present should already have been identified and measures taken to control them. Whether this is the case or not, the Safety Case, based on the Appraisal, should provide the formal record of the system under review, the hazards identified, any analysis and assessments made, and actions taken to mitigate the hazards, and manage any residual hazards.

12.2.13.3.

Where legacy Products, Systems or Services are being subjected to a Safety Appraisal, the output of the appraisal should be a Safety Case Report. The assessment will be based on a top down review of the likely safety risks presented by the equipment in its operational roles, and experience with the equipment e.g. accident and defect records, as well as anecdotal evidence. It will examine, or audit, the extant

arrangements for ensuring safety and its support, against the likely risks identified in the assessment. Any identified shortfalls in the adequacy of arrangements should be recorded, and recommendations should be made to ensure that the required level of safety can be sustained.

12.2.13.4.

The extent of any Safety Case will only be decided after a preliminary, top-down Safety Assessment has been undertaken (see Procedure SMP04 – Preliminary Hazard Analysis [5]). This consists of a brief but structured identification of tasks and issues implicit in the User Requirements and functionality, followed by a brainstorming of what associated hazards may arise.

12.2.14. Extent of the Safety Case

12.2.14.1.

The size and scope of a Safety Case will vary, and should be proportional to the complexity of the system and level of risk involved.

12.2.14.2.

The process for removal of caveats should also be carefully planned, including the use of reviews and application of the normal approvals process.

12.2.14.3.

The extent of the work required will depend upon the age and condition of the equipment, the hazards associated with the system and the effort required to demonstrate that the risks are ALARP. An appraisal of the future exposure to risk during the remaining service life is an important factor in the level of study undertaken.

12.2.14.4.

It is unlikely that a safety scoping analysis will be sufficiently detailed to give a confident assurance that all identified risks are ALARP. The results instead give guidance for subsequent work and form a logical basis for more detailed Risk Evaluation. The subsequent effort allocated during the entire Safety Assessment process should be in proportion to the nature, number and risk (likelihood and severity) of the hazards identified. The size of a Safety Case may range from a few pages, for relatively low-risk equipment, to the extensive requirements for a nuclear licence.

12.2.14.5.

The Project will take advice from suitably competent individuals, both within the Project and externally, to judge the level of assurance required and decide when the increasing levels of confidence as work progresses and knowledge increases, create a sufficiently robust Safety Case to stop further analysis. Appropriate Senior Managers, Commanding Officers and Central Customers should be advised when the Project is unable to mitigate a serious hazard or produce a sufficiently robust argument, due to a lack of resources, unavailable information or inadequate stakeholder support. Recommendations will also be submitted to address these shortcomings. Where these issues prove difficult to resolve, the Project or Independent Safety Auditor (if appointed) should approach the relevant Defence Safety Regulator for advice and to facilitate arbitration.

12.2.15. Depth of the Safety Case Report

12.2.15.1.

Although the Safety Case comprises the complete documentation providing evidence that the system is safe, there may be a requirement to summarise the arguments in a number of forms according to the defined readership. For example, the individual responsible for approving the Safety Case Report would require a concise summary (an Executive Summary) illustrating the strength and completeness of the arguments used and the reasons as to why the system is safe. A Regulator would require considerably more in the way of technical details to support the arguments offered, with references to the low-level detailed documentation.

12.2.16. Scope of Safety Claims

12.2.16.1.

It should be recognised that Legislation includes absolute, prescriptive and proscriptive requirements, as well as those requiring risk to be made tolerable and ALARP. Thus the Safety Requirements for an equipment or service are likely to include absolute aspects as well as risk-based aspects. The Safety Case will therefore do more than show that all identified risks have been made ALARP.

12.2.17. Rigour of Safety Case Argument

12.2.17.1.

The nature of the argument for safety should vary according to the complexity and type of system under scrutiny, and hence the rigour of argument offered will reflect the nature of the system. The Safety Case should be regarded as being a single, coherent argument for safety, this will usually be broken down into a series of detailed arguments, which may be further broken down as appropriate. To provide an indication of the degree of rigour that will be required in the arguments offered, a safety integrity requirement for the system will be agreed between the Project, the Contractor (where relevant) and any regulatory or approval authorities.

12.2.17.2.

In general, deductive and inductive arguments based on explicit product evidence are more credible than those that appeal to development processes. Arguments should be developed in accordance with the following order of precedence:

1. Deductive, where the conclusion is implicit in the evidence used to support the argument;
2. Inductive, where the argument is firmly based on the evidence presented, but extrapolates beyond the available evidence;
3. Judgmental, where expert testimony, or appeal to custom and practice is necessary to support the conclusion.

12.2.18. Review and Approval of Assumptions

12.2.18.1.

The Safety Case, particularly early in the life cycle, is likely to be built on several assumptions. These may be for issues where direct evidence is not yet available (e.g. trials results), but the strength of the Safety Claim depends on the realism and credibility of these assumptions.

12.2.18.2.

It is important that assumptions which cannot be replaced by evidence should be reviewed and agreed by the stakeholders with direct subject matter knowledge. This review and agreement should be sought early rather than when the Safety Case Report including the assumptions is being reviewed. A mechanism for this is to document the assumptions in a standalone report (eg Master Data and Assumptions List or MDAL). The MDAL can be issued, reviewed and updated well before the production of the Safety Case Report.

12.2.19. Justification of Assessment Processes

12.2.19.1.

The robustness of the Safety Case should be dependent on the appropriate techniques being applied at the right time to ensure that risks are properly identified, are fully understood and attract the appropriate level of mitigation. The techniques and processes used to undertake these activities will be demonstrated in the Safety Case as being adequate.

12.2.20. What if the Safety Case Concludes that the System is not Safe Enough?

12.2.20.1.

The Safety Case may not be able to conclude that the system is adequately safe for its given application and given environment. In such situations, the Safety Case Report should identify the areas of shortfall and provide a clear conclusion that the system is not considered to be adequately safe.

