Ministry of Defence

# Defence Standard 00-56 Part 1

**Issue 7** **Date: 28 February 2017**

# Safety Management Requirements for Defence Systems

## Part 1: Requirements

# Contents

# Foreword

## REVISION NOTE

This Defence Standard (Def Stan) Part 1 has been raised to Issue 7 to update its content. To reduce the impact of numerical and editorial changes to the requirements and its resulting impact on contract conditions, it has been agreed to retaining the contracting Clauses and Notes in Part 1 and move the guidance into Part 2. Acquisition staff should be aware that the changes to Def Stan numbering and this up-issues may have consequences on contracts referencing earlier issues.

## ISSUE 7 Update

There are a number of editorial changes in Part 1 that are grammatical or modified notes that will have no significant impact on current contracts. Domain Tailoring and Compliance Matrices detailed Part 2 of this Standard are mandated by the relevant Regulator. Changes to Part 2, Domain Tailoring and Compliance Matrices may contain significant amendments that may impact new contracts. Issues related to these changes should be addressed to the relevant Regulator.

## HISTORICAL RECORD

This Standard supersedes the following:

Defence Standard 00-56 Part 1 Issue 6 dated 02 Apr 2015

Defence Standard 00-56 Part 1 Issue 5 dated 29 January 2014

Defence Standard 00-56 Part 1 Issue 4 dated 01 June 2007

Defence Standard 00-56 Part 2 Issue 4 Amendment 1 dated 06 July 2012

Defence Standard 00-56 Part 3 Issue 1 dated 23 March 2012

a) Defence Standard 00-056, this Standard, provides Requirements (Part 1) and Guidance (Part 2) for the achievement, assurance and management of safety. It can be applied to any Ministry of Defence (MOD) project and in any phase of a project's life. Defence Contractors shall use this Standard as required by Contract. The effective application of this Standard requires close cooperation between all parties, as the responsibility for the achievement of safety is shared. This Standard also provides guidance for establishing a means of complying with the requirements for the management of safety. This Standard contains clauses that can be tailored by the MOD to meet safety requirements appropriate to the project.

b) This standard has been produced on behalf of the Ministry of Defence (MOD) by the Safety Standards Review Committee. This Standard is sponsored by Defence Equipment and Support (DE&S) Director Technical.

c) This Standard has been reached following broad consensus amongst the authorities concerned with its use and is intended to be used whenever relevant in all future designs, contracts, orders etc. and whenever practicable by amendment to those already in existence. If any difficulty arises which prevents application of this Standard, Defence Standardization (DStan) shall be informed so that a remedy may be sought.

d) Please address any enquiries regarding the use of this standard in relation to an invitation to tender or to a contract in which it is incorporated, to the responsible technical or supervising authority named in the invitation to tender or contract.

e) Compliance with this Standard shall not in itself relieve any person from any legal obligations imposed upon them.

f) This Standard has been devised solely for the use of the MOD and its contractors in the execution of contracts for the MOD. To the extent permitted by law, the MOD hereby excludes all liability whatsoever and howsoever arising (including, but without limitation, liability resulting from negligence) for any loss or damage however caused when the standard is used for any other purpose.

# 0 Introduction

**0.1** The Acquisition Systems Operating Model[1] includes requirements placed on Ministry of Defence (MOD) acquisition organisations by Commands and Strategic Programmes for the delivery of Equipment, Services, Logistics and Support (ESL&S) on behalf of Defence. The purpose of this Standard is to support acquisition organisations delivery of ESL&S by setting Safety Requirements on Contractors that enable procurement of Products, Services and/or Systems (PSS) that are compliant with safety legislation and regulations and with MOD safety and acquisition policy. The intent is that compliance with these requirements will place MOD in a position to discharge its obligations with regard to the management of Risk to Life associated with the in-service use of PSS.

**Note.** Abbreviations used in this Standard, eg PSS, are to be considered as singular or plural in context with their use in the text.

**0.1.1** PSS is used to describe all the articles or artefacts that are being delivered as defined in the Contract. The Standard is intended to capture a broad spectrum of deliverables eg:

a) Service. Access to a commercially owned, commercially operated satellite communications system or a maintenance contract for military vehicles.

b) Product. A vehicle, engine or its components.

c) System. Air traffic control facility with integrated radar and radio equipments.

**0.2** Under UK law, all employers have a duty of care to their employees, the general public and the wider environment. For the MOD this includes, but is not limited to, an obligation to manage the Risk to Life associated with operation of military systems. In accordance with general guidance provided by the Health and Safety Executive, and as defined in Defence Safety Authority (DSA) Regulatory publication DSA01.1, MOD will discharge this duty by ensuring that all identified risks to life are reduced to levels that are As Low As Reasonably Practicable (ALARP) and tolerable, unless legislation, regulations or MOD Policy imposes a more stringent standard.

**0.3** Contractors who supply PSS to the MOD are subject to legal duties, which may vary with the place of manufacture and supply or operation. MOD shall have regard to the needs of Contractors to discharge their legal duties when interpreting and applying the requirements of this Standard.

**0.4** The requirements are grouped into three main areas as follows:

a) **Safety Management.** Section 2. The requirements for organisational and general processes to ensure that Risk to Life is managed effectively.

b) **Safety Engineering.** Section 3. The requirements for guiding the design of a PSS so that it can be operated safely, on its own, as part of a wider system, or in a system of systems, and providing evidence that this has been done.

c) **Safety In-Service.** Section 4. The requirements for managing safety where a Contractor is supporting the MOD by providing a service, which may include operating a PSS.

**Notes:**

i. If the Contract does not include provision of services (by the Contractor) then the clause of paragraph 16 will not be applicable; similarly, if the Contract does not include support, then clauses in paragraph 15 will not be applicable.

ii. The clauses can be tailored at a more detailed level, depending on the scope of contract, standards or the approach to regulation in a particular sector. Guidance is given on tailoring in Part 2, but this is likely to be project dependent. Tailoring can be done only by the MOD, or as suggested by industry and with the agreement of the MOD; and must reflect the relevant domain Defence Safety Regulatory publication.

[1] Available from the Acquisition System Guidance website via the Internet Defence Gateway.

iii. This standard is not intended to be applied to consultancy contracts for Independent Safety Auditor (ISA) services or manpower substitution services.

iv. Throughout this Standard, unless otherwise specified, the data to be recorded or documented must be retained with the information set.

**0.5** This Standard is based upon a definition of safe, which addresses fatality, physical or psychological injury or damage to the health of people, including MOD employees and the general public; in this Standard we use the term Risk to Life in this sense. This Standard may be applied to address the damage to (or loss of) PSS, environmental damage elements, or the management of environmental issues where Risk to Life results.

**0.6** This Standard sets out requirements for achievement, assurance and management of safety, including overarching objectives and principles. Part 2 of this Standard provides guidance on establishing a means of compliance with the requirements.

**Note.** In contracts for PSS in the Air Domain, henceforth referred to as Defence Air Environment (DAE) as defined in the Military Aviation Authority (MAA) Glossary MAA02, the “should” term is the permissive verb to allow the contractor to consider an alternative approach in meeting the clause. Any alternative approach must be agreed with the MOD.

**0.6.1** Sections 2 to 4 expand on the specific requirements on a clause-by-clause basis.

**0.7** This Standard is applied to all PSS procured to meet diverse capabilities across all Defence systems and may necessitate tailoring. The MOD may tailor the application of clauses and sub-clauses of this Standard or, in consultation with the Contractor, agree tailoring.

**0.8** The scope of contract encompasses the scope of supply and scope of analysis. The scope of contract is the boundary of the safety activities of the Contract. It is negotiated during the early phases of a project where the scope of supply and the scope of analysis are determined.

**0.9** This Standard identifies requirements for the achievement and demonstration of safety by a Contractor who has Safety and Quality Management Systems in place.

# Safety Management Requirements for Defence Systems

# Part 1: Requirements

## Section 1 - General

### 1 Scope and Applicability

**1.1** This Standard specifies the requirements for achieving, assuring and managing the safety of PSS defined by the scope of contract.

**1.1.1** This Standard provides the Contractor with guidance for compliance with the requirements, thereby supporting the MOD in meeting their obligations with regard to the management of Risk to Life associated with the operation of military systems.

**1.1.2** This Standard considers that a product can be an engineering artefact, whether physical, Data or software, from the small scale, such as a pump or a digital map, to the large scale, such as a ship or a geographically distributed logistics application.

**1.1.3** This Standard considers that a system is a combination of elements, with defined boundaries, which are used together in a defined operating environment to perform a given task or achieve a specific purpose. These elements may include personnel, procedures, materials, tools, products, facilities, services and/or Data as appropriate.

**1.1.4** This Standard considers a Service to be any activity using a System, eg providing air-to-air refuelling, running a naval dockyard, or calculating the safe flight envelope for an aircraft, which are provided by the Contractor.

**1.2** The Contractor, together with the MOD, has responsibility for safety of all deliverable PSS. This Standard is intended to cover the full range of possibilities including:

a) Where the Contractor has visibility and understanding of in-service Risk to Life, and can design PSS taking operation into account.

b) Where the Contractor does not have visibility of in-service Risk to Life but is responsible for providing information to those who are responsible for in-service Risk to Life of the PSS.

**1.2.1** The MOD considers all Defence Lines of Development for PSS, but this may not be included in the scope of contract, eg Concepts and Doctrine would consider Risk to Life and would be a MOD responsibility.

**1.3** The responsibility of the Contractor also varies with the scope of analysis. This Standard is intended to cover the full range of possibilities including:

a) Enhanced, where the Contractor carries out safety engineering and safety management, for the duty holder, beyond the deliverable PSS.

b) Full, where the Contractor carries out safety engineering and safety management for the deliverable PSS.

c) Reduced, where the Contractor carries out safety engineering and safety management only for parts or aspects of the deliverable PSS, eg for maintenance of a product.

**1.3.1** The scope of analysis is intended to be adapted to the wide range of possible MOD acquisition scenarios.

**1.3.2** Guidance on MOD safety management is available through the ASG.

**1.4** Whilst Contract life may be limited, this Standard considers the whole life cycle of the PSS, including disposal. Various phases of the life of the PSS that need to be considered should be explicitly included within the scope of analysis. This applies to all in-service situations and scenarios including, but not limited to, trials, operations and training for operations as defined in the Contract.

**1.4.1** This Standard applies to all acquisition scenarios and all PSS but the responsibility of the Contractor varies with the scope of supply.

**1.4.2** The distinction between scope of supply and scope of analysis is intended to facilitate the clear definition of the Contractor's responsibilities.

**1.4.3** The scope of analysis may be extended beyond the scope of supply particularly where the contracted activity is limited to early phases of the CADMID/T cycle. The scope of analysis may need to cover the full CADMID/T cycle.

**1.5** This Standard applies to PSS that have identified duty holders, supported by Safety Committees and relevant stakeholders.

**1.5.1** For all PSS to which this Standard is applied, a crown servant will retain responsibility and accountability for the Risk to Life. The scope of contract is agreed between the MOD and the Contractor and would identify duty holders and relevant stakeholders who are responsible for managing safety of the PSS. The relevant stakeholders may include representatives from MOD and Industry (for other related PSS) that may impact the PSS safety interfaces.

**1.5.2** The mechanism for managing safety is through the agreed Safety Committees. Terms of Reference and membership will be specific to the scope of contract.

