

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 1

<b>0</b>	<b>SHOWING CONFORMANCE</b>
<b>0.1</b>	<b>Options</b>
0.1.1	<p>There are four options to demonstrate conformance when applying this system procedure:</p> <ol style="list-style-type: none"> <li>a. Follow the defined system procedure using the recommended guidance and tools, including allowed variations and options.</li> <li>b. Use an equivalent process and tool set generated elsewhere and document evidence of procedural equivalence.</li> <li>c. Use a bespoke process and tool set for the project and document how the bespoke procedure achieves the objectives defined for this system procedure.</li> <li>d. Where the procedure is considered to be not relevant, document the basis for this decision.</li> </ol>
<b>1</b>	<b>INTRODUCTION</b>
1.1.1	<p>A <b>Safety Case</b> is defined in Def Stan 00-56 Issue 4 as:</p> <p>“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.”</p>
1.1.2	<p>A <b>Safety Case Report</b> is defined in Def Stan 00-56 Issue 4 as:</p> <p>“A report that summarises the arguments and evidence of the Safety Case, and documents progress against the Safety Programme.”</p>
1.1.3	<p>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.</p>
1.1.4	<p>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 SMS supporting it in service.</p>
1.1.5	<p>The Safety Case will bring together all the 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 to SMP09.</p>

Issue	Authorised by CESO DE&S	ISSUE LEVEL:	Release V2.2s
Approval	Authorised by DG S&E	DATE:	November 2007
DOCUMENT IS UNCONTROLLED IN PRINT			

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 2

1.1.6 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 will ensure that important Safety information is recognised as such, and preserved in a traceable way.

1.1.7 The Safety Case provides the mechanism for Safety submissions to many MOD authorities providing Safety approvals (eg Safety Certificates) or acting as internal MOD Safety Regulators in specific areas (eg. Naval Authorities for Key Hazards). It is vital that IPTLs identify the approvals that will be required for their Project and plan how to provide the necessary information in a timely manner.

## **1.2 Safety Case Report Review and Sign-off**

1.2.1 When a Safety Case Report is generated, it must 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)

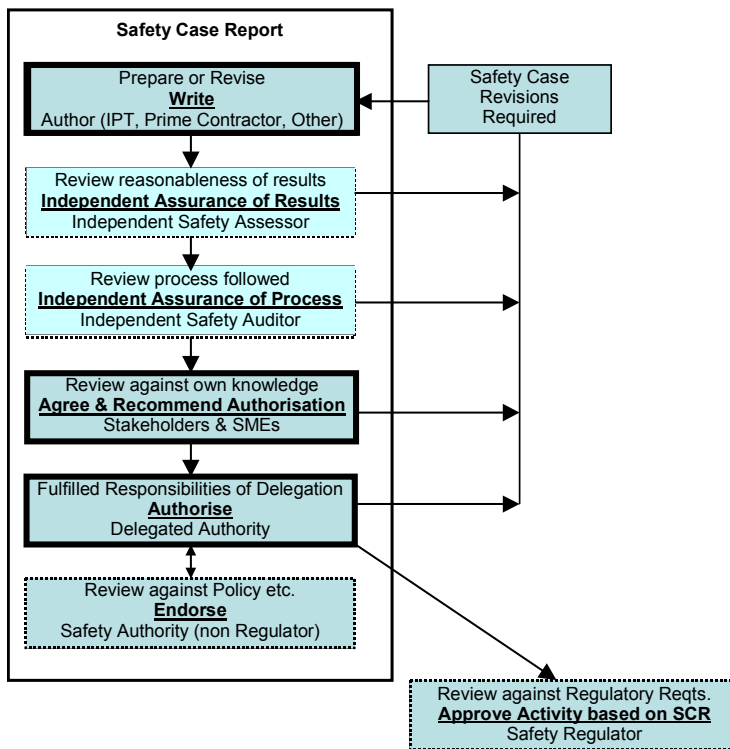
To assert that a document may be issued and that it reflects the individual’s acceptance of responsibility.