12.2.20.2.

The Safety Case Report will also record the measures taken to reduce Risk and the reasoning why any other identified strategies for Risk reduction have been judged not to be “reasonably practicable” (see Procedure SMP09 – Risk Acceptance [10]).

12.2.20.3.

It is a valid outcome for the Safety Case to conclude that the Product, System or Service is not safe enough and it should be the decision of the Duty Holder to determine if the Product, System or Service should be used. Nevertheless, the application of the Safety Case approach should ensure that such conclusions are identified early in the life cycle before the expenditure of too much time and cost on development routes which will not have adequate safety performance.

12.2.20.4.

If specific risks are identified and evaluated as being “Unacceptable” even after the application of all practicable risk reduction measures, then details of this will be raised up to 2* level within the Top Level Budget for discussion and resolution at 2* level with Equipment User and Duty Holder (see SMP09 – Risk Acceptance [10]). Agreement in writing will be referenced in the Hazard Log and included in Safety Case Report, defining the circumstances under which risk exposure is considered acceptable and explaining why (e.g. the over-riding military necessity under particular conditions).

12.2.21. Safety Case Report Review and Sign-off

12.2.21.1.

When a Safety Case Report is generated, it should be reviewed and agreed by the relevant stakeholders. The following terminology is used in this Procedure to distinguish between the different types of review and “sign off” that will be applied to Safety Case Reports:

- Agree (a document) - To agree that a document fairly represents the current situation, within the scope of knowledge of the signatory
- Endorse (a document) - To assert that a document meets the requirements of relevant policy, procedures and good practice.
- Authorise (a document) - To assert that a document may be issued and that it reflects the individual’s acceptance of responsibility.
- Assurance - Adequate confidence and evidence, through due process, that safety requirements have been met. (Def Stan 00-056 [1])

12.2.21.2.

To assist in understanding the relationship between the different terms, an example of a process for a document to be authorised is as shown:

Safety Case Report Approvals

12.2.21.3.

Endorsement by Independent Safety Auditors and Assessors is required as defined in domain-specific JSPs. Non-regulatory safety authorities should only be involved where a Project is relevant to their policy. Boxes with bold, solid borders show activities which are mandatory for every document approval cycle.

12.2.21.4.

The order of review by Independent Safety Auditors and the stakeholders may be different from that shown and may occur in parallel.

12.2.21.5.

The approvals process should also change at different stages of the life cycle, depending on the purpose of the Safety Case Report (see later in this document Further Guidance - Safety Cases during the Project Life Cycle). At early stages of the Project, the Safety Authority may act as a Subject Matter Expert before authorisation by the Team Leader, or individual with formally-delegated safety responsibilities. Safety Regulators should also be involved early, to indicate to the Project whether the Safety Case approach is likely to result in approval of the activity.

12.2.21.6.

By virtue of their MOD status, the Defence Safety Authority in its role as a Regulator has a variety of safety related sanctions at its disposal to manage enforcement actions required. These range from issuing Corrective Action Reports at the lowest level all the way up to either the removal of personal authorisations or the removal of the approvals needed to operate equipment at the highest level.

12.2.21.7.

It should be recognised that the same terms are used differently in other documents (e.g. “Endorsement” of Safety Case Reports by the Duty Holder is specified in DSA02-DMR MOD Shipping Regulations for Safety and Environmental Protection [1]).

12.2.21.8.

The Safety Case body of evidence cannot itself be approved, accepted, endorsed and authorised. However, the Safety Case Report, which provides a summary of this evidence at a particular time, will be subjected to this process.

12.2.22. Review of Safety Case Reports by the Project and Panel

12.2.22.1.

A Safety Case Report will be produced at key milestones and as a periodic status report on the safety of the developing system. Their content and delivery points will be contractually agreed between the Contractor and the Project and will be defined in the Project Safety Management Plan. Typically for a major project, Safety Case Reports should be produced at the following times;

1. Approval of the project Business Case at Initial Gate;
2. Approval of the project Business Case at Main Gate;
3. Clearance to begin Demonstration trials;
4. Completion of the major aspects of design, (design baseline agreed);
5. Commitment to production;
6. Clearance to begin testing/acceptance/User trials;
7. Introduction to Service;
8. Significant changes to the design or material state (e.g. mid-life update);
9. Significant changes in operational usage;
10. Disposal.

12.2.22.2.

Authorisation of the Safety Case Report signifies that the Project has followed due process and that all identified risks have been addressed. Prior to the Safety Case Report’s authorisation, any risks that cannot be reduced to ALARP, should be recorded in the Hazard Log as uncompleted actions and included in the Project Safety Plan and Safety Case Report for corrective action in the next phase. All Project Safety Committee members will agree the interfaces and responsibilities for such outstanding actions defined within the Safety Plan. Where risks cannot be mitigated further, Projects should either seek a judgement on military ALARP, or additional resource from a Senior Manager, who in turn may notify the Defence Safety Board, of concerns regarding resource shortfalls.

12.2.23. Approval and Authorisation within the Project

12.2.23.1.

Authorisation of a Safety Case Report by the member of the Project with formally-delegated safety responsibilities indicates their satisfaction with the progress of the Safety Case and their acceptance of the safety risks associated with the Project. The authorised Safety Case Report forms an auditable record.

12.2.23.2.

The satisfactory resolution of any deficiencies or observations raised by advisors, including the Project Safety Committee and Independent Safety Auditor (if appointed), should be ensured prior to authorisation of the Safety Case Report.

12.2.24. Approval and Authorisation outside the Project

12.2.24.1.

The Duty Holder responsible for the Product, System or Service is likely to be part of the Front Line Command. The Duty Holder may also be the lead User, but in all circumstances, these should be consulted in the development of the safety management through the life of the Product, System or Service. The ability to determine what level of risk may be endorsed by a Safety and Environmental Management Committee or Project is in the context of the Front Line Command's Duty Holder model and that Duty Holder's willingness to accept the risk as presented to them.