**Notes:**

i. This Standard is specifically about safety and there is expectation that requirements will be set by the MOD and be included in the project documentation, eg capability, performance and reliability criteria and User and System Requirements Documents (URD/SRD).

ii. This clause is an indicative commitment from the MOD to the Contractor and a limitation on the scope of this Standard. The Contractor must assume that the MOD has a Safety Management System (SMS) for their PSS responsibilities, eg a Safety Committee exists prior to Invitation to Tender (ITT). Agreeing a scope of contract is intended to clarify responsibilities between the MOD and the Contractor. As the PSS evolves through life the scope of contract may need to be revisited and may need to be re-negotiated.

iii. The interface and degree of support/co-operation between the MOD SMS and the Contractor's equivalent would form part of the MOD/Contractor agreed scope of contract. This Standard defines the requirements placed on the Contractor. For information on MOD processes and responsibilities, Contractors can refer to the MOD publications and procedures, eg Regulatory publications such as the Military Aviation Authority Regulatory Publications (DSRPs), which are available through the Defence Gateway or GOV.UK websites or the MOD Project-Oriented Safety Management System (POSMS) manual, which can be accessed from the MOD Acquisition Safety and Environmental Management Systems (ASEMS) website http://www.asems.mod.uk.

iv. One of the main mechanisms of the MOD SMS is managing safety through the relevant Safety Committees. The Contractor's Terms of Reference and membership of Safety Committees will be specific to the agreed scope of contract, and based on POSMS guidance.

vi. Where there is any doubt over the validity of assumptions, or the scope of analysis, the contractor must discuss resolution with the MOD.

## 2 Warning

The Ministry of Defence (MOD), like its contractors, is subject to both United Kingdom and European laws regarding Health and Safety at Work. Many Defence Standards set out processes and procedures that could be injurious to health if adequate precautions are not taken. Adherence to those processes and procedures in no way absolves users from complying with legal requirements relating to Health and Safety at Work.

# 3 References

## 3.1 Normative References

**3.1.1** The publications shown below are referred to in the text of this Standard. Publications are grouped and listed in alpha numeric order.

| | |
|---|---|
| DEF STAN 00-055 | Requirements for Safety of Programmable Elements (PE) in Defence Systems |
| DSA01.1 | Defence Policy for Health, Safety and Environmental Protection |
| ISO 9001 | Quality Management Systems - Requirements |
| JSP 440 | The Defence Manual of Security |

**Notes:**

i. Def Stan's can be downloaded free of charge from the DStan web site by visiting **<http://dstan.uwh.diif.r.mil.uk>** for those with RLI access or **<https://www.gov.uk/uk-defence-standardization>** for all other users. All referenced standards were correct at the time of publication of this standard (see 3.1.2, 3.1.3 & 3.1.4 below for further guidance), if you are having difficulty obtaining any referenced standard please contact the DStan Helpdesk in the first instance.

ii. In the Defence Safety Authority, the Regulators will deliver general and domain specific policy and guidance through Defence Safety Regulatory Publications (DSRP). These documents will be available through the http://www.gov.uk websites.

iii. In the DAE, the MAA Regulatory Publications (MRPs) define Air Safety Management Systems requirements through Regulatory Articles, https:/www.gov.uk/government/collections/maa-regulatory-publications. MRPs referenced Part 1 of this Standard are in the context of the DAE only. MRPs referenced in the DAE Tailoring and Compliance Matrix (Part 2) are to be considered in addition to the normative references.

iv. As many PSS will be procured from international sources, international standards have been referenced. National equivalents will be identical, eg BS ISO 26262.

**3.1.2** Reference in this Standard to any normative references means in any Invitation to Tender or contract the edition and all amendments current at the date of such tender or contract unless a specific edition is indicated. Care should be taken when referring out to specific portions of other standards to ensure that they remain easily identifiable where subsequent amendments and supersession's might be made. For some standards the most recent editions shall always apply due to safety and regulatory requirements.

**3.1.3** In consideration of clause 3.1.2 above, users shall be fully aware of the issue, amendment status and application of all normative references, particularly when forming part of an Invitation to Tender or contract. Correct application of standards is as defined in the ITT or contract.

**3.1.4** DStan can advise regarding where to obtain normative referenced documents. Requests for such information can be made to the DStan Helpdesk. Details of how to contact the helpdesk are shown on the outside rear cover of Defence Standards.

## 3.2 Other References

**3.2.1** Other references in this Standard are to recognised good practice, sources of additional guidance and context to provided notes.

| | |
|---|---|
| AERC | Airborne Equipment Release Certificate |
| ALWRC | Air Launched Weapon Release Certificate |
| ARP 4754 | Guidelines for Development of Civil Aircraft and Systems. |
| ASEMS | DE&S Acquisition Safety and Environmental Management System |
| Def Stan 05-057 | Configuration Management of Defence Materiel |
| Def Stan 05-135 | Avoidance of Counterfeit Materiel |
| Def Stan 05-138 | Cyber Security for Defence Suppliers |

| | |
|---|---|
| Def Stan 00-251 | Human Factors Integration for Defence Systems |
| IET Blue Book | Competence Criteria for Safety-Related System Practitioners |
| IET COPISA | Code of practice for independent safety assessors |
| ISO 26262 | Road Vehicles - Functional Safety |
| POSMS | DE&S Project Oriented Safety Management System |
| White Book | An Introduction to Safety Management in the MOD |

# 4 Definitions

## 4.1 Terms and Definitions

For the purposes of this Standard, the terms and definitions detailed in Annex A shall apply.

**Note.** MOD Regulatory publications, a Contractors' Safety Management System (SMS), this Standard and open standards may use definitions that are diverse. Where there is divergence, the Contractor will need to agree a glossary with the MOD which will need to be documented, eg in the Safety Management Plan (SMP).

## 4.2 Mandatory Requirements

A requirement which uses the word 'shall' identifies the clause or sub-clause as mandatory. Sub-clauses using the word 'should' allows the contractor the opportunity to consider an alternative approach in meeting the sub-clause. Any proposed alternative approach must be agreed with the MOD.

# 5 Abbreviations

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| ARP | Aerospace Recommended Practice, |
| ASG | Acquisition System Guidance |
| ASIC | Application-Specific Integrated Circuit |
| CADMID/T | Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal/Termination. |
| CONDO | Contractors on Deployed Operations |
| CSA | Contractor Safety Auditor |
| DAE | Defence Air Environment |
| Def Stan | Defence Standard |
| DID | Data Item Description |
| DO | Document Order |
| DSA | Defence Safety Authority |
| DStan | UK Defence Standardization |
| ESL&S | Equipment, Services, Logistics and Support |
| FMEA | Failure Modes and Effects Analysis |
| FMECA | Failure Modes Effects and Criticality Analysis |
| FPGA | Field-Programmable Gate Array |
| FRACAS | Failure Reporting Analysis and Corrective Actions Systems |
| GFX | Government Furnished Equipment (GFE) or Assets (GFA) |
| IET | Institution of Engineering and Technology |
| ISA | Independent Safety Auditor |
| ISAWG | Independent Safety Assurance Working Group |
| ISO | International Organization for Standardization |
| ISSS | Information Set Safety Summary |
| ITT | Invitation to Tender |
| JSP | Joint Service Publication |
| MIL-STD | Military Standard |

| | |
|---|---|
| MOD | Ministry of Defence |
| PE | Programmable Elements |
| PLD | Programmable Logic Device |
| POSMS | DE&S Project Oriented Safety Management System |
| PSS | Products, Services and Systems |
| SRD | System Requirement Document |
| SMP | Safety Management Plan |
| SMS | Safety Management System |
| URD | User Requirement Document |

This Page is Intentionally Blank

# Section 2 - Safety Management Requirements

## 6 Safety Management System

The Contractor shall operate an SMS that defines the framework for the Contractor's organisation to direct, control and monitor its safety management activities.

**Notes:**

i. Safety Culture and SMSs are very important to the achievement and assurance of safety. This Standard mandates an SMS, but does not place requirements on safety culture as that cannot be enforced through contract. MOD guidance on safety management and safety engineering such as the Project Oriented Safety Management System (POSMS) and An Introduction to Safety Management in the MOD (White Book) are available via the http://www.asems.mod.uk website.

ii. Regulatory Article (RA) RA1200 and the Manual of Air Safety provide detail on how an SMS is to be implemented In the DAE.

### 6.1 Safety Management Plan

The Contractor shall define and implement a coherent approach to management of all safety-relevant activities, throughout the life of the Contract and document their approach in an SMP.

**6.1.1** The Contractor shall identify civil, open or other standards, or good practice, where they are used in full or partial fulfilment of the requirements of this Standard, and document the means by which any differences to this Standard will be resolved.

**6.1.2** The Contractor should show that use of civil, open or other standards or good practice is appropriate for their Contract.

**6.1.3** The Contractor should analyse the civil, open or other standards or good practice which they intend to apply to the contract; identify the divergences with this Standard; applicable regulations and legislation; and document the results of the analysis and their proposed means of resolving the divergences between them in the SMP.

**6.1.4** The Contractor should ensure that the SMP covers all safety-relevant activities to a level of detail that is reasonably practicable, so as to determine what activities are to be performed, by whom, at what time, and with what methods and tools, throughout the Contract.

**6.1.5** The Contractor should ensure that the SMP covers the work of all Sub-Contractors, including the mechanisms that the Contractor will use for oversight of Sub-Contractor work, such as auditing.

**6.1.6** Where the Contract includes provision of a service the Contractor should agree with the MOD the balance between the activities managed through the service SMP and through other relevant plans, drawing on the service SMP as the key plan for the safety aspects of the delivery, prior to commencement of the service.

**6.1.7** Where the Contractor has an SMS in place, the SMP should draw on that system.

**6.1.8** Where the Contractor does not have an SMS in place, the SMP should address the core principles of systems engineering and safety management.

**Notes:**

i. It is mandatory for Contractors to operate an SMS. In exceptional circumstances, MOD may work with some specialist Contractors who do not have an SMS. These requirements, identified in the scope of contract, will be reflected in the scope of supply or scope of analysis for the specific project or as directed by the MOD Regulators. Information on the MOD's Acquisition Safety and Environmental Management Systems is available from the ASG. The White Book and the ASG contains guidance on acquisition safety management in a systems engineering context.

ii. The SMP defines the safety-relevant activities to be undertaken, and these are agreed with the MOD before they are performed. Where services are provided on the Contract, there may be additional plans which govern these activities. The reporting is intended to give visibility to the Safety Committee and to other stakeholders of the progress of the safety relevant activities, and to identify issues which need management attention, as and when they arise.

iii. The MOD encourages the use of open, civil standards where possible, eg ARP 4754/DO-178 in an air application, or ISO 26262 in an automotive application. Further guidance is provided on Contracting, Tailoring and Open Standards Adoption in Part 2 of this Standard.

iv. A Data Item Description (DID) for the SMP is provided in the DID Annex in Part 2 of this Standard.

v. The MOD mandates that acquisition projects must have an SMS. The intent is that the Contractor also operates an SMS. This requirement may be tailored by the MOD, depending on the project requirements.

## 6.2 Agreement

The Contractor shall agree the SMP with the MOD.

**6.2.1** The Contractor should define an SMP as part of the tendering process, and formalise and agree the plan with the MOD at Contract award.

**Notes:**

i. Part 2 to this Standard gives some guidance on contracting, tailoring, tendering and other pre-contract activities.

ii. The detail in a draft SMP might not be complete at the ITT stage, for example because the tenderer may not have been able to identify all Sub-Contractors, or because they have not been able to assess Government Furnished Equipment or Assets (GFX). As a consequence there may be substantive work to be undertaken in formalising the SMP during Contract negotiations and from Contract award. The SMP must be agreed with the MOD before any extensive safety work is undertaken.

## 6.3 Review and Update

The Contractor shall review and update the SMP to reflect changes throughout the life of the Contract.

**6.3.1** The Contractor should review the SMP on a regular basis, depending on the scale and stage of the Contract or on significant events, eg change in supplier, introduction of a new technology or changes to risk mitigation strategy, and agree the SMP changes with the MOD before implementation.

**6.3.2** When the Contract includes support, the Contractor should ensure that all changes in design and their implementation are managed through the SMP, or in subsidiary plans, together with mechanisms for safe and effective distribution and installation of those changes.