Assurance

Adequate confidence and evidence, through due process, that safety requirements have been met. [Def Stan 00-56 Issue 4]

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

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007



- 1.2.3 Boxes that are shown dotted and pale blue do not occur in every situation. Endorsement by Independent Safety Auditors and Assessors is required as defined in Domain-specific JSPs. Non-regulatory Safety Authorities are only involved where a Project is relevant to their Policy. Boxes with bold, solid borders show activities which are mandatory for every document approval cycle.
- 1.2.4 The order of review by ISA(s) and the Stakeholders may be different from that shown and may occur in parallel.
- 1.2.5 The approvals process will also change at different stages of the life cycle, depending on the purpose of the Safety Case Report (see **Guidance Sheet SMP12/G/02 - 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 IPT Leader. Safety Regulators should also be involved early, to indicate to the IPT Leader whether the Safety Case approach is likely to result in Approval of the activity.
- 1.2.6 Where a body has a “red card” and can prevent an Activity from happening, they are referred to as a “Safety Regulator”. Where they have no “red card” they are shown as a “Safety Authority (non Regulator)”. Approval of an activity may be through issuing an explicit approval statement or through statement of “no objection”.
- 1.2.7 It should be recognised that the same terms are used differently in other documents (eg “Endorsement” of Safety Case Reports by the Duty Holder is specified in JSP430).

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 4

1.2.8 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, should be subjected to this process.

## **2 PROCEDURE OBJECTIVES**

2.1.1 The purpose of the Safety Case is:

- a. to document evidence that the Safety Requirements are being met, and that all identified risks are tolerable and ALARP;
- b. to demonstrate that any activities underway at that time (including tests or trials) can be carried out safely;
- c. 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.
- d. for systems requiring Safety approval outside the IPT (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.

2.1.2 The Safety Case Report is the means by which the IPT Leader 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 4.2 of this Procedure.

## **3 RESPONSIBILITIES**

### **3.1 Accountability**

3.1.1 The IPTL is accountable for the completion of this procedure.

### **3.2 Procedure Management**

3.2.1 The IPTL may delegate the management of this procedure to a member (Safety Manager) or members of the IPT.

### **3.3 Procedure Completion**

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

3.3.2 Where different contractors are in competition with each other and have carried out separate Hazard Analyses, contractual and managerial arrangements should be made

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 5

for the output from all to be made available to the successful contractor. This will reduce the likelihood of hazards being missed.

3.3.3 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 Contractor's control, are captured and managed through the Hazard Log.

**4 WHEN**

**4.1 Initiation of Safety Case**

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

**4.2 Production of Safety Case Reports**

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

- a. Approval of the project Business Case at Initial Gate;
- b. Approval of the project Business Case at Main Gate;
- c. Clearance to begin Demonstration trials;
- d. Completion of the major aspects of design, (design baseline defined);
- e. Commitment to production;
- f. Clearance to begin testing/acceptance/User trials;
- g. Introduction to Service
- h. Significant changes to the design or material state (eg mid-life update);
- i. Significant changes in operational usage;
- j. Disposal.

4.2.2 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.

**4.3 Approval of Safety Case Reports**

4.3.1 When a Safety Case Report is issued to support a key project milestone, it should be reviewed by the Project Safety Committee including the ISA, if appointed, and agreed

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 6

by them if they are satisfied that it fairly represents the current Safety status for the Project. Their observations and recommendations should be included as part of the Safety Case Report which will then be presented to the IPTL for authorisation.

#### **4.4 Acceptance and Endorsement of Safety Case by Regulators and Certification/Approval Authorities**

4.4.1 The Project SMP 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. Examples of those who may be involved in reviewing Safety submissions and providing Safety approvals (or similar), include:

- a. OME Safety Review Panel;
- b. Naval Authorities (for Ship Key Hazards);
- c. Military Laser Safety Committee;
- d. JATE;
- e. Authorities for Platforms or systems onto which the equipment will be fitted (including for Trials);
- f. Authorities for Facilities or sites where the equipment will be used, stored etc;
- g. Authorities responsible for Safe transportation.

4.4.2 It is important for the IPTL to recognise the difference between authorities providing Safety advice and 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 responsibility for Safety from the IPTL to the advisor, Regulator or approving authority.

#### **4.5 Periodic Review of the Safety Case**

4.5.1 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 SMP.