12.2.24.2.

For Land Systems (see DSA02-DLSR-LSSR [1]), the Duty Holder responsible for the Product System or Service should demonstrate their acceptance of the safety argument and what is required to manage the activity of operating the Product, System or Service. This is demonstrated by jointly signing the Part 3 Safety Case together with the member of the Project with formally-delegated safety responsibilities. When a Safety Case is updated, each new issue should be similarly signed.

12.2.25. Endorsement by Authorities Responsible for Regulation, Certification and/or Approval

12.2.25.1.

For those systems being acquired under a formal regulatory regime, the Safety Case should include the documentary evidence that supports the submission to the regulator. Any certificates or other approval notifications confirming that the relevant regulatory requirements have been met should be included within the Safety Case. Such approvals/certificates may also be associated with particular safety requirements.

12.2.26. Approval of Safety Case Reports

12.2.26.1.

When a Safety Case Report is issued to support a key project milestone, it will be reviewed by the Project Safety Committee including the Independent Safety Auditor, if appointed, and agreed by them if they are satisfied that it fairly represents the current Safety status for the project. Their observations and recommendations will be included as part of the Safety Case Report which will then be presented to the member of the Project with formally-delegated safety responsibilites for authorisation

12.2.27. Acceptance and Endorsement of Safety Case by Regulators and Certification/Approval Authorities

12.2.27.1.

The Project Safety Management Plan will identify the Safety Approvals that will be required for the project and show how the necessary information will be provided in a timely manner. For example those who may be involved in receiving Safety submissions and providing Safety Approvals (or similar), include;

1. Ordnance, Munitions & Explosives Safety Review Panel;
2. Naval Authorities (for Ship Key Hazards);
3. Military Laser Safety Committee;
4. Authorities for Platforms or Systems onto which the equipment will be fitted (including for trials);
5. Authorities fir Facilities or Sites where the equipment will be used, stored etc.;
6. Authorities responsible for safe transportation.

It is important for the Project to recognise the difference between authorities providing safety advice with those with the responsibility for operating Regulatory regimes. Whilst following appropriate advice and complying with a regulatory regime are evidence of good practice, they do not transfer the Project's safety responsibilities to the Advisor, Regulator or Approving Authority.

12.2.28. Review and Revision of Safety Case and Re-Issue of Safety Case Report

12.2.28.1.

The age and status of equipment is not about how old the Product, System or Service is; it’s about what you know about its condition, the impact of change and use in the operating environment, and how that changes over time. Any change in age or status of the equipment that challenges the basis on which the original Safety Case was developed or issued should initiate a review. This is particularly relevant in circumstances where changes in operations, equipment state, organisation or control measures have the potential to appreciably alter risk.

12.2.28.2.

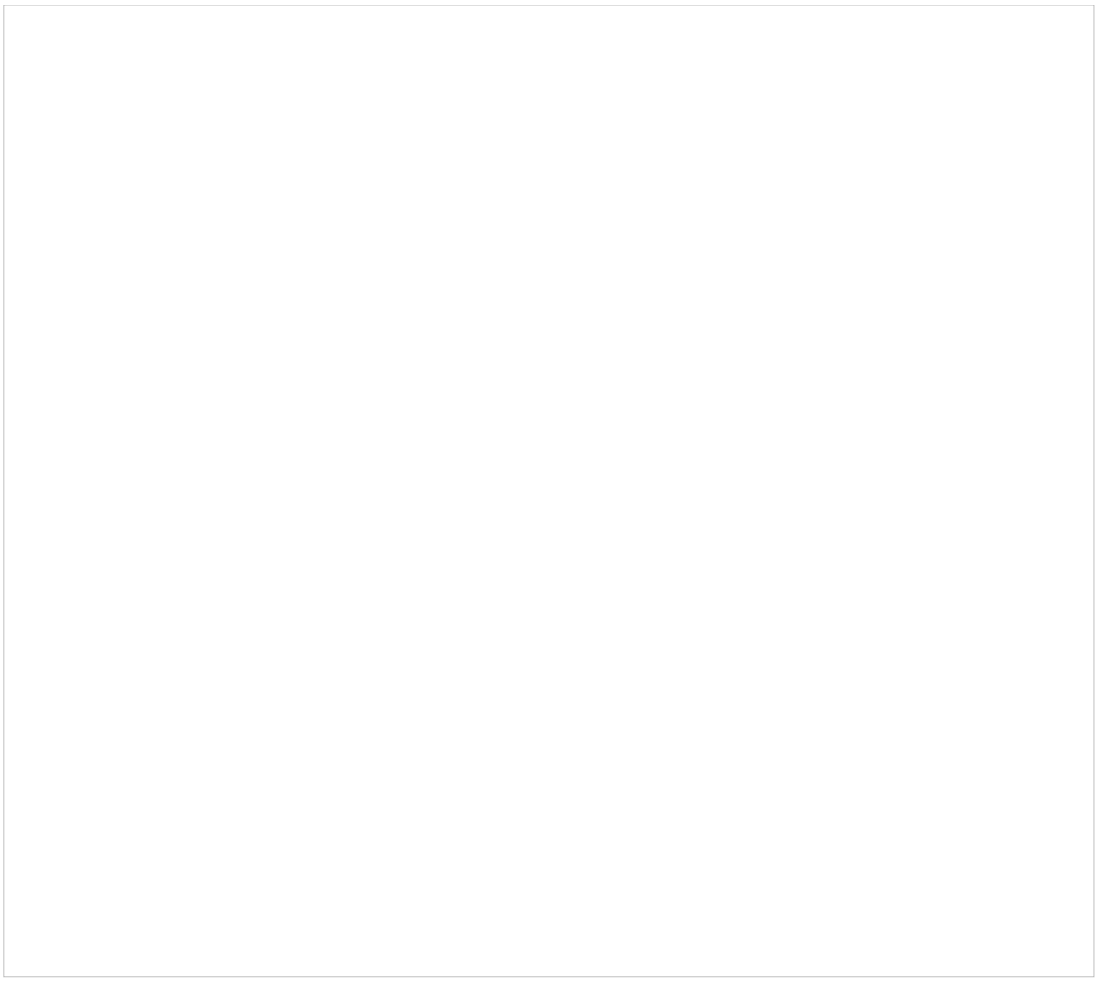
The identification of impacts that would initiate review can be communicated through numerous channels. These will be captured across the Safety Case and supporting Safety Management System and may include both physical modifications and operational management changes. Figure 12.1 indicates the relationship between the Safety Management System and Safety Cases where this information may be managed effectively.