## 6.4 Progress Reports

The Contractor shall report progress against the SMP to all stakeholders as identified in the SMP, and shall report on any necessary actions to correct deviations from the SMP.

**6.4.1** The Contractor should ensure that Progress Reports highlight significant safety issues and proposed remedial actions, as well as documenting progress against planned tasks.

**Note.** The DID for the Progress Report is provided in the DID Annex in Part 2 of this Standard.

# 7 General Requirements

**Note.** The general requirements deal with the broad legislative and contractual context for the core safety management and safety engineering activities covered in this Standard. In several cases, eg deviation from requirements, the requirements act as constraints on other parts of the Standard, or on the application of the Standard.

## 7.1 Deviation from Requirements

Any deviations from the requirements of this Standard shall be formally agreed between the MOD and the Contractor prior to their implementation, and documented in the SMP.

**7.1.1** Where there are conflicts between the requirements of this Standard and other requirements, a means of resolving the conflicts shall be agreed between the MOD and the Contractor.

**7.1.2** In the response to an ITT, the tenderer should specify how they intend to meet the requirements of this Standard.

**7.1.3** The tenderer should provide a compliance matrix for this Standard with their response to the ITT, showing:

a) Which clauses will be or have been fully complied with.

b) Which clauses will not be or have not been fully complied with, and why, including a description of any alternative approaches and why they are acceptable.

**7.1.4** For any intended deviations, the tenderer should indicate how their approach will meet the intent of this Standard or explain why compliance is not considered to be necessary.

**Notes:**

i. The domain tailoring and compliance matrices may provide specific requirements for a means of resolving the conflicts. However, there must be an agreed solution in the scope of contract.

ii. At Contract award, the relevant tailoring and compliance matrix will form part of the scope of contract and hence future variance will need to be agreed by the MOD and Contractor and may result in contract amendment.

iii. The ITT may identify tailoring of the Standard as required by the MOD. Agreement to further removal or replacement of specific requirements of this Standard depends on the Contractor showing that there is no adverse impact on the safety, or on the evidence of the safety of the PSS and agreed by the MOD, eg during Contract negotiation.

iv. Part 2 of this Standard includes tailoring principles and contracting guidance and provides a clause-by-clause tailoring and compliance matrix templates.

## 7.2 Legislation, Regulations, Standards and Policy

The Contractor shall identify and document all relevant safety legislation, regulations and standards applicable to the PSS delivery.

**7.2.1** The Contractor shall work with the MOD to identify and agree relevant MOD policy appropriate to the scope of supply and scope of analysis, addressing the domain and the technology used.

**7.2.2** The Contractor should agree with the MOD, all legislation, regulations and standards applicable to the scope of supply and scope of analysis, addressing the domain and the technology used.

**Notes:**

i. Legislation and standards will be documented in a legislation register which is fundamental to any SMS, eg the MOD POSMS Project Safety Initiation procedures identifies a legislative register as an integral part of the Safety Case. Legislation, regulations and standards risks to delivery of PSS will be managed through safety engineering.

ii. The Contractor has responsibility for identifying relevant UK/EU and International legislation, and this will be dependent on the Contractor's chosen solution, eg where the legislation is technology related, the MOD will expect the Contractor to be fully aware of their obligations to deliver compliant PSS.

iii. The MOD complies with all applicable Health Safety and Environmental Protection legislation within the United Kingdom (UK) and overseas applies MOD's UK arrangements where reasonably practicable and, in addition, responds to host nations' relevant Health Safety and Environmental Protection expectations. MOD guidance on application of legislation is delivered through JSPs and Regulatory Publications which the Contractor may not be aware of. However there is a requirement on the Contractor to obtain agreement on compliance, exemption or disapplication, dependent on the applicable legislation for their chosen solution, eg where materials may be subject to European Union Directives restricting manufacture or import.

iv. It is recognised that the contractor is unlikely to be able to apply MOD policy directly. However, it is likely that the Contractor will be able to work with the MOD in addressing such policy through derived requirements.

## 7.3 Sub-Contracting

Where work is Sub-Contracted, the Contractor shall ensure and provide assurance that the relevant requirements of this Standard are met throughout the supply chain.

**7.3.1** The Contractor should identify their requirements to Sub-Contractors, appropriate to the Contractor's scope of supply and scope of analysis.

**7.3.2** The Contractor should place requirements on Sub-Contractors to ensure that the Contractor's compliance to the relevant requirements of the Standard are met.

**7.3.3** The Contractor should identify deliverables and audit mechanisms to provide assurance that the requirements of the Standard are met throughout the supply chain, and record the evidence to demonstrate compliance in the information set.

**Notes:**

i. Many of the requirements of this Standard relate to the relationship between the MOD and the Contractor. It is the Contractor's responsibility to meet the requirements of this Standard.

ii. This Standard has requirements for managing interfaces that must be addressed at the boundary with Sub-Contractors. This may lead to involving Sub-Contractors in the top-level Safety Committee, or setting up special working groups, rather than key stakeholders becoming involved in the Sub-Contractor's Safety Committee.

## 7.4 Multiple Deliverables

Where there are multiple deliverable PSS, the Contractor shall apply the clauses of this Standard relevant to each PSS element, grouping common PSS elements where appropriate, and document the approach adopted in the SMP.

**7.4.1** The Contractor and the MOD should discuss and agree where it is necessary to apply specific requirements of the Standard across each deliverable PSS.

**7.4.2** Safety Case Reports and Information Set Safety Summaries (ISSSs) should be produced for each related PSS so that they are "self-contained" from a safety perspective.

**Notes:**

i. These clauses are intended to address the situations where the Contractor is asked to produce a variety of different PSS types, eg a fleet of different vehicle types, or supports product trials or demonstrations which are services, in the terms of this Standard. The aim is to make the analysis and safety assessments specific enough to control risk effectively for each of the elements of the PSS without repeating work which is essentially identical for each of the elements.

ii. In the case of services interfacing to other PSS, as part of the Contract, there may be a need for separate Safety Cases Reports for each interfacing PSS. For example, a demonstration may necessitate some additional hazard analysis and safety analysis.

iii. In the DAE, only the Air System Safety Case is recognised as a Safety Case. It is supported by a number of Safety Assessments (defined in MAA02). Where the Contractor is required to supply Safety Cases, Safety Cases Reports, in the DAE they are referred to as Safety Assessments and Safety Assessment Reports unless specifically referring to the Air System Safety Case.

iv. Guidance on the concept, use and applicability of the Safety Case Report and ISSS are provided in Part 2 to this Standard and their relevant DIDs provided in the DID Annex.

## 7.5 Information Management

The Contractor shall provide the MOD with visibility of the safety engineering, support and safety management activities throughout the life of the Contract.

**7.5.1** The Contractor shall define and agree with MOD an information set which is sufficient to enable all safety relevant design and safety analysis activities to be reviewed and repeated.

**7.5.2** The Contractor shall ensure that the information set is kept up to date as the design and analysis evolves, and that it is managed in a suitable configuration management framework. (eg Def Stan 05-057).

**7.5.3** The Contractor shall maintain consistency between the information set and the configuration of deliverable PSS.

**7.5.4** The Contractor shall preserve the information set for the period or periods specified in the Contract.

**7.5.5** The Contractor shall ensure that the information set remains accessible as techniques, methodologies and tools change, through the life of the Contract.

**7.5.6** The Contractor shall pass information to the MOD, Regulators and any other organisations identified in the Contract, where that information is necessary for other parties to be able to fulfil their safety responsibilities with regard to the deliverable PSS, or interfacing or interacting PSS.

**7.5.7** The Contractor should seek to be inclusive in defining the information set, to ensure that data and information that might have a safety role are included.

**7.5.8** The Contractor should define, and agree with the MOD, processes for information management, including periodic review of media, compatibility with current tools (both specialist and general purpose) and devise means of migrating data as appropriate to ensure that it remains both accessible and usable.

**7.5.9** Where the Contractor anticipates difficulties, or very high costs, in preserving access to parts of the information set they should discuss approaches and options with the MOD.

**7.5.10** The Contractor should consider obsolescence of the technologies used for preserving the information set.

**Notes:**

i. Information set refers to data that Contractors would necessarily produce when developing and analysing PSS. The term information set is a label for what would be normally produced, not a new imposition. Not all data generated will be a deliverable, but must be retained where it provides evidence to

support the specific safety case. It is unlikely that there will be a single document forming the information set. Instead the information set will typically include documents, databases, spread sheets, etc. The scope of supply defines what is deliverable from the information set.

ii. Contractors will need to ensure that the information set is manageable, and that there is no unjustifiable burden in maintaining this information for extended periods. Technology changes due to obsolescence may make continued information accessibility infeasible, or prohibitively expensive, and the Contractor will need to be consult with the MOD about the cost-benefit trades.

iii. It must be assumed that an Independent Safety Auditor (ISA), if appointed, would need access data from the information set used as evidence to substantiate the Safety Case.

## 7.6 Documentary Deliverables

The Contractor shall produce documentary deliverables relevant to safety, including interim versions, as Contracted. Documentary deliverables identified in this Standard are:

a) Command Summary.
b) Information Set Safety Summary.
c) Safety Audit Plan.
d) Safety Audit Report.
e) Safety Case Report.
f) Hazard Log Report.
g) Safety Management Plan.
h) Progress Reports.

**7.6.1** The Contractor shall agree with the MOD the format and content for all Contracted safety-related deliverables in the scope of supply and document this information in the SMP.

**7.6.2** The Contractor should define deliverable formatting and content taking into account the DIDs and the requirements of any civil, open or other standards being used, as identified in the SMP.

**7.6.3** The Contractor should develop and update the deliverable plans, reports and summaries at appropriate stages of the Contract as defined in the SMP.

**Notes:**

i. DIDs for deliverables are provided in the DID Annex in Part 2 of this Standard and are intended to identify scope and content of the deliverables, not the contents list. They also give guidance on the "life-cycle" of the deliverables.

ii. The Release To Service RAs, RA1300, RA1345 and RA1350, must not be subverted by a Command Summary. In the provision of services a Command Summary may be appropriate, however great care should be taken in all other circumstances on invoking this clause.

## 7.7 Agreement of Deliverables

The Contractor shall agree with the MOD, the PSS and safety-related documentation to be delivered and record this information in the SMP.

**7.7.1** The Contractor should define the boundaries and operating environment including any known interfacing or interacting PSS, whether extant or planned.

**7.7.2** The Contractor should define the PSS to include all relevant elements across the Defence Lines of Development, as Contracted.

**7.7.3** The Contractor should record the definition of the PSS, and the results of activities within the scope of analysis, in the information set and update it throughout the Contract to ensure that it accurately reflects the status of the design, safety analysis and engineering activities.

**Note.** Although this Standard includes DIDs, it is anticipated that the definition of deliverable contents and format will be a key part of the SMP; it is likely to depend to a significant degree on the Regulatory Publications applicable to the Contract.

# 8 Roles and Responsibilities

## 8.1 Safety Organisation

The Contractor shall define the roles and responsibilities of those individuals responsible for safety within the scope of contract and document them in the SMP.

**8.1.1** The Contractor shall identify the normal point of contact for safety matters within the safety organisation.

**8.1.2** The Contractor shall demonstrate how responsibility is delegated to ensure safety is treated with appropriate authority within the organisation and on the Contract.

**8.1.3** The Contractor should keep the definition of roles and responsibilities of those individuals responsible for safety up to date.