### **5 REQUIRED INPUTS**

- 5.1.1 This procedure for the Safety Case and Safety Case Report requires inputs from:
- a. Outputs from Procedure SMP01 – Safety Initiation;
  - b. Outputs from Procedure SMP02 – Safety Committee;
  - c. Outputs from Procedure SMP03 – Safety Planning;
  - d. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis;

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 7

- e. Outputs from Procedure SMP05 –Hazard Identification and Analysis;
  - f. Outputs from Procedure SMP06 –Risk Estimation;
  - g. Outputs from Procedure SMP07 –Risk and ALARP Evaluation;
  - h. Outputs from Procedure SMP08 –Risk Reduction;
  - i. Outputs from Procedure SMP09 –Risk Acceptance;
  - j. Outputs from Procedure SMP10 –Safety Requirements and Contracts;
  - k. Outputs from Procedure SMP11 –Hazard Log.
- 5.1.2 The Safety Case body of information will include outputs from all the Safety Management activities conducted on a Project. In particular, it will include:
- a. Safety Plans;
  - b. Disposal Plans;
  - c. Hazard Log;
  - d. Register of Legislation and other significant Requirements;
  - e. Minutes of PSC meetings;
  - f. Safety Reports (eg. Hazard Identification, Hazard Analysis, Risk Estimation, Risk Evaluation);
  - g. Safety Assessment or Safety Case Reports for particular aspects of the system or activities associated with the system (eg Software Safety Case, Disposal Safety Assessment);
  - h. Safety Requirements;
  - i. Records of Design Reviews and Safety Reviews;
  - j. Results of Tests and Trials;
  - k. Incident reports and records of their investigation and resolution;
  - l. Safety Audit Plans;
  - m. Safety Audit Reports;
  - n. Records of Safety advice received;
  - o. Results of Safety inspections;
  - p. Records of Safety approvals (eg Certificates);

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 8

- q. Minimum Equipment List (ie vital to Safe operation);
- r. Emergency and Contingency Plans/Arrangements;
- s. Limitations on Safe Use;
- t. Master Data and Assumptions List;
- u. Evidence of compliance with Legislation and Standards;
- v. Evidence of adequacy of tools and methods used.

## **6 REQUIRED OUTPUTS**

- 6.1.1 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.
- 6.1.2 The physical outputs of the Safety Case are the Safety Case Reports. These are the means by which the IPT Leader 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.

## **7 DESCRIPTION**

### **7.1 Arrangements for Production of Safety Case Documentation**

- 7.1.1 The Project SMP must:
  - a. Identify the person responsible for overseeing the production of the safety documentation.
  - b. Define the process for approval of the safety documentation, both within and external to the IPT.
  - c. Describe the arrangements in place to:
    - i. prepare, review and assess safety documentation pertaining to design, construction, manufacture, operation and disposal/decommissioning,
    - ii. show how safety documentation is categorised in accordance with its safety significance,
    - iii. have such documentation produced by Suitably Qualified and Experienced Persons,
    - iv. have the documents approved at the appropriate level and reviewed at appropriate intervals.
    - v. where necessary, have the document reviewed by independent, Suitably Qualified and Experienced Persons,
    - vi. where necessary, submit documents to Safety Regulator(s) and/or

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

approval Authorities external to the IPT;

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

## **7.2 Necessary Evidence in the Safety Case**

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

- a. 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.
- b. The set of Safety Requirements is valid, ie they have been derived by thorough analysis of appropriate specifications and artifacts, and that they correspond to the system as designed and implemented.
- c. That the assessment undertaken is appropriate to the equipment and level of risk identified.
- d. Derived Safety Requirements are traceable to and from their source,
- e. Derived Safety Requirements are sufficient to meet Safety Requirements from which they are derived.
- f. The Safety Management System has been implemented as defined.
- g. The staff undertaking key roles with defined responsibilities had the appropriate competencies for those roles.
- h. All applicable legislation, regulations, Standards and MOD policy have been complied with.
- i. All contractual safety requirements have been met.

## **7.3 Development Through the Life cycle**

7.3.1 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 PSP as part of the continuous management process.

7.3.2 During system development, Safety Case Reports 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.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

- 7.3.3 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 **Guidance Sheet SMP12/G/02 - Safety Cases during the Project Life Cycle**):
- At Main Gate setting out the issues to be dealt with and the strategy to be followed to achieve the requirements.
  - 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.
  - 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).
  - Prior to production – to confirm that productionisation has not reduced the level of Safety performance achieved during the design stages.
  - Prior to Introduction to Service – to confirm that all necessary prerequisites (eg facilities) and management arrangements (eg training courses, logistic support) are in place to maintain the predicted level of Safety performance throughout the in-service phase.