12.2.28.3.

Examples of status changes that should warrant revisions are:

1. Structural modifications or repairs of any system where the changes have an impact upon safety;
2. Introduction of new activities to the system or in connection with it;
3. Changes to the operating environment or equipment role;
4. Information received as a result of Accidents/Incidents;
5. Information received as a result of Maintenance/ Inspections ;
6. Changes to the Safety Management System, including the contracting out of or change to safety management functions;
7. Extension of use of the system beyond its original design intent and/or design life;
8. Decommissioning prior to disposal;
9. Major changes in technology.

Figure 12.1: Relationship between the Safety Management System and Safety Case in terms of Age and Status



12.2.29. Review of the Safety Case

12.2.29.1.

Throughout the life of the system, the evidence and arguments in the Safety Case should be challenged in an attempt to refute them. Should evidence arise which undermines a previously accepted argument, the validity of the whole Safety Case should be questioned and the safety of the system be re-assessed. In such cases it may be necessary to obtain further evidence, carry out remedial action or even take the system out of service, depending on how seriously the Safety Case has been undermined by this counter-evidence.

12.2.29.2.

The Safety Case is a live set of documentation that should be reviewed and updated as the system progresses through its life. For example, specific safety requirements for the disposal of a system element may emerge that did not apply when disposal was addressed during earlier project phases. This review process will be particularly important when a system has been in service for a long period of time. Special care is necessary when upgrading systems, as part of a mid-life update for instance. Due regard should continue to be paid to the issue of safety as previously considered safe systems can become unsafe over time.

12.2.30. Ownership and Administration

12.2.30.1.

Irrespective of contractual arrangements, the member of the Project with formally-delegated responsibility for safety has a special responsibility for delivering capability and managing most forms of risk. The safety delegation holder should be the appointed custodian of the entire Safety Case, responsible for co-ordinating all safety activities, with specifically delegated responsibility for construction and maintenance of the Safety Case and for elements of the Safety Management System associated with Designers, including oversight and compilation of all safety justifications.

12.2.30.2.

Severe degradations in material state and/or invalid certification will demonstrate a clear failure in safety management arrangements that may undermine justifications with a Safety Case.

12.2.30.3.

Responsibility for the production or maintenance of the Safety Case may change over the system life, but the safety delegation holder retains ultimate ownership of the Safety Case. The Contractor (who may also change through the life of the system) will often develop and maintain the Safety Case through the life of the system on behalf of the Project.

12.2.30.4.

Even where the scope of the Contractor's activities is limited to a part of the system life, the Safety Case should still address the entire life of the system. This should ensure that safety issues are not neglected until it is too late to do anything about them.

12.2.30.5.

The Contractor should not produce a Safety Case in isolation. Significant input from the Project, Users and other organizations, where appropriate, should be obtained, particularly in relation to operational safety. The Contractor should work closely with the Project to ensure that all parties are aware of the scope of their involvement and that they deliver what is expected from them.

12.2.30.6.

The Safety Case documentation and other material may pass from one Contractor to another during the life of the system, including when the system is accepted into service. Although the Safety Case is owned by the Project, how and when the Safety Case will be delivered should be clearly defined and agreed.

12.2.31. Records and Project Documentation

12.2.31.1.

Where relevant, the outputs from this procedure should feed into the following:

1. System Requirements Document – for any specific Safety requirements;
2. Customer Supplier Agreement – to document agreements on Safety information to be delivered by the Project;
3. Through Life Management Plan;
4. Safety elements of Initial Gate and Main Gate submissions.

12.2.31.2.

Records of all management assessments, processes and procedures, including all decisions on mitigation and the acceptability of suitable alternatives should be held for each project within the Project's Safety Case.

12.2.31.3.

The Safety Case will normally be held by the Project Safety Manager, and maintained by them as up-to-date.

12.2.31.4.

The Safety Case documentation will be subject to configuration control and it may be appropriate to use a computer-based Document Management System. It should be noted that not all the documentation will necessarily be held by MOD.

12.2.31.5.

The Hazard Log (see Procedure SMP11 – Hazard Log [13]) is a key part of the Safety Case.

12.2.31.6.

A Safety Case Report will provide a snapshot summary of the Safety Case at key milestones. In addition, Safety Case Reports will provide details of the progress made in managing safety since the previous report. A Safety Case Report will be structured around the safety claims for the system and the planned activities. A Safety Case Report will provide justifiable confidence that the Safety Case is, or will be, adequate and that the expected progress is being made on planned activities.

12.2.31.7.

The contents of the Safety Case Report should vary according to the maturity of the Safety Case and the intended readership. It has two functions: firstly, to assure the member of the project with formally-delegated responsibility for safety that safety risks are being managed effectively, so it should include a clear and concise summary of the Safety Case and safety progress; secondly, to highlight key areas of risk to

the operators and users, so it will provide information that will support operational decision-making, such as a decision to operate outside the design envelope.

12.2.32. Warnings and Potential Project Risks

12.2.32.1.

The warnings and potential project risks identified in all the other procedures, from SMP01 [2]to SMP11 [13]can manifest themselves through effects on the Safety Case which brings their outputs together. In addition to these, the following other project risks specific to the Safety Case, have been identified.

12.2.32.2.