**8.1.4** The Contractor should identify and record, in the information set, competency requirements for each role.

**Notes:**

i. In practice, responsibilities will be shared between MOD and Industry and the Safety Committee is the primary mechanisms to ensure coordination and interfaces with other organisations and stakeholders.

ii. A clear definition of roles and responsibilities within the MOD and Contractors organisation is essential to ensure that safety issues are owned at an appropriate management level. Sufficient authority must be delegated within the Contractors organisation to ensure that safety management is given the appropriate priority and resources that are commensurate with the risk.

iii. POSMS, Project Safety Initiation procedures, suggest methodology to ensure that the safety management process is commenced on a firm basis by identifying basic information, interfaces and responsibilities. This may include use of a Responsible, Accountable, Consulted and Informed chart, or equivalent, which would be recorded in the SMP and updated through the PSS lifecycle.

## 8.2 Safety Committees

The Contractor shall contribute to Safety Committees and other liaison activities to ensure effective coordination of safety with the MOD and other stakeholders.

**8.2.1** The Contractor shall provide visibility of the information set to the Safety Committee to enable it to oversee safety management, safety engineering and safety-related support activities.

**8.2.2** The Contractor shall support the Safety Committee in recommending, endorsing or providing guidance on issues with a potential safety impact and in assuring the results of work, within the scope of analysis, either directly or through subsidiary committees.

**8.2.3** The Contractor shall support the Safety Committee in any additional roles/tasks as agreed with the MOD and recorded in the SMP.

**8.2.4** Where there is an MOD Safety Committee, the Contractor should participate in its work.

**8.2.5** Where there is no appropriate committee, the Contractor should work with the MOD to establish a Safety Committee that includes relevant stakeholders and define the constitution and Terms of Reference in the SMP.

**8.2.6** Where appropriate the Safety Committee should delegate work to subsidiary committees or working groups, and document the policy on delegation of responsibility and escalation of issues in the SMP. These sub-committees may be largely staffed by Contractor personnel.

**8.2.7** Where there is concurrent work on interfacing or interacting PSS, the Safety Committee should collaborate with other Safety Committees to manage interfaces, and should refine the scope of analysis if necessary to minimise gaps in analysis, or overlaps and duplication of effort.

**8.2.8** Where the Contract involves support, the Safety Committee should approve proposed changes to all PSS before they are implemented and ensure the proposed changes comply with domain regulatory requirements.

**8.2.9** The Contractor should record all their support to the Safety Committee and safety-related meetings.

**Notes:**

i. Management of safety is a collaborative activity between the MOD and its Contractors. In the case of Defence projects, the Contractor will normally have extensive knowledge about engineering and means of controlling risk, which is complemented by the MOD's in-service knowledge of operations, other interacting PSS, and the acceptability of risk. The Contractor's and the MOD's knowledge need to be brought together to enable effective management of safety, and the Safety Committee is the primary mechanism for doing this. To be effective, the Safety Committee must have an open and co-operative approach to all aspects of managing safety; this is indicative of a positive safety culture.

ii. Normally the MOD will have already established a Safety Committee and the obligations on the Contractor will be discharged through engagement in the Safety Committee. In the unlikely situation that there is no established MOD Safety Committee, the Contractor must liaise with the MOD to establish such a committee.

iii. The MOD expects the Contractor will keep records of their contribution and support safety-related meetings, in line with statutory requirements and for audit purposes. The Contractor's responsibilities may also include producing formal records of Safety Committee meetings.

iv. The mandatory (shall) requirements are on the Contractor. Where the "should" clauses refer to the Safety Committee, the Contractor is expected to support the work of the Safety Committee as agreed through the tailoring and compliance matrix and defined in the Contract.

## 8.3 Contractor Safety Audit Independence

The Contractor shall ensure that Contractor Safety Auditors (CSAs) are independent from those areas within the Contractor's organisation, or any Sub-Contractors, that are subject to Contractor safety audit.

**Note.** Good practice for CSAs may be taken from the IET Code of Practice for Independent Safety Assessors (COPISA), eg be sufficiently independent that any commercial, financial or other interests do not compromise their ability to carry out the assessment or their judgements.

## 8.4 Competencies

The Contractor shall ensure that all safety-relevant tasks within their scope of contract are carried out and managed by individuals, teams or organisations that are competent to perform those tasks.

**8.4.1** The Contractor should record the evidence of competence, on an individual, team and organisational basis, in the information set.

**8.4.2** The Contractor should undertake competence management, for all project staff, drawing on publicly available competence frameworks, where possible.

**8.4.3** Contractors should ensure that competent personnel are appointed to all posts that affect safety and confirm details in the relevant section of the SMP and in the Safety Case.

**Notes:**

i. The notion of competency also extends to organisations. In some cases there is an explicit scheme of organisational assessment, eg in the Defence Air Environment (DAE) there are multiple approval schemes including Maintenance Approved Organization Scheme and the Design Approved Organization Scheme. The presence, or otherwise, of such assessments of organisational competence does not alter the requirements of this Standard, but the evidence produced to achieve approval may be used to provide material which is an acceptable means of compliance.

ii. There are schemes for assessing safety competency relevant to particular standards. Examples of safety practitioner competence schemes are: Managing Competence for Safety-Related Practitioners (developed by the Health and Safety Executive (HSE), the Institution of Electrical Engineers and the British Computer Society) and the Competence Criteria for Safety-Related System Practitioners (IET's Blue Book). The MOD also provides guidance on MOD safety-related competence through the ASG. The ASG contains the Acquisition Safety and Environmental Management System Safety and Environmental Protection Leaflets, eg Duty Holder and Role Profiles. Contractors will have their own schemes based on these or similar publications. Whichever scheme is used it is expected that the Contractor will provide sufficient evidence of competence of personnel undertaking tasks to meet contracted Safety requirements.

# 9 Interfaces

**Note.** The Standard applies on a Contract and it is likely that multiple Contracts will need to be placed to deliver a capability for the MOD; this clause deals with the interfaces with other Contractors and with government organisations where they are involved in the provision of parts of the capability.

## 9.1 Organisational Interfaces

The Contractor shall cooperate, and coordinate safety activities, with all relevant organisations identified in the SMP.

**9.1.1** The Contractor should define processes for managing organisational interfaces, eg to suppliers or to operators of peer PSS, and document them in the SMP. These processes should cover the full scope of contract.

**9.1.2** The Contractor should ensure timely and accurate communication with all relevant organisations identified in the SMP and participate in relevant Safety Committees to ensure coordination of safety management and engineering activities.

**Note.** There may be an urgent need for timely communication between stakeholders, eg to manage an emergent risk that impacts in-service safety.

## 9.2 Technical Interfaces

The Contractor shall record, as part of the information set, all assumptions and information necessary to enable safe integration or interoperation with other PSS, including in a system of systems.

**9.2.1** The Contractor shall identify and record, as part of the information set, their assumptions about any known interfacing or interacting PSS, whether extant or planned, to enable them to carry out safety-related activities within the scope of contract.

**9.2.2** The Contractor shall record, as part of the information set, assumptions which other organisations are entitled to make about their deliverable PSS.

**9.2.3** The Contractor should define and manage the technical interfaces to each element which can be operated in a system of systems.

**Notes:**

i. The aim is to ensure that the configuration of the elements is not constrained by the way in which they have been defined and analysed, eg by considering only a single possible configuration, thereby maximising the extent to which they can be deployed with confidence that the safety issues have been properly understood.

ii. The intent is that the documentation of assumptions enables the Contractor responsible for one PSS to say what properties they can achieve and assure, given the assumptions they can legitimately make about interacting or interfacing systems. Such a scheme will not be infallible, and there is a limit to the extent to which Contractors can anticipate usage, but the aim is to limit the risk of unsafe emergent properties, without imposing an excessive burden on Contractors.

iii. Management of interfaces is important to safety as hazards can be initiated at technical interfaces, and because misunderstandings can occur at aligned technical and organisational interfaces, especially where several Contractor's PSS are brought together to form a system of systems.

iv. Where interfaces are at the boundary of the PSS produced by a Contractor (or at the boundary of the Scope of Analysis) then information needs to be provided for other stakeholders, eg the users of the PSS, or system integrators. Another stakeholder will need to know what they can assume, or rely on, about an interface in order that they can meet their Safety Requirements, or to provide guarantees to others. The assumptions might be physical or to do with information, for example: maximum electromagnetic field strength; materials used for connectors or latency in Data provided.

v. The information on assumptions must always be included in the ISSS. A DID for the ISSS provided in the DID Annex in Part 2 of this Standard.

vi. This Standard identifies the need for Safety Case Reports and ISSSs for each PSS supplied. These reports and/or summaries would include the assumptions as necessary to demonstrate safety, or to provide information to enable safe assembly of a system of systems.

### 9.3 External Interacting Interfaces

The Contractor shall assess information provided by the MOD or other Contractors for interacting PSS and take steps to resolve any inconsistencies in the assumptions made at interfaces, in discussion with the MOD if necessary.

**9.3.1** The Contractor should seek to reconcile assumptions made at boundaries with other PSS to ensure safe operation of the whole, recognising that changes may need to be made in PSS still under development, to cater for limitations of other system elements.

**Notes:**

i. The focus is on what is known about interacting PSS, where there may be limited opportunity to redesign.

ii. Information provided about interfacing or interacting products may need to be analysed, and therefore must be defined in the scope of analysis. This clause deals with the case where analysis identifies incompatibilities between assumptions, or difficulties in meeting Safety Requirements, given all that can be assumed about interacting PSS.

iii. Changes to resolve incompatibilities will need to be agreed with the MOD as they may go beyond the boundary of the Contractor's responsibility. Also, these responsibilities apply at any level in the system hierarchy, but are particularly onerous for top-level system integrators, and for those assembling System of Systems. The ASG provides guidance on systems integration.

## 10 Safety Audits

**Note.** These clauses cover both audit by the Contractor, and enabling Independent Safety Audit. Extensive guidance on Independent Safety Audits is available through the ASG. ISAs are appointed by the MOD, not by the Contractor and guidance on the ASG supports management of expectations. The focus here is on Contractor safety audits although there is no intent in using that term to imply that the Contractor

cannot employ a third party to carry out audits on their behalf. The intent of Contractor safety audits is to show that the Contractor has implemented the SMP, as defined, or to identify remedial action in the case of deviations. This would give a baseline for the ISA who can then take a more wide-reaching role, including assessing the appropriateness of the SMP.

## 10.1 Audits and Reports

The Contractor shall carry out safety audits as specified in the SMP, to assure the implementation of the SMP.

**10.1.1** A Safety Audit Report shall be produced, following each safety audit, which fully describes the findings of the safety audit.

**10.1.2** All audit findings should be assessed for significance and the need for remedial action identified.

**10.1.3** The Contractor should ensure that all Sub-Contract activity is audited.

**Notes:**

i. The Contractor may audit Sub-Contractors themselves, or rely on third parties, or assess the results of the Sub-Contractors internal audit. The mechanism is not material; what is important is that the audit extends throughout the whole supply chain.

ii. It may be helpful for the CSA to make recommendations on remedial action to the Contractor and, where appropriate, the MOD.

## 10.2 Independent Safety Audit

The Contractor shall allow an Independent Safety Auditor, if one is appointed, reasonable access to the information set.

**10.2.1** Where restrictions on access to elements of the information set, required for safety audit, are unavoidable, eg foreign export controls, the Contractor should identify and communicate them to the MOD at the earliest opportunity.

**Note.** The intent here is that the Contractor work with the ISA and MOD to overcome access obstacles. Common approaches include the establishment of Non-Disclosure Agreements.

## 10.3 Remedial Action

The Contractor shall identify and implement timely remedial actions to rectify any agreed non-conformities or other issues found in safety audits.

**10.3.1** The Contractor should agree the remedial actions with the MOD through the Safety Committee, and any other relevant stakeholders, as appropriate.

**10.3.2** The Contractor should update the SMP, if appropriate, to reflect the agreed remedial actions.

**Notes:**

i. It is important to agree changes with the Safety Committee and other relevant stakeholders, to ensure that the most effective and efficient route is found.

ii. Some judgment is required as to what nature and scale of remedial action needs to be incorporated into the SMP, and how that must be done. If the audit shows that the PSS is inadequate, and a major redesign is required, then the impact will go beyond the SMP.