#### **7.4 Ownership and Administration**

- 7.4.1 Irrespective of contractual arrangements, IPT Leaders have a special responsibility for delivering capability and managing most forms of risk. The IPT Leader is thus 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 SMS associated with Design Authority, including oversight and compilation of all safety justifications.
- 7.4.2 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.
- 7.4.3 Responsibility for the production or maintenance of the Safety Case may change over the system life, but the IPT Leader 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 IPT Leader.
- 7.4.4 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.
- 7.4.5 The Contractor cannot produce a Safety Case in isolation. Significant input from the

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 11

	<p>IPT, Users and other organizations where appropriate, will be required, particularly in relation to operational safety. The Contractor should work closely with the IPT Leader to ensure that all parties are aware of the scope of their involvement and that they deliver what is expected from them.</p>
7.4.6	<p>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 IPT Leader, how and when the Safety Case will be delivered should be clearly defined and agreed.</p>
<b>7.5</b>	<b>Approval and Authorisation within the IPT</b>
7.5.1	<p>Authorisation of a Safety Case Report by the IPT Leader indicates their satisfaction with the progress of the Safety Case and their acceptance of the safety risks associated with the project. The Authorised SCR forms an auditable record.</p>
7.5.2	<p>Before Authorisation, the IPT Leader must ensure the satisfactory resolution of any deficiencies or observations raised by their advisors, including the PSC and ISA (if appointed).</p>
<b>7.6</b>	<b>Endorsement by Authorities Responsible for Regulation, Certification and/or Approval</b>
7.6.1	<p>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.</p>
<b>7.7</b>	<b>Review of the Safety Case</b>
7.7.1	<p>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.</p>
7.7.2	<p>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.</p>

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 12

## **8 RECORDS AND PROJECT DOCUMENTATION**

- 8.1.1 Where relevant, the outputs from this procedure should feed into the following:
- a. SRD (System Requirements Document) – for any specific Safety requirements;
  - b. CSA (Customer Supplier Agreement) – to document agreements on Safety information to be delivered by the IPT;
  - c. TLMP (Through Life Management Plan);
  - d. Safety elements of Initial Gate and Main Gate submissions.
- 8.1.2 Records of all management assessments, processes and procedures, including all decisions on mitigation and the acceptability of suitable alternatives will be held for each project within the project's Safety Case.
- 8.1.3 The Safety Case will normally be held by the IPT Safety Manager, and maintained by them as up-to-date.
- 8.1.4 The Safety Case documentation should 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.
- 8.1.5 The Hazard Log (see Procedure SMP11 – Hazard Log) is a key part of the Safety Case.
- 8.1.6 A Safety Case Report provides 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 should be structured around the safety claims for the system and the planned activities. A Safety Case Report should provide justifiable confidence that the Safety Case is, or will be, adequate and that the expected progress is being made on planned activities.
- 8.1.7 The contents of the Safety Case Report will vary according to the maturity of the Safety Case and the intended readership. It has two functions: firstly, to assure the IPT Leader 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 should provide information that will support operational decision-making, such as a decision to operate outside the design envelope

## **9 RECOMMENDED TOOLS**

- 9.1.1 **Guidance Sheet SMP12/G/01** (Typical Content of a Safety Case Report) of this Procedure contains an example format for a Safety Case Report, it should be adapted to suit the project characteristics or phase of the programme to which it relates.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 13

## **10 GUIDANCE**

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

### **10.2 Extent of the Safety Case**

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

10.2.2 The extent of any Safety Case can only be decided after a preliminary, top-down Safety Assessment has been undertaken (see Procedure SMP04 – Preliminary Hazard Analysis). 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.

10.2.3 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.

10.2.4 The IPT Leader must 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 IPT Leader 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 should also be submitted to address these shortcomings. Where these issues prove difficult to resolve, the IPT Leader or ISA (if appointed) may approach the relevant FSMO for advice and to facilitate arbitration.

### **10.3 Depth of the Safety Case Report**

10.3.1 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 IPT Leader 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.

### **10.4 Scope of Safety Claims**

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 14

10.4.1 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 must therefore do more than show that all identified Risks have been made ALARP.

## **10.5 Rigour of Safety Case Argument**

10.5.1 The nature of the argument for safety will vary according to the complexity and type of system under scrutiny, and hence the rigor of argument offered will reflect the nature of the system. The Safety Case can be regarded as being a single, coherent argument for safety, but 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 rigor that will be required in the arguments offered, a safety integrity requirement for the system should be agreed between the IPT Leader, the Contractor (where relevant) and any regulatory or approval authorities.