If the authorities with a safety approval role external to the Project are not identified and consulted early in the project, then it is likely that their information requirements will not be considered. The effects of this could include delays in achieving safety approval, unexpected cost to provide the necessary submission evidence or failure to identify Safety requirements that prevent the introduction to service. Alternatively, the member of the project with formally-delegated responsibility for safety might authorise the release of the system for service use when it does not comply fully with the requirements of regulatory or approval authorities.

12.2.32.3.

If the Safety Case is not reviewed on a regular basis, then it is likely not to be an accurate reflection of the system, its usage pattern and its Safety performance. Examples of counter-evidence which invalidate areas of the Safety Case might not be identified and necessary corrective measures would not be considered or taken.

12.2.32.4.

If insufficient time is allowed for the review of the Safety Case Report then either problems may not be detected and rectified, or authorities may be unwilling to sign it off. This could lead to delays to the milestone covered by that Safety Case Report (e.g. introduction to service).

12.2.32.5.

If the Safety Case is not maintained consistent with the material state of the in-service system, then the safety argument which it contains will not be credible.

12.2.32.6.

If Safety Case documentation is not well managed, then key safety evidence may not be retained or it might not be easily found. Either of these outcomes would weaken the ability of the Safety Case to provide an auditable record of the decision making process for safety and thus the justification for current status.

12.2.32.7.

If the techniques used for the safety assessment are not appropriate a weak or incomplete Safety Case will result.

12.2.33. Procedure Completion

12.2.33.1.

The Project Safety Manager will be responsible for the completion of this procedure. However, in most cases, a large part of the detailed work may be carried out by contractors. In all cases Project Safety Committee members and other stakeholders should be involved in providing both inputs and reviewing outputs.

12.2.33.2.

Where different contractors are in completion with each other and have carried out separate Hazard Analyses, contractual and managerial arrangements should be made for the output from all to be made available to the successful contractor. This will reduce the likelihood of hazards being missed.

12.2.33.3.

In large or complex projects, the Project Safety Manager must co-ordinate the Safety Case across the project to ensure that all relevant and credible hazards identified through Hazard Analysis by any party, including those outside the scope of a particular contractors control, are captured and managed through the Hazard Log.

12.3. Timing

12.3.1. Initiation of the Safety Case

12.3.1.1.

The Safety Case body of evidence will start to be populated as soon as Safety Management activity is initiated.

12.3.2. Production of Safety Case Reports

12.3.2.1.

A Safety Case Report will be produced at key milestones and as a periodic status report of the developing system. Their content and delivery points should be contractually agreed between contractor and the Project and be as defined in the Project Safety Management Plan. Typically for a major project, Safety Case Reports would be produced at the following times;

1. Approval of the Project Business Case at Initial Gate;
2. Approval of the Project Business Case at Main Gate;
3. Clearance to begin demonstration trials;
4. Completion of the major aspects of the design, (design baseline defined);
5. Commitment to production;
6. Clearance to begin testing/acceptance/User trials;
7. Introduction to Service;
8. Significant changes to the design or material state (e.g. midlife update);
9. Significant changes in operational use;
10. Disposal.

The Safety Case report may be produced by MOD, the Design or Support Contractor or by third parties, depending on the life cycle stage and other factors. Nevertheless, it will be subjected to a similar process of review and approval.

12.3.3. Periodic Review of the Safety Case

12.3.3.1.

Since a Safety Case is a live set of documents that require update, configuration control and review to ensure that they address all safety considerations, these reviews should be specified in the Project Safety Management Plan.

12.4. Required Inputs

12.4.0.1.

This procedure for the Safety Case and Safety Case Report requires inputs from:

1. Outputs from Procedure SMP01 – Safety Initiation [2];
2. Outputs from Procedure SMP02 – Safety Committee [3];
3. Outputs from Procedure SMP03 – Safety Planning [4];
4. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [5];
5. Outputs from Procedure SMP05 – Hazard Identification and Analysis [6];
6. Outputs from Procedure SMP06 – Risk Estimation [7];
7. Outputs from Procedure SMP07 – Risk and ALARP Evaluation [8];
8. Outputs from Procedure SMP08 – Risk Reduction [9];
9. Outputs from Procedure SMP09 – Risk Acceptance [10];
10. Outputs from Procedure SMP10 – Safety Requirements and Contracts [12];
11. Outputs from Procedure SMP11 – Hazard Log [13].

12.4.0.2.

The Safety Case body of information will include outputs from all the Safety Management activities conducted on a Project. In particular, it will include:

1. Safety Plans;

2. Disposal Plans;
3. Hazard Log;
4. Register of legislation and other significant requirements;
5. Minutes of Project Safety Committee meetings;
6. Safety Reports (e.g. Hazard Identification, Hazard Analysis, Risk Estimation, Risk Evaluation);
7. Safety Assessment or Safety Case Reports for particular aspects of the system or activities associated with the system (e.g. Software Safety Case, Disposal Safety Assessment);
8. Safety Requirements;
9. Records of Design Reviews and Safety Reviews;
10. Results of Tests and Trials;
11. Incident reports and records of their investigation and resolution;
12. Safety Audit Plans;
13. Safety Audit Reports;
14. Records of Safety advice received;
15. Results of Safety inspections;
16. Records of Safety approvals (e.g. Certificates);
17. Minimum Equipment List (i.e. vital to Safe operation);
18. Emergency and Contingency Plans/Arrangements;
19. Limitations on Safe Use;
20. Master Data and Assumptions List;
21. Evidence of compliance with Legislation and Standards;
22. Evidence of adequacy of tools and methods used.

12.5. Required Outputs

12.5.0.1.

The primary outputs of the Safety Case are an identified and controlled body of information relating to the Safety of the system, supporting a documented and reasoned argument that allows a claim to be made that the system is tolerably safe.

12.5.0.2.