This Page is Intentionally Blank

## Section 3 - Safety Engineering

**Notes:**

i. The intent of the Standard is that safety engineering can be undertaken for PSS, but that knowledge of the broader context is needed if full hazard analysis is to be undertaken for a product. In general, this would be specified in the scope of analysis.

ii. The Standard covers both the analysis of new (developmental) and pre-existing PSS.

# 11 Safety Requirements, Hazard and Risk Analysis

## 11.1 Safety Requirements

The Contractor shall clearly identify, record and track Safety Requirements throughout the Contract.

**11.1.1** The Contractor shall document the process for identifying, recording and tracking Safety Requirements in the SMP.

**11.1.2** The Contractor shall identify and record Derived Safety Requirements resulting from MOD policy, regulations and standards appropriate to the scope of supply and scope of analysis, addressing the domain and the technology used, relevant to the Contract.

**11.1.3** The Contractor shall identify and record all Derived Safety Requirements arising from safety engineering and safety analysis activities.

**11.1.4** The Contractor shall identify and record Safety Requirements to ensure Design Integrity.

**11.1.5** The Contractor should identify and record all Safety Requirements, including Top Level Safety Requirements, in the information set.

**11.1.6** The Contractor should identify and record all Derived Safety Requirements needed to ensure control of risks associated with hazards, and potential risks associated with identified failure modes whether they are to mitigate the effects of the hazards or failure modes, or to make them less likely to occur.

**11.1.7** The Contractor should identify and record Derived Safety Requirements on properties of the PSS, where necessary to manage risk.

**11.1.8** The Contractor should identify and record Derived Safety Requirements on processes, eg to show independence of elements of the PSS, where necessary to manage risk.

**Notes:**

i. Safety engineering activities may influence the design resulting in decisions that generate Derived Safety Requirements. Other system engineering activities may also result in a design decisions which generate Derived Safety Requirements.

ii. Design Integrity is a generic term, intended to cover mechanical components as well complex electronics. This Standard does not impose an integrity scheme as the intent is to use civil, open or other standards so far as possible. Guidance on addressing the Design Integrity of Programmable Elements (PEs), eg software and its data, contained in complex electronics is provided in Def Stan 00-055. Further guidance on Integrity is provided in the Integrity and Open Standards Annex in Part 2 of this Standard.

iii. Top Level Safety Requirements are normally imposed by the MOD on the Contractor, eg URD/SRD. However, relevant standards, policy and legislation may change during the Contract life, requiring revision of the Top Level Safety Requirements.

iv. Derived Safety Requirements are drawn from policy, etc. as often the MOD's policies will be set out in general terms, and interpretation will be needed to produce requirements specific to the PSS in the scope

of supply. Derived Safety Requirements, included in the SMP, must be met using recognised procedures and it is important that they are recorded for traceability.

v. There may be cases where compliance with regulations and standards, eg for CE marking, a declaration of compliance with new approach and global approach standards, is sufficient to meet Safety Requirements. If the Contractor believes this to be the case then this must be documented in the SMP (ideally at ITT stage) for agreement by the MOD. If this is the case, then many of the detailed safety engineering requirements may not apply.

vi. Data Safety Requirements are a subset of PE Safety Requirements which, during the systems engineering and safety assessment activities, may emerge as Derived Safety Requirements where PE contributes to a hazard or impairs mitigation of a hazard.

## 11.2 Safety Requirements Management

The Contractor shall maintain records to show traceability between each Safety Requirement, the source of the requirements including safety analysis and mitigation for hazards or potential accidents.

**11.2.1** The Contractor should record the evidence which shows that each Safety Requirement (including Derived Safety Requirements) has been validated as being correct and complete in the information set.

**11.2.2** The Contractor should record the evidence which shows that each Safety Requirement (including Derived Safety Requirements) has been met, or documents any shortfall in the information set.

**11.2.3** The Contractor should record the evidence such that it can be included in, or referenced from, the Hazard Log.

**Note.** Traceability is fundamental, without it, it is not possible to understand how the results of low level activities contribute to demonstrating satisfaction of requirements. If traceability is lost then this can seriously undermine the validity of the Hazard Log, and hence the Safety Case for a PSS. Traceability is bi-directional (top-down and bottom-up).

## 11.3 Hazards and Accidents

The Contractor shall identify all hazards and associated potential accidents, from all credible causes, within the scope of analysis.

**11.3.1** The Contractor should employ systematic analysis processes for identification of hazards and accidents as defined in the SMP.

**11.3.2** The Contractor should ensure that human factors are considered where they may be a contributory cause of a hazard.

**11.3.3** The Contractor should ensure that cyber security is considered where security breaches may be a contributory cause of a hazard.

**11.3.4** The Contractor should ensure that systematic and random failures are considered where they may be a contributory cause of a hazard.

**11.3.5** The Contractor should ensure that the undesired impact of normal functions is considered; this is especially important for Contractors carrying out systems integration.

**Notes:**

i. There are established approaches to hazard analysis. Further guidance on techniques is available on the ASG.

ii. Def Stan 00-251 provides requirements and guidance for the achievement, assurance and management of Human Factors Integration.

iii. JSP 440 provides policy and guidance for security.

vi. Def Stan 05-138 provides requirements and guidance for the levels of cyber protection required to be achieved by Defence Suppliers.

v. Counterfeit materials may contribute to a hazard. It is expected that the Contractor will have a policy for the avoidance of counterfeit materials. Def Stan 05-135 defines the arrangements that a supplier is required to establish to demonstrate that they are actively planning and managing the risk of counterfeit materiel in their supply chain to prevent delivery of such materiel to the MOD.

vi. Def Stan 00-055 is concerned with the overall behaviour of Programmable Elements (PE) including cases where the use of PE and Data may contribute to a hazard or impair mitigation of a hazard at the system level.

## 11.4 Hazard Tracking

The Contractor shall ensure that the status of the control of all hazards is visible throughout the Contract.

**11.4.1** The Contractor shall implement a Hazard Log.

**11.4.2** The Contractor shall ensure that Hazard Log Reports are delivered as defined in the SMP.

**11.4.3** The Contractor should update the Hazard Log throughout the Contract to ensure that it accurately reflects the status of the design, hazard analysis, safety analysis and safety engineering activities.

**Notes:**

i. Guidance on the management of a Hazard Log is available through the ASG.

ii. The DID for a generic Hazard Log Report is provided in the DID Annex in Part 2 of this Standard.

iii. Some civil, open or other standards do not include use of a Hazard Log; in this case agreement will need to be reached with the MOD whether or not the intent of the Standard is met by other Military or civil standards, or to consider tailoring this clause. If such tailoring is not agreed, then the Contractor will be expected to supply a Hazard Log in addition to meeting the requirements of the agreed standards.

## 11.5 Design for Safety

The Contractor shall undertake the design of the PSS so as to meet all Safety Requirements.

**11.5.1** The Contractor shall identify mitigation strategies to minimise safety risk and meet Safety Requirements.

**11.5.2** The Contractor shall select and implement a combination of mitigation strategies for hazards or failure modes that contribute to a hazard, according to the following precedence:

a) Elimination.

b) Reduce the Risk to Life by engineering means.

c) Reduce the Risk to Life by means based on human factors, incorporating requirements from Def Stan 00-251, as appropriate.

**11.5.3** The Contractor shall demonstrate the effectiveness of the process for identifying and selecting mitigation strategies, and shall record the rationale, including the application of the ALARP principle, for the selection of each mitigation strategy in the information set.

**11.5.4** The Contractor shall manage identified mitigation strategies through Derived Safety Requirements, taking into account design decisions and any potential shortfalls in meeting Top Level Safety Requirements.

**11.5.5** The Contractor should identify Derived Safety Requirements which represent the partitioning and allocation of Safety Requirements to parts of the PSS.

**11.5.6** Where there are identified shortfalls, the Contractor should meet the mitigating Derived Safety Requirements where practicable, enabling any identified shortfalls to be eliminated or where elimination is not possible, reduced so far as is reasonably practicable.

**11.5.7** Where the shortfall does not directly impact safety, eg a non-conformance with an agreed process standard, the Contractor should use engineering judgement to identify the most appropriate mitigation strategies and agree them with the Safety Committee.

**11.5.8** The Contractor should record the results of applying the mitigation strategies and ALARP, the evidence that Safety Requirements are met, and any residual shortfalls against Safety Requirements in the information set.

**Notes:**

i. References informing designing for safety, based around the use of Derived Safety Requirements and links between the safety activities and other systems engineering activities, are available through the ASG.

ii. The Top Level Safety Requirements and Derived Safety Requirements will be linked, and traceability will be established between them, and between the requirements, design or safety activities from which they arise. In general, low-level requirements will either expand on the higher-level requirements, or deal with Contractor controlled decisions, design and analysis.

iii. The ultimate responsibility for accepting and operating a system lies with the MOD. The decision to deploy a System can be made only by a duty holder who has considered the Risk to Life ALARP. Contractors must apply ALARP principles through generating and satisfying Derived Safety Requirements, applying mitigation strategies and possibly using Cost-Benefit Analysis to justify decisions.

iv. In the DAE, the aviation Duty Holder or Accountable Manager (Military Flying) are the designated posts who can accept risks as being tolerable and ALARP

## 11.6 Safety Analysis

The Contractor shall carry out, using processes as defined in the SMP, safety analysis to identify how failures or defects in the design might contribute to hazards or accidents.

**11.6.1** The Contractor shall ensure that safety analysis covers all technologies, applicable to the PSS, and is carried out through the design decomposition to a sufficient level of detail to address all credible causes of hazards, accidents or failure modes that contribute to a hazard or accident.

**11.6.2** The Contractor should use the results of the safety analysis to identify Derived Safety Requirements.

**11.6.3** The Contractor should document the results of the safety analysis in the information set.

**11.6.4** The Contractor should ensure that the safety analysis results remain consistent with the design.

**Note.** Safety analysis can be started in the Concept phase but must be started before the design is mature in order to help guide the design by establishing Derived Safety Requirements, eg for one component to detect and mitigate the failure of another. The safety analysis may discover sufficiently serious flaws in the design, eg a single point of failure to a life-threatening hazard that it will also lead to a re-design. Where there is re-design the safety analysis will need to be repeated or updated to remain consistent with the design.

## 11.7 Failure Modes

The Contractor shall identify potential failure modes, from all credible causes, which might contribute to a hazard in the PSS, or in any known interfacing or interacting PSS, whether extant or planned.

**11.7.1** The Contractor shall ensure that the status of control of all identified failure modes that contribute to a hazard is visible throughout the Contract.

**11.7.2** The Contractor shall include, in the information set, information about the identified failure modes.

**11.7.3** The Contractor shall include in the ISSS, information on the status of identified failure modes.

**11.7.4** The Contractor shall estimate the likelihood of occurrence and opportunities for mitigation for all identified failure modes that contribute to a hazard and record the results in the information set.

**11.7.5** The Contractor should employ systematic safety analysis processes for identification of failure modes which might contribute to a hazard in the PSS as defined in the SMP.

**11.7.6** The Contractor should ensure that human factors are considered where they may be a contributory cause of a failure mode.

**11.7.7** The Contractor should ensure that cyber security is considered where security breaches may be a contributory cause of a failure mode.

**11.7.8** The Contractor should ensure that systematic failures are considered where they may be a contributory cause of a failure mode.

**11.7.9** The Contractor should ensure that the undesired impacts of normal functions are considered; this is especially important for Contractors carrying out systems integration.

**11.7.10** The Contractor should update information on identified failure modes throughout the Contract to ensure that it accurately reflects the status of the design, safety analysis and safety engineering activities.