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

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

## **10.6 Review of Safety Case Reports by the Project Team and Panel**

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

- a. Approval of the project Business Case at Initial Gate;
- b. Approval of the project Business Case at Main Gate;
- c. Clearance to begin Demonstration trials;
- d. Completion of the major aspects of design, (design baseline agreed);
- e. Commitment to production;

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

- f. Clearance to begin testing/acceptance/User trials;
- g. Introduction to Service;
- h. Significant changes to the design or material state (eg mid-life update);
- i. Significant changes in operational usage;
- j. Disposal.

10.6.2 Authorisation of the Safety Case Report signifies that the IPT Leader has taken best and competent advice and that all identified risks have been addressed. Prior to the SCR's authorisation, any risks that cannot be reduced to ALARP, should be recorded in the Hazard Log as uncompleted actions and included in the PSP and Safety Case Report for corrective action in the next phase. All PSC members should agree the interfaces and responsibilities for such outstanding actions defined within the Safety Plan. Where risks cannot be mitigated further, IPT Leaders should either seek a judgement on military ALARP, or additional resource from a Senior Manager, who in turn may notify the Functional Safety Board, of concerns regarding resource shortfalls.

### **10.7 Review and Approval of Assumptions**

10.7.1 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 (eg trials results), but the strength of the Safety Claims depends on the realism and credibility of these assumptions.

10.7.2 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.

### **10.8 Justification of Assessment Processes**

10.8.1 The robustness of the Safety Case is 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 should be demonstrated in the Safety Case as being adequate.

### **10.9 Retention of Safety Information**

10.9.1 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

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

latest information available to the FSMOs is that specific legal requirements for keeping records are for:

- a. 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;
- b. exposure to biological agents for ten years after any incident;
- c. health surveillance records on ionising radiation for fifty years after any incident;
- d. compartment air monitoring for exposure to hazardous substances must be kept for forty years after the incident;
- e. personnel breathing apparatus records (including compressed gases) are to be kept for forty years after any incident;
- f. general work place monitoring, test or maintenance records of control equipment to be kept for five years after any incident;
- g. respiratory protective equipment records for two years after any incident;
- h. personal accident records (medical) for three years after any incident;
- i. 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;
- j. monitoring and documentation retention of nuclear plant safety and munitions disposal are specified by the Naval Authority;
- k. 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.

10.9.2 Departmental SMSs 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.

### **10.10 Disclosure of Safety Information**

10.10.1 The Public Interests Disclosure Act permits the exemption of MOD establishments and operational training areas from disclosing sensitive information. However the SofS 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.

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

10.10.2 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.

### **10.11 Hierarchy of Safety Cases**

10.11.1 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.

10.11.2 If the equipment is part of a larger system (eg integrated onto a Platform or arranged in a “system of systems”), then the Delegated Authority responsible for the higher level system must 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) and will be covered by the system acceptance process.

### **10.12 Safety Case(s) for Options**

10.12.1 Where an IPT is considering more than one option for a given capability, a generic Safety Case must be initiated pre Initial Gate which must 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.

### **10.13 Safety Cases for Systems with Variants etc**

10.13.1 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.

### **10.14 Safety Case Caveats and their Removal**

10.14.1 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 (eg trials, training and in-service usage), the Delegated Authority must carefully consider how this information shortfall can be addressed.

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

- a. How are the caveats or limitations on usage to be promulgated to those who need to know?
- b. How is compliance with the caveats or limitations to be enforced?
- c. Do the caveats or limitations introduce additional Hazards or increase the Risks associated with any known Hazards?

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 18

d. If there are multiple caveats or limitations, might they interact in some way that degrades Safety?

10.14.3 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.

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

**10.15 Use of Existing Safety Information**

10.15.1 In some instances, the IPTL may base the Safety Case on data that already exist; for example from civilian certification authorities or other Nations' approval regimes. If these data are to well-known standards, the IPTL may decide to provide justification, in the Safety Case, as to why he is content to dispense with or reduce the scope of other safety analyses and independent tests and trials.

10.15.2 The value that may be attached to data about previous experience and use of the system should be discussed with the IPT Leader and any certification authority involved. For such data, the Contractor should demonstrate its applicability to the updated system.