The physical outputs of the Safety Case are the Safety Case Reports. These are the means by which the Project demonstrates that all of the safety issues relating to the Project have been brought to a condition appropriate for the stage in the life cycle.

12.5.0.3.

An example for a Safety Case Report can be seen under Further Guidance - typical content of a Safety Case Report; it will be adapted to suit the project characteristics or phase of the programme to which it relates.

12.6. Annex A

12.6.1. Typical Content of a Safety Case Report

12.6.1.1.

The following document is a template for a Safety Case Report and should be tailored to meet individual project requirements.

12.6.1.2.

Executive Summary

The executive summary should enable the Duty Holder to provide assurance to stakeholders that they are content with the progression of work and that safety requirements have been, or will be, met by:

1. Confirming that Safety Case work has been, or is being, progressed satisfactorily;
2. Confirming that all other stakeholders have acknowledged their safety responsibilities;
3. Recommending or otherwise progression to the next stage of the acquisition cycle or the next defined milestone confirming that safety risks associated with the next stage can be satisfactorily managed.

12.6.1.3.

Summary of System Description

A brief description of the system should be provided, noting that a full system description should be contained within the Safety Case. The summary should be sufficient to enable the boundaries and scope of the Safety Case and its interfaces with other Safety Cases to be clearly defined and understood.

12.6.1.4.

Assumptions

Assumptions that underpin the scope of the safety case, or the safety requirements, argument or evidence, should be stated. For example, this may include numbers of personnel, training levels, operational profiles, time in service, operating environment etc.

12.6.1.5.

Progress against the Programme

An assessment of progress against the safety programme should be provided that describes:

1. An indication of the current status relative to the expectations documented within the programme, including an assessment of any impacts on future progress;
2. Progress on safety management since the previous Safety Case Report, including identification of any new Hazards and Accidents and progress on Risk Management activities;
3. Progress against agreed actions placed on stakeholders.

12.6.1.6.

Meeting Safety Requirements: The following should be included:

1. A statement describing the principle agreed Safety Requirements;
2. A summary of the argument and evidence that demonstrates how the Safety Requirements have been, or will be, met. This will described:
    1. Summary of the Hazards and likely Accidents associated with the system, noting the main areas of risk. Note: The main areas of risk will also be highlighted under the Operational Information heading. Safety requirements that are unlikely to be met, either in part or in full, with remedial/follow-up actions identified;
    2. Risk management actions that are outstanding identifying both the risk and the organisation responsible for its management;
    3. The residual risk that is, or is anticipated to be, posed by the System;
    4. Issues of particular sensitivity, e.g. use of restricted materials, or with significant project or corporate risk;
    5. Regulatory approvals/certificates, and any associated restrictions, that are currently in place;
    6. Any counter evidence found that may invalidate the Safety Case, including a description of the activities taken to address this counter-evidence;
    7. Feedback, reporting and auditing arrangements for defects and shortfalls;
    8. Particular issues related to interfaces between different systems.

12.6.1.7.

Emergency/Contingency Arrangements

A statement confirming that appropriate Emergency/Contingency Arrangements (e.g. procedures) have been or will be put in place and identification of any areas where such arrangements do not exist or are inadequate.

12.6.1.8.

Operational Information (this section will be aimed specifically at the operator). Outputs from the Safety Case that are relevant to the management of operational safety, including:

1. A description of the operational envelopes;
2. Any limitations on use or operational capability;
3. The main areas of risk e.g. Class A/B risks;
4. Relevant information that can assist the operator in balancing the operational imperative against safety risk;
5. Demonstration that operating and maintenance procedures and publications have been, or will be, developed.

12.6.1.9.

Independent Safety Auditor Report

Where an Independent Safety Auditor is engaged, a formal Independent Safety Auditor report should be prepared for inclusion in the Safety Case Report.

12.6.1.10.

Conclusions and Recommendations

Conclusions will be provided, including an overall assessment of the safety of the system and any recommendations to enable issues identified within the report to be resolved.

12.6.1.11.

References

A list of key reference documents will be provided.

12.7. Annex B

12.7.1. Safety Cases During the Project Life Cycle

12.7.1.1.

Appendices

These will include:

1. Hazard Log sheets;
2. Diagrams of the Safety Case Claim and Argument structure (e.g. Goal Structured Notation);
3. Calculations;
4. Analyses;
5. List of Hazardous Materials (e.g. Control of Substances Hazardous to Health and Classification, Labelling and Packaging);
6. List of lifting and manual handling Hazards, together with their weight and reference to approved lifting procedure;
7. Safety certificates.

12.7.1.2.

Concept Stage/Initial Gate Safety Case

12.7.1.3.

During the production of the User Requirement Document, the Project, working with the Equipment Capability Customer will ensure that the safety requirements are identified and recorded in the developing Safety Case. At this early stage of the project, there will be little technical data available and the Safety Case should be in outline form, with the Risk Estimation being carried out for each business option on a functional basis. Safety assessment will test ideas embedded in initial requirements and identify Hazards to facilitate safety-led design.

12.7.1.4.

Each potential acquisition strategy may have a different safety philosophy and Safety Case. In particular, potential solutions may involve the acquisition of Products, Systems and Services rather than just equipment and in these cases, the safety assessment should cover the whole service and not just the equipment design. By the end of the Concept phase, the Project should have developed a safety strategy in sufficient detail to demonstrate that: the safety risks are understood; the Safety Case can be properly managed throughout the remainder of the acquisition phases; and that key milestones and acceptable feasible high level safety targets have been identified. These factors will be described in a Safety Case Report in support of the Business Case seeking approval at Initial Gate.

12.7.1.5.

At this stage in a programme there may be a number of unknown factors, or areas that are not fully defined. The submission should identify these areas and the assumptions made, justifying the strategy for dealing with them as the programme progresses.

12.7.1.6.

Assessment Phase/Main Gate Safety Case

12.7.1.7.