**11.7.11** The Contractor should use qualitative estimates where it is not practicable to quantify likelihood.

**11.7.12** The Contractor should identify potential mitigations for the failure modes that contribute to a hazard where this is practicable; in particular they should identify any observable attributes of the PSS which could be used as triggers for mitigations.

**11.7.13** The Contractor should consider human factors where they may provide risk mitigation.

**11.7.14** The Contractor should record the results of the failure mode assessment in the information set.

**11.7.15** The Contractor should record all assumptions, data, judgements and calculations underpinning the risk estimation in the information set.

**Notes:**

i. Identification of failure modes that might contribute to a hazard is an important step in safety analysis. Contractors may consider using techniques such as Failure Modes and Effects Analysis (FMEA) or a Failure Modes Effects and Criticality Analysis (FMECA), but may also include functional analyses, eg Functional Failure Analysis (FFA).

ii. Knowledge of normal functioning of a PSS is also important to understand potential hazards arising from the operation of the PSS. A normal function or previously identified safe failure mode when the PSS is used in different context, eg used in a new environment, can lead to emergent hazardous behaviour. Access to the relevant information would be expected and must be included in the relevant ISSS.

iii. All failure modes that have been identified must be documented (they form part of the information set), but they may not be relevant to the PSS safety case. Failure modes that contribute to a hazard must be tracked as they are relevant to the PSS safety case. It may be necessary to revisit the identified failure modes as the design progresses or requirements change.

iv. The risks associated with failure modes cannot be fully evaluated where the Contractor does not have enough information, eg to estimate the likelihood of a failure mode evolving to an accident, hence the need to document assumptions and judgements. The intent here is to evaluate the likelihood of the failure

mode, either qualitatively or quantitatively, and to identify potential mitigations which must be considered by the designers of systems employing the PSS or system integrators.

v. Guidance on risk estimation and evaluation, including identifying some of the difficulties and limitations of quantitative risk assessment is available through the ASG.

vi. Def Stan 05-138 provides requirements and guidance for the levels of cyber protection required to be achieved by Defence Suppliers.

vii. Def Stan 00-251 provides requirements and guidance for the achievement, assurance and management of Human Factors Integration.

viii. Def Stan 00-055 provides requirements and guidance for supporting PE Failure Assessment where PE unintended behaviour leads to a potential PSS failure mode.

## 11.8 Risk Estimation

The Contractor shall carry out risk estimation to determine systematically the severity of the harm and the likelihood of occurrence for all identified hazards and accidents, utilising the results of the hazard analysis and safety analysis and record the results in the Hazard Log.

**11.8.1** The Contractor, with the agreement of the MOD, should use qualitative estimates for risk assessment, where it is not practical to quantify severity or likelihood.

**11.8.2** The Contractor should consider human factors where they may provide risk mitigation, and the human element is within the scope of analysis.

**11.8.3** The Contractor should record assumptions, data, judgments and calculations underpinning the risk estimation in the information set, such that they can be reviewed and reconstructed.

**Note.** Risk estimation should be done in terms of Risk to Life. Use of risk criteria such as domain specific risk matrices may be required by MOD policy or regulation.

## 11.9 Risk and Compliance Evaluation

The Contractor shall evaluate Risk to Life, for all identified hazards and accidents, and compliance with relevant legislation, standards, regulations and requirements derived from MOD Policy, as defined in the SMP and record the results in the information set.

**11.9.1** The Contractor should evaluate risks against the criteria agreed in the SMP.

**11.9.2** The Contractor should record all assumptions, data, judgements and calculations underpinning the evaluations in the information set, such that they can be reviewed and reconstructed.

**11.9.3** The Contractor should use the evidence produced to evaluate compliance with relevant legislation, standards, regulations and requirements derived from MOD policy.

**11.9.4** The Contractor should record the risk and compliance evaluation results in the information set.

**Note.** It is expected that the Contractor would always be able to evaluate compliance with legislation, standards, regulations and requirements derived from MOD policy, regardless of the scope of supply and scope of analysis.

## 11.10 Satisfaction of Requirements

The Contractor shall carry out safety and systems engineering activities, including but not limited to test, to provide evidence that all Safety Requirements, including Derived Safety Requirements, have been met.

**11.10.1** The Contractor shall undertake systems engineering activities which are capable of detecting counter-evidence.

**11.10.2** The Contractor should identify the most effective method, or methods, for showing satisfaction of requirements, or providing counter-evidence, and include this information in the SMP.

**11.10.3** Whilst there might be general identification of techniques early in the process, the Contractor should ensure that the methods chosen are appropriate to the specific Derived Safety Requirements identified.

**Notes:**

i. In some cases, the only way to show a Derived Safety Requirement has been met might be through a safety analysis technique, eg a FMEA supported with manufacturer's failure rate data can show satisfaction of a quantitative target for the occurrence of a failure mode identified through fault tree analysis. However, in general, as the Derived Safety Requirements can range across any specialty systems engineering discipline, a wide range of techniques might be relevant.

ii. Counter-evidence indicates that the PSS may not meet its Safety Requirements and can arise from incidents, accidents, engineering processes or changes in the operating environment. The systems engineering processes is to be of sufficient rigour to generate counter-evidence when the design solution does not satisfy the Safety Requirement, eg if the requirement has been incorrectly or poorly translated into design then the engineering verification/review process is expected to identify the shortfall. If an incident/accident arises during in-service use then this class of counter-evidence could be an indication that the systems engineering and safety processes were insufficient.

# 12 Health Monitoring and Reporting System

Where practicable and where there is clear evidence that in-service safety will benefit, the Contractor shall incorporate a health monitoring and reporting system with an open and accessible interface standard in the design for the PSS.

**Notes:**

i. There needs to be an agreed process of ownership and management for retrieval and analysis of reported data.

ii. Some regulations and standards require defined recording systems, eg accident data recorders or voyage recorders.

# 13 Safety Reporting

**Note.** The safety reports produced by the Contractor will vary with the scope of supply and scope of analysis, and also with the domain.

## 13.1 Information Set Safety Summary

The Contractor shall produce an ISSS as defined in the SMP.

**13.1.1** The Contractor shall ensure that the ISSS contains sufficient information from the information set to enable a system integrator or operator to discharge their safety responsibilities.

**13.1.2** The Contractor shall ensure that the ISSS contains information on assumptions and limitations regarding the safe use of the PSS.

**13.1.3** The Contractor shall ensure that the ISSS includes a justification of the scope of the information provided.

**13.1.4** The Contractor should ensure that the ISSS is delivered incrementally, as Contracted and as defined in the SMP, to give the MOD visibility of progress in safety engineering and safety analysis.

**Notes:**

i. Guidance on the concept, use and applicability of ISSS and its relationship with Safety Case

Reports is included in Part 2 of this Standard.

ii. The intent is that the ISSS provides information which a system integrator or user needs to employ the PSS safely, and where the Contractor does not have enough knowledge (within the scope of analysis) to assess Risk to Life. In some cases a Contractor will produce both an ISSS and a Safety Case Report.

## 13.2 Safety Case

The Contractor shall produce a Safety Case or Safety Cases for a PSS as defined in the SMP.

**13.2.1** The Contractor shall ensure that the Safety Case consists of 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.

**13.2.2** The Contractor shall ensure that the evidence for the Safety Case is drawn from the information set.

**13.2.3** The Contractor shall address the life of the PSS, as defined in the SMP.

**13.2.4** The Contractor shall ensure that the Safety Case identifies how to address any residual shortfalls in meeting Safety Requirements.

**13.2.5** The Contractor shall provide evidence to demonstrate the competence of individuals and organisations responsible for tasks that have a bearing on safety.

**13.2.6** The Contractor shall develop, maintain and refine the Safety Case as defined in the SMP and in developing the Safety Case the Contractor shall address the full lifecycle (CADMID/T) of the PSS.

**13.2.7** Where practicable, the Contractor should provide objective evidence.

**13.2.8** The Contractor should provide diverse evidence, to ensure that that the overall safety argument is not compromised by errors or uncertainties in individual pieces of evidence.

**13.2.9** The Contractor should demonstrate that the arguments and evidence in Safety Cases are sound, comprehensive and trustworthy.

**13.2.10** The Contractor should provide evidence to demonstrate the adequacy and suitability of the methods and techniques used for safety and risk analysis and in safety engineering.

**13.2.11** The Contractor should develop, maintain and refine the Safety Case through the life of the Contract.

**13.2.12** The Contractor should provide evidence of competency of those whose work could impact safety and confidence in the Safety Case.

**13.2.13** The Contractor should ensure that any related Safety Cases or information sets already in existence and identified in the scope of analysis are utilised and integrated as necessary.

**Notes:**

i. The Safety Case addresses hazards where the Contractor can assess risk, whereas the information set is much broader, addressing, for example, failure modes where the Contractor cannot assess risk (in their scope of analysis).

ii. The Safety Case may not be deliverable and, if the MOD wish to pass on support of the PSS to a third party, explicit provision for the delivery of the Safety Case would have to be made in the scope of contract.

iii. The requirements for the scope and content of the Safety Case are likely to vary with domain, eg the DAE has one safety case "The Air System Safety Case". It is supported by a number of Safety Assessments (defined in MAA02). Where the Contractor is required to supply Safety Cases, Safety Cases Reports; in the DAE they are referred to as Safety Assessments and Safety Assessment Reports and the detailed requirements are set out in the domain-specific MOD policy and DSA Regulatory publications.

iv. In developing the Safety Case, the Contractor may need to consider the full lifecycle (CADMID/T) of the system. For example, a delivered Service applies to the in-service phase of CADMID/T but if the Service life is extended, then the C, A, D and M phase lifecycle assumptions may need to be re-evaluated.

v. The Contractor may not be employed through all phases of the lifecycle but will be required to consider all CADMID/T in the analysis, eg disposal. In all cases this requirement will be defined in the scope of the contract as an extension of the scope of analysis.

## 13.3 Safety Case Reports

The Contractor shall produce a Safety Case Report or Reports as defined in the SMP.

**13.3.1** The Contractor shall produce Safety Case Reports that incorporate the key elements of the safety argument and references to evidence so that, in principle, it would be possible to access the complete Safety Case, starting from the Report, or counter-evidence where it has been identified.

**13.3.2** Where there are shortfalls in the evidence the Contractor shall ensure that the Safety Case Report provides the rationale for operating the PSS, and the ways of mitigating the residual risk.

**13.3.3** The Contractor shall ensure that the Safety Case Report contains information on assumptions and limitations regarding the safe use of the PSS.

**13.3.4** The Contractor shall produce Command Summaries, as defined in the SMP, documenting the assumptions and limitations for safe in-service use of the PSS.

**13.3.5** The Contractor should ensure that any related Safety Case Reports or ISSSs already in existence and identified in the scope of analysis are utilised and integrated as necessary.

**13.3.6** The Contractor should deliver the Reports incrementally, as Contracted, to give the MOD visibility of progress in safety engineering and safety analysis.

**Notes:**

i. Where there are shortfalls in evidence and if the Contractor cannot provide a rationale, then this must be raised with the MOD and other stakeholders so that the relevant duty holder and Safety Committee can take the necessary steps to assist the Contractor in addressing the shortfalls.

ii. The concept, use and applicability of Safety Case Reports, Command Summaries and their relationship with ISSS are included in Part 2 to this Standard and their relevant DIDs provided in the DID Annex. Further guidance on the concepts of MOD Safety Cases and Safety Case Reports are available through the ASG.

iii. The DAE use of Safety Assessments and Safety Assessment Reports to support the Air System Safety Case is defined in MAA02.

iv. Detailed requirements for safety-related report and summaries may vary with domain regulatory requirements.

# 14 Supply and Change Management

## 14.1 Build State Definition

The Contractor shall produce records which show the build state definition (configuration) of each PSS element supplied.