**10.16 Retrospective Application**

10.16.1 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 is to be undertaken. A Safety Appraisal is aimed at ensuring that all the hazards presented by a piece of equipment or a system are understood and that adequate measures are in place to manage those hazards.

10.16.2 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, will 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.

10.16.3 Where legacy equipments are being subjected to a Safety Appraisal, the output of the Appraisal will be a Safety Case Report. The assessment should 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 eg accident and defect records, as well as anecdotal evidence. It should 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.

10.16.4 The extent of the work required will depend upon the age and condition of the

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 19

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.

**10.17 What if the Safety Case Concludes that the System is not Safe Enough ?**

10.17.1 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 must identify the areas of shortfall and provide a clear conclusion that the system is not considered to be adequately safe.

10.17.2 The Safety Case Report should 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).

10.17.3 It should be recognised that it is a valid outcome for the Safety Case to conclude that the system is not safe enough. 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.

10.17.4 If specific risks are identified and evaluated as being “Unacceptable” even after the application of all practicable risk reduction measures, then details of this must be raised up to 2\* level within the TLB for discussion and resolution at 2\* level with Equipment User (see SMP09 – Risk Acceptance). Agreement in writing must 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 (eg the over-riding military necessity under particular conditions).

**10.18 Safety Case as Good Practice**

10.18.1 The Safety Case concept is considered best-practice because:-

- a. 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;
- b. almost all highly complex industries, particularly those involving hazardous processes are now regulated through a Safety Case;
- c. common law considers written evidence (safety justifications) to have more weight than verbal testimony, making a written SMS, prioritised by a Safety Assessment, essential for the discharge of legal obligations;
- d. 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;
- e. information developed within system specific Safety Cases can be developed and reused for similar system types, facilitating feed-back of lessons learnt and

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

economies of scale;

- f. Safety Cases, efficient SMSs and a robust Safety Culture reduce whole life costs, facilitating better change management, business improvement, improved morale and efficiency by reducing accidents;
- g. 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.

### **10.19 Review and Revision of Safety Case and Re-Issue of Safety Case Report**

10.19.1 Where a change to the system is an equipment/capability change that is not covered by the existing Safety Case, the Case is to be revised with a description of the change and the evidence for Safety following the change. The Safety Case Report. Should be revised as follows:

- a. For major changes or changes with a large safety impact, as a complete re-issue of the previous Safety Case Report.
- b. For minor changes with little safety impact, as an annex to the previous Safety Case Report, providing a safety statement.

### **10.20 Domain-Specific Guidance and References**

10.20.1 Additional guidance on Project Safety Cases is contained in the following references:

- a. Land Systems: JSP 454 Issue 4:
  - i. Part 2 Section 6.3 – 6.8
  - ii. Part 2 Section 7.8
  - iii. Part 2 Annex C
- b. Ship Safety Management: (JSP 430 Issue 3):
  - i. When ships are built, refitted or maintained by shore-based personnel, SEMS are subject to land-based regulations. An IPT Leader should seek assurance from their contractor(s) that safety is properly managed at key events such as launching, dry-docking, during trials and re-commissioning. Documentary evidence should be provided that:-
    - the ship is safe to enter or re-enter service;
    - any new Hazards arising from eg maintenance activities, introduction of new systems/equipment or development of new configurations for existing systems have been incorporated into the Hazard Log;
    - Risk Management is in-place and highlighted within relevant Safety Case Reports.
  - ii. A Safety Case should be developed in accordance with the Policy when the system's application is within the maritime Functional Area. The

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 21

Safety Case must address and communicate the risks to third parties, be they other MOD personnel, the general public, facilities or the environment via a hazard footprint. It is for the third party IPT Leader to consider the information within any Hazard Footprint and mitigate risks to their own activities accordingly, in the same manner as the equipment IPT Leader relates to a system or ship IPT Leader.

iii. Second/third-party Duty Holders may seek to use this data in their own Safety Cases, flotilla/mission Safety Assessments or Operational Analysis.

c. Airworthiness: (JSP 553 1<sup>st</sup> Edition):

i. The Safety Case described in this JSP addresses airworthiness; other aspects of aviation safety will be covered by other safety cases.

ii. The Safety Case should be subjected to independent assessment, as described in Para 2.58.

iii. Safety Cases underpin each of the two release documents: the Military Aircraft Release (MA Release) and the Release to Service (RTS).