The safety aspects of the Main Gate Business Case should be based on a Safety Case Report that updates and reviews the work done in the first iteration, based on improved knowledge of the options being followed. It should consider the safety work undertaken on the possible solutions being followed, and argue the strength, and weaknesses from a safety point of view, for the recommended technical and acquisition option.

12.7.1.8.

During the development of the System Requirements Document, the Project will ensure that the technical solutions under consideration are subject to a safety assessment, and that the strategies for achieving the safety requirements are documented. Preliminary safety assessments of each of the competing technical solutions, identifying the Hazards and risks through life and the strategies for their control, are to be undertaken. The Projest, in conjunction with the Equipment Capability Customer, should then consider, the feasibility of meeting, or in accordance with the ALARP principle exceeding, the baseline safety criteria, for each of the potential technical solutions. The Project will describe these assessments in Safety Case Reports in support of the Business Case seeking approval at Main Gate.

12.7.1.9.

Demonstration/Manufacture and Trials Safety Case

12.7.1.10.

The safety of the planned Demonstration phase tests and trials will be assessed and documented to justify embarking on the trials programme. In particular, prior to the commencement of significant trials phases, the safety of the planned trials should be addressed by Safety Case Reports.

12.7.1.11.

Test and trials should form an important role in demonstrating the achievement of safety Requirements. Projects have a responsibility to consider the risks associated with the conduct of the tests and trials they require. In particular, they should review circumstances that fall outside the assumptions regarding normal operation, so that the design intention/material state of the platform, system or equipment concerned is not compromised.

12.7.1.12.

The Safety Assessment should influence how safety requirements are demonstrated to be achieved. This might be through calculation, simulation, test, inspection, factory equipment test, user trails, with the optimum balance reflected in the Integrated Trials, Evaluation and Assessment Plan. The Safety Case will address the Project’s responsibilities for ensuring that sufficient instruction, guidance, training and resources are available and that all those with safety responsibilities clearly understand their duties, i.e. the Safety Management System in operation during the trials is appropriate.

12.7.1.13.

Where Contractors conduct trials the arrangements for limiting MOD’s liability should be specified contractually. Project representatives will ensure that the safety arrangements for attending MOD staff are adequate and that the arrangements for MOD’s assets and of equipment it seeks to own are sufficient before each test or trial occurs (in accordance with the Integrated Trials, Evaluation and Acceptance Plan). Such assurance will be in place before any Service personnel are contracted or co-opted for testing, approval or acceptance activities or whenever they assist in platform/system operation prior to its entry into service. Given the management complexity and the potential Hazards during Contractor Trials, Projects will commission specific Safety Assessments and raise a Trials Safety Management Plan for such events, as part of, or cascaded from, the Project Safety Plan and the Integrated Trials, Evaluation and Assessment Plan.

12.7.1.14.

Safety Case for Introduction to Service

12.7.1.15.

The Safety Case will be developed to support the introduction of the system to service. In particular, this will demonstrate that the prerequisites for continuing Safety during the in-service phase are adequate and in place. This should typically include aspects such as support facilities, training arrangements, competent Users and Maintainers, Logistic Support arrangements etc.

12.7.1.16.

This Safety Case will be maintained throughout the In-Service life and reviewed as changes are introduced to the design, the equipment’s operation or the conditions under which it is used.

12.7.1.17.

Disposal Safety Case

12.7.1.18.

The safety risks related to planned or inadvertent disposal will be considered at the earliest stages of the programme to avoid designing into the equipment hazardous features such as materials or stored energy which cannot be recovered, disarmed or made safe when required.

12.7.1.19.

It should be remembered that ‘Disposal’ also occurs throughout life (typically from the Demonstration phase onwards, although any Disposal Plan should be considered at the concept stage) as, for example, prototypes or test articles are no longer used, consumables are discarded, lubricants changed, parts are made redundant through wear or modification, repair schemes are implemented and accident damaged systems are made safe and recovered. The Project must ensure that all eventual and through life disposal safety risks are addressed in the Safety Case for each phase; defining the procedures to be followed for the safe management of all disposal risks.

12.7.1.20.

The Project must ensure that the Safety Case addresses decommissioning and disposal of the system or equipment. The Safety Case should cover:

1. Disposal of hazardous materials;
2. Safe recovery and disposal, or neutralisation of the hazard if recovery is impractical, following an incident or accident.

12.7.1.21.

MOD is increasingly being expected to operate in an environmentally sustainable manner. Projects must design for the disposal of systems and equipment, considering the increasing need to eventually recycle components. Systems sold at the end of life should comply with all current health, safety and environmental legislation and should not be sold in a condition that would be considered unacceptable for continued UK service.

12.7.1.22.

The Project must ensure that the disposal agent (e.g. Disposal Sales Agency) is informed of the relevant safety issues, prior to their joint agreement as to the best contractual route for disposal. Designers are reminded that they may only transfer their responsibilities to a competent body.

12.7.1.23.

A disposal Safety Case should therefore be created for systems sold for scrap as well as for those sold or transferred on loan for further use. In cases of loan or continuing use, the Project must focus effort on confirming their contractual and legal obligations for safety in order to minimise MOD’s liability for subsequent claims for compensation. Disposal customers may require evidence of a Safety Case.

12.7.1.24.