**14.1.1** The Contractor shall ensure that all stakeholders identified in the SMP as needing to be kept up to date regarding the build state to ensure or preserve safety are provided with the build state definition.

**14.1.2** The Contractor should ensure that all parts employed are as specified in design, or provide information to enable an assessment of the impact of change where the original parts are not available or have changed.

**14.1.3** The Contractor should ensure that the build state definition is specific to each delivered instance of a PSS, so that specific instance is properly managed.

**Notes:**

i. An important concept here is the build state definition, which identifies each individual PSS both as initially designed, and as it evolves through life. The responsibility for the build state definition may migrate from the initial Contractor to the support organisation as the PSS evolves through life; in some cases responsibility for the build state may rest with the MOD.

ii. Defence Standard 05-057 addresses configuration management, including giving domain-specific requirements.

iii. No DID is supplied for the build state definition, as this is a general systems engineering concept, not something specific to safety.

## 14.2 Change Control

The Contractor shall define in the SMP, a change control system so that the safety impact of any planned or unplanned change can be identified and assessed.

**Note.** Change control is important in the early phases of the CADMID/T cycle but more so in the in-service phase, as mitigation and management procedures may apply to PSS in active operations. All changes must be managed but unplanned in-service changes, due to operational circumstances, will need to be identified and assessed.

## 14.3 Planning for Change

Where changes are anticipated, eg for managing obsolescence, the Contractor shall develop and implement plans for proactively identifying and addressing those changes to ensure the continued safety of the PSS.

**14.3.1** The Contractor should consider all relevant change drivers, including modified operating requirements, the availability of new technologies, as well as supply chain issue such as changes to legislation, obsolescence or ageing components, and put in place plans for dealing with all of these issues and coordinating plans to minimise the impact of change.

**Notes:**

i. Although the Contractor may not be in a position to make ALARP judgements directly, they will be in a position to support the decision process by identifying new technology options which may enable more cost-effective mitigations, or which make previously discarded design options practicable. The SMP is reviewed and agreed by the Safety Committee, and is the appropriate mechanism to propose design enhancements arising out of compliance with this clause. This is to enable the MOD to judge which

improvements can be implemented in order to comply with its obligations, and meet its operational commitments.

ii. Implementing change plans may require a contractual review; such commercial issues are outside the scope of this Standard. However, such a review may result in a modified scope of contract.

## 14.4 Safety of Changes

The Contractor shall manage all changes under their control so as to preserve safety as in the original design intent or to improve the safety of the deliverable PSS.

**14.4.1** The Contractor shall review and update the information set and ISSS, as defined in the SMP, to ensure that they remain valid.

**14.4.2** The Contractor shall review and update the Safety Case and Safety Case Report, as defined in the SMP, to ensure that they remain valid.

**14.4.3** The Contractor should update the design where there are agreed changes to the Safety Requirements, updating the information set accordingly.

**14.4.4** The Contractor should update the hazard analysis and safety analysis as necessary for all changes, both intended and unplanned, updating the information set accordingly.

**14.4.5** Following any change which has an adverse effect on safety, the Contractor should propose, agree and implement further revisions to the design so as to preserve safety.

**Note.** It is desirable to maintain safe PSS. However, due to operational necessity the MOD can decline to endorse changes or may impose operational limitations on equipment in-service that may be out of control of the Contractor and have an adverse effect on safety. The aim is to restore safety as soon as possible.

## 14.5 Safe Update

The Contractor shall supply updated PSS and associated information, as defined in the SMP, to enable safety to be preserved.

**14.5.1** The Contractor shall supply appropriate installation instructions to enable changes to be made safely to the in-service PSS.

**14.5.2** The Contractor shall update the build state definition for each modified PSS, so that it reflects the modified build state and provide an audit trail of those modifications.

**Note.** The safe update clauses are intended for Contractors with responsibility for determining and enabling the required update. The incorporating change and supporting systems in the Safety In-Service Section identifies the safety requirements where the Contractor is also responsible for implementing the update.

## 14.6 Monitoring Change

The Contractor shall monitor changes to in-service PSS that are visible to them, including using the results of normal reporting, to identify cases where the changes may have undesired safety impacts.

**14.6.1** Where undesired safety impacts are identified, the Contractor shall notify the relevant stakeholders and, where practicable, recommend mitigation to control Risk to Life.

**14.6.2** To ensure visibility of changes, the Contractor should agree with the MOD the monitoring channels to be used; these should be recorded in the SMP.

**Note.** The Contractor may have visibility of the in-service use of the PSS, in such cases the Contractor will need to keep accurate build state configuration records of the individual PSS. This visibility may include changes in use of the PSS in-service. The extent of the responsibility of monitoring and reporting safety impacts due to changes will be part of the agreed scope of supply.

## 14.7 Incorporating Change

The Contractor shall incorporate any new or modified PSS into the in-service system, as defined in the SMP, so as to maintain or improve safety.

**14.7.1** The Contractor shall provide information to other relevant stakeholders, including the MOD in all cases, to enable them to assess the impact of changes made to the in-service system.

**14.7.2** The Contractor should assess supplied PSS, together with installation instructions, and develop and implement plans for safe installation and maintenance.

**14.7.3** The Contractor should ensure that the installation plans address changeover from the old to new PSS, to ensure that safety is managed throughout the change and, so far as is reasonably practicable, to ensure that a reversion to the previous configuration could be carried out should this prove necessary.

**14.7.4** Where temporary modifications have been made to manage risk the Contractor should ensure that they are removed once a permanent resolution has been implemented.

**14.7.5** The Contractor should agree with relevant stakeholders what changes are to be made, including any necessary deviations from the original installation instructions, to enable them to discharge their obligations, eg to maintain an accurate record of the build state.

**Notes:**

i. In many PSS cases the Contract development and manufacture phases will overlap the in-service phase of the CADMID/T lifecycle. These clauses may apply during the overlap and will, depending on the scope of contract, extend to full in-service support. Therefore, these requirements relate to safety maintenance support which may form part of a Contractor provided service. Contractors will need to include relevant safety in-service requirements for supporting PSS and provision of services detailed in this Standard.

ii. For a specific build state, the Safety Case, the associated Safety Case Report and the Command Summary or Summaries, where relevant, need to be amended immediately so all the information remains valid. In practice a judgement needs to be made regarding the necessity of change, as there is a cost to updating documentation but also a risk of not doing so.

iii. Where in-service PSS would be required to be taken out of operational service, safety updates may not be achievable in the short term and may require alternative mitigation to be considered and effectively implemented.

iv. MOD necessarily has control over in-service requirements. It will be the duty holder who makes decisions on implementation of mitigation and responsibility for Risk to Life.

v. In the DAE, the aviation Duty Holder or Accountable Manager (Military Flying) are the designated posts who can accept risks as being tolerable and ALARP.

## Section 4 - Safety In-Service

**Notes:**

i. This section of the Standard relates to additional requirements when the PSS is in the in-service phase of the CADMID/T cycle and is concerned with Contractor support to in-service PSS and Contractor provided services. This Section would be tailored to meet the scope of contract, and may be applied to trials and demonstrations.

ii. The boundary between what is provided in support of the in-service PSS, and a Contractor managed services will depend on the scope of analysis or scope of supply, the in-service/operational scenarios and form part of the agreed scope of contract. In all cases the SMP and other associated plans must delineate the roles, responsibilities, and communication channels and decision-making mechanisms.

iii. Regulators may have domain specific requirements for in-service support or service provision. The intent here is to set generic requirements on Contractors that are independent of those domain specific requirements or regulations.

# 15 Supporting Systems In-Service

## 15.1 Management of Safety-Related In-Service Data

The Contractor shall coordinate the management of safety-related in-service data where the deliverable PSS interface or interact with other PSS.

**15.1.1** The Contractor should exchange in-service data, or the results of analysing the data, with the stakeholders responsible for the operation of interfacing and interacting PSS where they might be able to use it to help sentence problems, and to determine remedial action.

**Notes:**

i. The Contractor will establish organisational interfaces with other stakeholders applicable to the safety management elements of the Standard. This requirement expands on a general obligation to deal with in-service data, by referring to stakeholders who may be integrators or responsible for interfacing PSS.

ii. Hazards on one PSS in a system may result in new hazards that manifest in another interfacing system. Interfacing with other stakeholders (MOD and other Contractors) need to be agreed, which may require change to the scope of contract and managed through the SMP.

iii. This Standard cannot place requirements on the MOD. Any Contractor requirements for data must be agreed in the scope of contract and captured in the scope of analysis. If health monitoring and reporting system is employed then supply of data will be agreed at scope of contract.

## 15.2 Monitoring and Reporting

The Contractor shall define and operate a process for recording and analysing relevant data from operation of the PSS (including accident and incident reporting data), to control in-service Risk to Life and to inform the stakeholders responsible for support activities.

**15.2.1** The Contractor shall review the Safety Case, in the light of the recorded data to identify areas where operations vary from predictions or assumptions, eg the actual Risk to Life is significantly higher than the estimated Risk to Life, or a PSS is operated outside declared limitations.

**15.2.2** The Contractor shall sentence the results of analysis of the data and the review of the Safety Case to determine situations which indicate the need for remedial action and, once agreed with the MOD, shall implement those actions within their sphere of responsibility.

**15.2.3** The Contractor shall inform all relevant stakeholders where they have identified the need for remedial action, and provide those stakeholders with sufficient information to enable them to take appropriate action.

**15.2.4** The Contractor should define and operate a process for collecting, analysing and documenting safety-relevant in-service data including but not limited to usage and environment.

**15.2.5** The Contractor should define and operate a process for collecting, analysing and documenting defect or failure data.

**15.2.6** The Contractor should define and operate a process for collecting incident, accident and near miss reports, and comparable data from other operations available to the Contractor or supplied by the MOD.

**15.2.7** The Contractor should analyse all collected data addressing both individual events and longer-term trends, to identify those events which require action.

**Notes:**

i. These clauses require coordination between operations and support, regardless of whether the support is provided by MOD or industry (or both) and the boundaries of responsibilities will be defined clearly in the SMP or in a different plan as agreed with the MOD.

ii. Defect or failure data will be obtained from various sources some of which may be management processes or part of the PSS (eg Accident Data Recorders).

## 15.3 In-Service Data Analysis

The Contractor shall define and operate a process, agreed with the MOD, for sentencing and prioritising reported data from the in-service use of the PSS to identify remedial action to preserve or improve safety.

**15.3.1** The Contractor should liaise with the MOD to establish, or interface to, a Failure Reporting Analysis and Corrective Action Systems (FRACAS) or equivalent, to ensure that support is based on as accurate and timely data from operations, as is practicable.

**15.3.2** The Contractor should analyse reported defects, errors or failures, including human errors, across all Defence Lines of Development, for their impact on safety to identify remedial action to preserve or improve safety.

**15.3.3** The Contractor should analyse reported incident, accident and near miss reports, and comparable data from other operations available to the Contractor or supplied by the MOD, for their root causes to identify remedial action to improve safety.

**15.3.4** Where the Contractor supports in-service PSS which are in use by multiple stakeholders, the Contractor should, so far as is reasonably practicable, use information relating to the PSS to efficiently and effectively manage safety.

**Note.** It is likely that much of the analysis of in-service data will require operational or engineering judgement, rather than being based on solely statistical analysis.

## 15.4 Remedial Action

The Contractor shall implement remedial actions to preserve or improve safety, agreed with the MOD and prioritized accordingly.

**15.4.1** The Contractor should plan remedial actions taking into account the need for efficient change management, to enable updates to the in-service PSS with minimum disruption.

**15.4.2** The Contractor should plan remedial actions taking into account the need to deal with foreseeable changes, as well as those driven by analysis of in-service events.