iv. Military Aircraft Release

v. The MA Release is, inter alia, the statement on behalf of CDM to the Project Sponsor that an acceptable Safety Case has been prepared for the aircraft or equipment. It includes or references the aircraft's limitations and description. The MA Release is described in detail in Para 4.12.

vi. The approval of the initial issue of the RTS to the RTSA needs to be conducted by the nominated DE&S 2\* (DAWS or DG Log(Strike)).

vii. Release to Service

viii. The RTS is the release document giving authority for Service regulated flying. The RTS is derived from the MA Release but includes extant SDs. It is based on a Safety Case covering the as-flown configuration of the aircraft. The RTS is described in detail in Para 5.5.

d. Ordnance, Munitions & Explosives (OME): (JSP 520 Issue 2.0):

i. IPTs responsible for acquisition programmes that include OME must develop a Safety Case that, in most cases, will form part of a larger system or platform Safety Case. It is to be initiated upon identification of a new OME related capability, and will evolve as the project develops.

ii. The OME Safety Case Report must be independently reviewed and endorsed by an OSRP which will be convened by DOSG. The level at which Review Panels will be chaired and OME Safety Case Reports reviewed shall be proportional to the OME safety risks involved.

iii. OME Safety Review Panel

iv. The OSRP will be independent of the IPT. Its Chairman, appointed by D DOSG, will have delegated authority to endorse the OME Safety Case

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

Report. Any significant safety concerns identified in the course of reviewing the OME Safety Case Reports which cannot be resolved within a reasonable timescale shall be referred to Director DOSG.

- v. The OME Safety Case Report must provide sufficient detail to satisfy the OME Safety Review Panel that residual risks are in the tolerable region and that the ALARP arguments are comprehensive, credible and robust, and where practicable that the system complies with relevant legislation and standards.
- vi. DOSB is required to monitor the clearance status of all OME systems. In support of this, DOSG will maintain an OME System Safety Clearance Register, and report any significant shortfalls.
- vii. At specified project milestones (see paragraph 0224) OME Safety Case Reports shall be submitted to the OSRP. All submissions of the OME Safety Case Report must include a submission statement and be sent to the Secretariat of the OSRP (Operating Procedure 2.2 refers). Where an Independent Safety Auditor is appointed by the IPT, all relevant conclusions drawn from audit reports shall be included in the OME Safety Case Report to provide support to safety arguments and declarations.
- viii. The periodicity of submission of the OME Safety Case Report to the OSRP should be proportional to the risks associated with the OME system, although as a minimum, submissions should align with major project milestones and the approvals process. In addition, submissions should be made when changes to the system or the environment have been made, which affect the intrinsic safety of the system. Chapter 4 provides guidance on what the OSRP will expect to see in OME Safety Case Report submissions throughout the life cycle. For projects which are not required to pass Initial and Main Gate (Category D projects and Urgent Operational Requirements for example), special arrangements should be made which must include endorsement of the OME Safety Case Report prior to Acceptance.
- ix. The OME Safety Case Report must be independently reviewed by an OSRP, which will be convened by DOSG. Submissions of the OME Safety Case Report should align with major project milestones, but as a minimum should be at Initial Gate, Main Gate, Acceptance to Service, Mid Life Update and changes to the design or environment which has a direct effect on the intrinsic safety of the OME system. The level at which Review Panels will be chaired shall be proportional to the Risk Level Category (see Operating Procedure 1.3). The outcome of a successful review will be endorsement, by the Chairman of the OSRP, in the form of a Certificate of Safety OME. The Panel may decide that caveats and provisos of use are appropriate, in which case the Chairman must ensure that they are clearly identified as part of the Certificate of Safety OME.

e. Nuclear Propulsion (JSP 518 Issue 2):

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007

<b>MOD</b>	<b>SMS Procedures</b>	Procedure SMP12
<b>SMP12: Safety Case and Safety Case Report</b>		Page 23

i. Chapter 3

ii. Annex A

### **10.21 Warnings and Potential Project Risks**

10.21.1 The warnings and potential Project Risks identified in all the other Procedures, from SMP01 to SMP11 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.

10.21.2 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 IPTL might authorise the release of the system for service use when it does not comply fully with the requirements of regulatory or approval authorities.

10.21.3 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.

10.21.4 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 (eg introduction to service).

10.21.5 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.

10.21.6 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.

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

DOCUMENT IS UNCONTROLLED IN PRINT	ISSUE LEVEL:	Release V2.2s
	DATE:	November 2007