Stage in Project	Safety Case Report Purpose	Authorise by Project Member with Formally-Delegated Safety Responsibilities	Endorse After Delegation Holder Authorisation (not able to "Red Card")	Approval of Activity after Delegation Holder Authorisation (able to "Red Card")	Comments
Initial Gate	To demonstrate, through an adequate assessment of the capability being pursued, that the potential safety risks are	After reviews by: 1. Stakeholders & Subject Matter Experts (Safety Panel) 2. Independent Safety Assessors (if relevant) 3. Independent Safety Auditors (if relevant) And taking account of their		Initial Gate submission contains short summary of Safety Case Report. Scrutinisers examine Business Case only (not Safety Case Report itself). Project **will** consult potential MOD Regulators (Naval Authorities &	Initial Gate

Stage in Project	Safety Case Report Purpose	Authorise by Project Member with Formally-Delegated Safety Responsibilities	Endorse After Delegation Holder Authorisation (not able to "Red Card")	Approval of Activity after Delegation Holder Authorisation (able to "Red Card")	Comments
	understood and a strategy has been developed to control them.	recommendations		Ordnance, Munitions & Explosives Safety Review Panel) and approval authorities under Stakeholder and Subject Matter Expert review.	
Individual Assessment Phase Option (where necessary)	To document the Safety Feasibility for a specific Project Option	As above		Project **will** consult potential MOD Regulators (Naval Authorities & Ordnance, Munitions & Explosives Safety Review Panel) and approval authorities under Stakeholder and Subject Matter Expert review. Document may conclude that the Option cannot be made tolerably Safe.	Individual Assessment Phase Option (where necessary)
Main Gate	To compare Safety of Assessment Phase options, identifying any Safety aspects which prevent an Option being taken forward. Demonstrates that the identified safety risks can be managed and controlled for the selected Option.	As above	None	Main Gate submission contains short summary of Safety Case Report. Scrutinisers examine Business Case only (not Safety Case Report itself). Project **will** consult potential MOD Regulators (Naval Authorities & Ordnance, Munitions & Explosives Safety Review Panel) and approval authorities under Stakeholder and Subject Matter Expert review.	Main Gate
Demonstration Trials (where necessary)	To demonstrate that specific Demonstration Trials using MOD facilities and/or personnel can be conducted with adequate and known	As above	MOD Trials Authorities	Only relevant where MOD provides Trials facilities or personnel (if MOD are only observers, they **will** be covered by Contractor's Safety	Demonstration Trials (where necessary)

Stage in Project	Safety Case Report Purpose	Authorise by Project Member with Formally-Delegated Safety Responsibilities	Endorse After Delegation Holder Authorisation (not able to "Red Card")	Approval of Activity after Delegation Holder Authorisation (able to "Red Card")	Comments
	level of Safety.			Management System and Risk Assessments) Project will consult potential MOD Regulators (Naval Authorities & Ordnance, Munitions & Explosives Safety Review Panel) and approval authorities under Stakeholder and Subject Matter Expert review.	
System Acceptance	To demonstrate that System meets all Safety elements of User Requirements Document and System Requirements Document	As above		Equipment Capability Customer	Safety Case Report for System Acceptance
User Trials (where necessary)	To demonstrate that specific User Trials can be conducted with adequate and known level of Safety.	As above		Trials Authorities acting for Equipment User	
Safety Submission for Individual Hazard or Group of Hazards	To demonstrate for the System of interest that specific Hazards are managed in accordance with MOD Policy.	As above	Some Naval Authorities Ordnance, Munitions & Explosives Safety Review Panel/ Military Laser Safety Committee	Some Naval Authorities	Subset of System Safety Case relevant to a specific Hazard or Group of Hazards. The Ordnance, Munitions & Explosives Safety Review Panel and some Naval Authorities cannot “Red Card” Safety Case and prevent entry to service.
Introduction to Service (release to service) / Major Change (whole system)	To demonstrate that complete System is Safe for Use within defined limits and necessary support	As above	Some Naval Authorities Ordnance, Munitions & Explosives Safety Review Panel/Military	Release to Service Authorities or Nuclear Regulator Platform authority. Some Naval Authorities	The Ordnance, Munitions & Explosives Safety Review Panel and some Naval Authorities

Stage in Project	Safety Case Report Purpose	Authorise by Project Member with Formally-Delegated Safety Responsibilities	Endorse After Delegation Holder Authorisation (not able to "Red Card")	Approval of Activity after Delegation Holder Authorisation (able to "Red Card")	Comments
	elements (Including Disposal Strategy are in place to sustain Safe Operation through life.		Laser Safety Committee		cannot “Red Card” Safety Case and prevent entry to service. Platform authority may prevent System from being integrated onto his Platform, but not from entry to Service.
Disposal (where necessary)	To validate Disposal Strategy for “Out of Service”	As above		None	May be “Permissioning” Regulator for Nuclear systems.

12.8. Version Control

12.8.1. Version 2.3 to 3.0 Uplift

12.8.1.1.

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

12.8.2. Version 3.0 to 3.1 Uplift

12.8.2.1.

A minor update to correct spelling, grammar errors and hyperlinks

12.8.3. Version 3.1 to 4.0 Uplift

12.8.3.1.

Major reorganisation of all SMPs:

- Restructure into a consistent format.
- Responsibilities, Alignment with Environment and guidance for different acquisition strategies have been removed and included in the POSMS summary.
- All further guidance has been placed into the Procedure section, and duplicated text has been removed
- An Annex A for 'Typical content of a Safety Case Report' previously found in Further Guidance
- An Annex B for 'Safety Cases during the project lifecycle' previously found in Further Giudance

12.8.4. Version 4.0 to 4.1 Uplift

12.8.4.1.

Minor text changes to align with ASP taxonomy.

Links
[1] https://www.asems.mod.uk/ExtReferences
[2] https://www.asems.mod.uk/guidance/posms/smp01
[3] https://www.asems.mod.uk/guidance/posms/smp02
[4] https://www.asems.mod.uk/guidance/posms/smp03
[5] https://www.asems.mod.uk/guidance/posms/smp04
[6] https://www.asems.mod.uk/guidance/posms/smp05
[7] https://www.asems.mod.uk/guidance/posms/smp06
[8] https://www.asems.mod.uk/guidance/posms/smp07
[9] https://www.asems.mod.uk/guidance/posms/smp08
[10] https://www.asems.mod.uk/guidance/posms/smp09

[11] https://www.asems.mod.uk/sites/default/files/documents/SMP/smp12-g-02.pdf
[12] https://www.asems.mod.uk/guidance/posms/smp10
[13] https://www.asems.mod.uk/guidance/posms/smp11