**Notes:**

i. The emphasis in these clauses is on remedial action. However, the longer term actions are just as important, eg design changes, to remedy problems, as implementation plans based on risk analysis will be the responsibility of the duty holder.

ii. The Contractor will have a duty to notify relevant stakeholders if they identify that immediate remedial action is required. Domain specific requirements or regulations will be captured in the scope of contract.

iii. The Safety Committee will prioritise remedial action. The organisational arrangements will be defined in the SMP.

# 16 Service Provision

**Note.** These clauses apply only when the Contractor is supporting the MOD by providing a Service, which may include operating a PSS. It is intended that they cover development operations, eg test firings, sea trials, flight trials, etc. These are general requirements for such activities and there may be domain-specific requirements or regulations. These clauses will not be applicable if the scope of contract does not include service provision.

## 16.1 Safety Case Report

The Contractor shall produce a Safety Case Report and Command Summary and deliver them to the MOD for approval before commencement of services.

**16.1.1** The Contractor shall maintain the Safety Case, Safety Case Report and Command Summary so they are accurate representations of the service.

**16.1.2** The Contractor should produce Command Summaries so that each provision of the service can be properly assessed and controlled in terms of risk.

**16.1.3** The Contractor should provide information to support domain specific processes providing essential information for the duty holder responsible for the service to manage Risk to Life.

**Notes:**

i. The Command Summary is intended to provide essential safety information on the provided service for the mission commanding officer or manager to manage Risk to Life, and may be mission or sortie specific. Therefore, this may lead to the production of more than one Command Summary.

ii. The Command Summaries and Safety Case Reports will be reviewed and accepted by the MOD Regulators, duty holders and stakeholders, prior to commencement of operations.

iii. In the DAE, the Operating Duty Holder is responsible and accountable for the Air System Safety Case. All Duty Holder Facing organizations have a responsibility iaw RA1020 in the management of Risk to Life.

## 16.2 Service Provision Planning

The Contractor shall produce plans for management of service operations, covering all reasonably foreseeable situations including abnormal and emergency situations.

**16.2.1** The Contractor should ensure that the plans cover the safety of the full range of normal services and operations, including but not limited to defining standard operating procedures, resourcing, training, and oversight arrangements.

**16.2.2** The Contractor should ensure that the plans cover the safety of emergency situations, including but not limited to defining emergency response, coordination and decision making, including liaison with the service duty holder and relevant stakeholders.

**16.2.3** The Contractor should ensure that these plans cover safe update, including ways of making changes on continuously running systems, if necessary, building on installation instructions supplied from support, as appropriate.

**16.2.4** The Contractor should ensure that the communications plan, detailed in the SMP, includes processes for delivery of in-service data and build state definition.

**Note.** These plans may be part of the SMP or in a separate plan as agreed with the MOD where the Contractor provides a service that supports an in-service/operational capability. It is essential that the coordination mechanisms between relevant roles, responsibilities and delivery communication mechanisms are clear.

## 16.3 Risk Management

The Contractor shall support the MOD in managing predicted or emergent Risk to Life arising from hazards and accidents associated with the service, according to the ALARP principle, throughout the Contract life, and as defined in the Safety Case Report.

**16.3.1** The Contractor shall cooperate with the duty holders for interfacing or interacting services or operations to enable effective management of Risk to Life.

**16.3.2** Where necessary and with the duty holder agreement, the Contractor shall implement immediate action to manage Risks to Life until a longer-term resolution is identified.

**Notes:**

i. As these requirements relate to a service upon which a MOD military capability may depend, there is an explicit requirement on the Contractor to support the management of Risk to Life (as opposed to providing information to enable the MOD to do so). This is necessary and appropriate when the Contractor has responsibility for a service that may contribute directly to the in-service Risk to Life and will necessitate demonstrable compliance with the ALARP principle. This will be agreed with the MOD and defined in the scope of supply and documented in the SMP. Decisions on whether a Contractor service that impacts on the Risk to Life is compliant with the ALARP principle will be made by the MOD duty holder endorsed through the mechanism of the MOD SMS.

ii. Guidance on ALARP in a military equipment context is available on the ASG.

iii. DAE specific guidance on ALARP is contained in RA1210.

iv. It is essential that plans ensure that the roles, responsibilities, communications and decision and action mechanisms are in place so as to manage the emergent risk. This is particularly essential where immediate action is necessary to deal with an emergent risk.

## ANNEX A - DEFINITIONS

For the purpose of this Standard, the following definitions apply:

| Term | Definition |
|---|---|
| Accident | An event, or sequence of events, that causes unintended harm. |
| ALARP | As Low As Reasonably Practicable (for further clarification refer to extant MOD guidance). |
| CADMID/T | Reference to the acquisition lifecycle for capability, the term CADMID/T comes from the initial letters of its six phases, Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal/Termination. |
| Command Summary | A distillation of the safety case report providing essential information for the in-service/operational commanding officer or manager of a system or operator of a service to manage operating risk. |
| Contractor Safety Auditor | An individual or team, independent from those areas within the Contractor's organisation, or any Sub-Contractors that are subject to Contractor safety audit, that undertakes audits and other assessment activities on behalf of the Contractor. |
| Counter-evidence | Evidence that has the potential to refute specific safety claims, eg evidence showing that Safety Requirements, including Derived Safety Requirements, have not been met. |
| Data Safety Requirements | A subset of PE Safety Requirements that addresses inherent safety properties of data. |
| Defence Air Environment | A term equivalent to Military Air Environment used to emphasize the inclusion of contractors and industry engagement, support and operations. |
| Derived Safety Requirement | A safety requirement which is derived from a design or analysis activity. |
| Design Integrity | The extent to which the design is free from flaws which could give rise to or contribute to hazards or failure modes that contribute to a hazard. |
| Duty holder | A duty holder is a MOD person who is in key position which is responsible and accountable for the control of activities that are so hazardous that they could give rise to a risk to life (for further clarification, refer to extant MOD guidance). |
| Failure Mode | An unintended behaviour of a product, service or system which could be hazardous in the broader system context, eg when the product or service is integrated into a system, or system as part of a system of systems. |
| Harm | Adverse impact on people, including fatality, physical or psychological injury, or short or long term damage to health. |
| Hazard | Potential to cause harm, eg A physical situation or state of a system, often following from some initiating event that may lead to an accident. |
| Hazard Analysis | The process of analysing in detail the hazards and accidents associated with a system. |
| Hazard Identification | The process of identifying and listing the hazards and accidents associated with a system. |
| Hazard Log | The continually updated record of the hazards and accidents associated with a system. It includes information documenting risk management for each hazard and accident. |
| Hazard Log Report | A periodic report of status of the Hazard Log. |
| Health Monitoring and Reporting System | A system which monitors key parameters of a PSS to enable diagnosis of failures and, in some cases, prediction of impending failures to enable action to be taken to prevent failures occurring. |

| Term | Definition |
|---|---|
| Human Factors | The systematic application of relevant information about human capabilities, limitations, characteristics, behaviours and motivation to the design of systems. |
| Incident | The occurrence of a hazard that might have progressed to an accident but did not. |
| Independent Safety Auditor | An individual or team, from an independent organisation, that undertakes audits and other assessment activities on behalf of MOD to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose. |
| Information Set | The information from the design of a product, service or system and its analysis that is pertinent to safety. |
| Information Set Safety Summary | A summary of the information set which identifies the safety properties which support production of a safety case, particularly where the requirement includes integration or interfacing with other PSS for an intended use in a given operating environment. |
| Mitigation Strategies | Measures that, when implemented, reduce risk. |
| Operating Environment | The total set of all external natural and induced conditions to which a system is exposed at any given moment. |
| PE Safety Requirement | A Safety Requirement that is:<br>a) usually allocated from PSS systems engineering and safety assessment activities;<br>b) derived from the choice of standards to meet the PE Design Integrity, or;<br>c) derived as the PE design evolves |
| Product | An engineered artefact. Products can be from the small scale, eg a pump or a digital map, to the large scale, eg an aircraft carrier or a geographically distributed logistics application program. |
| Programmable Element | PSS that is implemented in software or programmable hardware, which includes any device that can be customised, eg ASICs, PLDs and FPGAs. |
| Progress Report | A periodic report of the status of the Safety Management Plan. |
| Risk | Combination of the likelihood of harm and the severity of that harm. |
| Risk to Life | Risk of harm. |
| Regulator | An agency that ensures compliance with laws, regulations and established rules. (May be MOD or civilian). |
| Risk Estimation | The systematic use of available information to estimate risk. |
| Risk Management | The systematic identification, evaluation and reduction of risk. |
| Safe | Freedom from unacceptable or intolerable levels of harm. |
| Safety Analysis | The systematic identification of potential causes of hazards or failure modes that contribute to a hazard. |
| Safety Audit | Audit to ensure that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives and related outputs are correct, valid and fit for purpose. |
| Safety Auditor | An individual or team that undertakes safety audits. |

| Term | Definition |
|---|---|
| Safety Audit Report | A report summarising the conduct of a safety audit, identifying findings, actions and recommendations. |
| Safety Case | A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. |
| Safety Case Report | A report that summarises the arguments and evidence of the safety case and documents progress against the safety management plan. |
| Safety Committee | A group of stakeholders that exercises, oversees, reviews and endorses safety management and safety engineering activities. |
| Safety Engineering | The development of products, services or systems which are safe, informed by hazard identification, hazard analysis, risk analysis, safety analysis and knowledge of failure modes that contribute to a hazard. |
| Safety Management | The application of organisational, management and engineering principles in order to achieve safety. |
| Safety Management System | The organisational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet Safety Requirements and safety policy objectives. |
| Safety Management Plan | A document that defines the strategy for addressing safety and documents the Safety Management System for a specific project. |
| Safety Requirement | A requirement that, once met, contributes to the safety of a product, service or system or the evidence of the safety of a product, service or system. |
| Scope of Analysis | The depth and coverage of the safety engineering activities defined in the Contract. The scope of analysis may apply to all, or more or less than, the scope of supply. |
| Scope of Contract | The scope of supply and scope of analysis. |
| Scope of Supply | The products and/or services and/or systems and deliverable information to be produced by the Contract. |
| Sentencing | A decision expressing a judgement on the required remedial safety action, eg mitigation strategy or derived safety requirement. |
| Service | The operation or usage of a system in a defined operating environment to achieve a specific purpose or purposes. A service can be any activity using a system, eg maintaining/updating military vehicles. |
| Severity | A measure of the degree of harm. |
| System | A combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate. |
| System of Systems | A system that includes more than one element that are themselves systems, and which are interdependent but are not necessarily controlled by the same authority or mechanism. |
| System Integrator | A Contractor or organisation responsible for the bringing together of PSS, ensuring that the components function together, to produce a higher-level system or capability as defined in the Contract. |
| Top Level Safety Requirement | Safety requirement explicitly imposed on the Contractor, usually arising from the Contract, relevant legislation, standards or MOD policy. |

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

**DStan Helpdesk**

Tel: +44 (0) 141 224 2531

Fax: +44 (0) 141 224 2503

Internet e-mail: enquiries@dstan.mod.uk

### File Reference

The DStan file reference relating to work on this standard is 21/56/1.

### Contract Requirements

When Defence Standards are incorporated into contracts, users are responsible for their correct application and for complying with contractual and statutory requirements. Compliance with a Defence Standard does not in itself confer immunity from legal obligations.

### Revision of Defence Standards

Defence Standards are revised as necessary by an up-issue or amendment. It is important that users of Defence Standards ensure that they are in possession of the latest issue or amendment. Information on all Defence Standards can be found on the DStan Websites https://www.dstan.mod.uk and http://dstan.uwh.diif.r.mil.uk/, updated weekly. Any person who, when making use of a Defence Standard, encounters an inaccuracy or ambiguity is encouraged to notify UK Defence Standardization (DStan) without delay in order that the matter may be investigated and appropriate action taken.