Ministry of Defence

Defence Standard 00-056 Part 01

Issue 8 **Date:** **14 October 2023**

Safety Management Requirements for Defence Systems

Part: 01 : Requirements and Guidance

Section 1

Foreword

Defence Standard Structure

Section 1 (Generated by the StanMIS toolset)

- Revision Note
- Historical Record
- Warning
- Standard Clauses

Section 2 (Technical information provided by Subject Matter Expert)

- Title
- Introduction (optional)
- Table of Contents
- Scope
- Technical Information to include Tables and Figures
- Annexes (as required)

Section 3 (Generated by StanMIS toolset)

- Normative References
- Definitions
- Abbreviation
- Changes Since Previous Issue

REVISION NOTE

Defence Standard 00-056 Part 1 Issue 8 has been reviewed and updated using a 2 tier mechanism within DE&S, consisting of a System Safety Working Group (SSWG) and the Safety and Environmental Standards Review Committee (SESRC). The SSWG and SESRC operating to extant Terms of Reference and the review conducted using an agreed scope.

The main change in this document, to avoid commercial ambiguity, is the changeover of all "should" requirements to "shall". The latter also promotes due diligence and interpretation to be applied to each requirement. The tailoring and compliance matrix in part 2 still provides a handrail for tailoring.

There has been a substantial format change (issue 8 uses a different template to issue 7) and there are many minor changes to part 1. The briefing pack available from DStan for this update provides an overlay document that details all changes conducted from issue 7 to issue 8.

HISTORICAL RECORD

This standard supersedes the following:

Def Stan 00-056 Pt 1 Iss 7

WARNING

The Ministry of Defence (MOD), like its contractors, is subject both to United Kingdom law and any EU-derived law that has been retained under the European Union (Withdrawal) Act 2018 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.

STANDARD CLAUSES

a) This standard has been published on behalf of the Ministry of Defence (MOD) by UK Defence Standardization (DStan).

b) 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 the Defence Standard, DStan shall be informed so that a remedy may be sought.

c) 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.

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

e) 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.

Section 2

Safety Management Requirements for Defence Systems

Part 1: Requirements

General

0 Introduction

0.1 Under United Kingdom (UK) law, all employers have a duty of care to their employees, the general public and the wider environment. For the UK Ministry of Defence (MOD) this includes, but is not limited to, an obligation to manage the risk to life associated with operation of military systems. The Secretary of State for Defence's policy statement (see note) defines the governance necessary to ensure the health and safety of all those who deliver defence activities, and those who might be affected by defence activities; amongst other governance policy statements, the Secretary of State for Defence appoints the Permanent Secretary to chair the Defence Safety and Environment Committee (DSEC) and supports the Defence Safety Authority (DSA) in its independent role, as defined by its Charter.

Note. Available from GOV.UK (https://www.gov.uk/government/publications/secretary-of-states-policy-statement-on-safety-health-environmental-protection-and-sustainable-development).

0.2 In accordance with general guidance provided by the UK Health and Safety Executive (HSE) and Joint Service Publication (JSP) 815, the Defence Safety Management System, the UK MOD will discharge its duty for health and safety 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 UK MOD policy imposes a more stringent standard. HSE guidance states that if societal risks can be shown to be broadly acceptable and that no group or individual is subject to relatively high individual risks, demonstration of ALARP can be based on adherence to up to date codes, standards and established good practice. Where the risks are deemed to be tolerable if ALARP, then the demonstration of ALARP can be based on good practice, plus risk reduction measures, with further risk reduction shown to be grossly disproportionate in terms of cost benefit. If risks are intolerable then risk reduction is required irrespective of cost.

Note. This standard does not address all aspects of UK Health and Safety Law. Areas not addressed by this standard should be identified and addressed by the appropriate accountable person.

0.3 For Defence acquisition projects, the Acquisition System Operating Model (see Note 2) defines how the UK MOD conducts, governs and controls the defence acquisition process. It is the primary bearer of all policy and guidance governing defence's project delivery and commercial functions. The specifics of individual acquisition projects that procure Products, Services and/or Systems (PSS) vary, but a UK MOD acquisition accountable person shall be responsible for health and safety in each case and they shall ensure adherence to relevant policy and legislation.

Notes:

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

2. Available from the KiD through the Defence gateway. Limited civilian access accounts can be requested, although the UK MOD should identify and provide all policy, process, procedures and standards applicable to a contract.

0.4 Delivery of safety-related PSS includes putting in place a safety management system and ensuring suitable safety reporting occurs. In accordance with the Acquisition System Operating Model, it is not uncommon for an acquisition project safety case to be produced against which the UK MOD acquisition accountable person might make decisions on safety against the evidence presented. This might be informed by various subordinate safety cases covering sub-sets of the overall PSS; known as safety analyses in some domains.

0.5 UK MOD operating accountable persons, who subsequently use the procured PSS, also assess health and safety in their specific operational or command context. This draws on the acquisition safety case and may produce a separate operating safety case where deltas exist.

0.6 Contractors may be utilised in support of any or all parts of these activities and roles associated with the safety of PSS. Although only accountable persons can judge if risk is ALARP and tolerable, all individuals responsible for the control of activity have a duty to mitigate risk in accordance with the ALARP principle.

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

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

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

0.8 PSS might be bespoke, Commercial-Off-The-Shelf (COTS) or Modified-Off-The-Shelf (MOTS). It might also be based on largely civil or historic PSS, or a Foreign Military Sale (FMS). The requirements of this standard equally apply in all cases. Where alternative standards have been utilised the contractor must ensure that the alternate standard's safety management requirements are equivalent to those defined in Part 1 of this standard and produce equivalent evidence to support the safety arguments. If the alternative standard fails to fully address those safety requirements, the contractor must derive safety requirements that will address the shortfall.

0.9 The purpose of this standard is to support acquisition organisation's delivery by setting safety requirements on contractors that enable procurement of PSS that are compliant with safety legislation and regulations and with UK MOD safety and acquisition policy. The intent is that compliance with these requirements will place UK 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. It is specific to requirements for contractors and does not define the totality of the UK MOD's requirements for managing risk to life, which are articulated in the various legislation, policy and so forth, and as per the Acquisition System Operating Model. For example, contractor obligations might equate to the design (equipment) contribution to risk to life only or, in some cases, the full operating risk to life.

Notes:

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

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

0.10 This standard defines requirements for contractors that might be called up by contract to cover their contribution to safety management, safety engineering and/or safety in-service. It does not absolve the UK MOD from its responsibilities to these ends and in no way absolves contractors from complying with legal requirements relating to health and safety at work.

0.11 To support the varied nature of defence acquisition projects, this standard is designed to be tailorable and flexible. This flexibility is based on the premise of a clear definition of the scope of contract supply and analysis, as well as the production of safety cases and command summaries to support the overarching acquisition and operating safety cases. It requires interfaces between safety cases, external organisations and PSS be defined, thus ensuring clarity in the scope, management and integration of safety across all such contracts.

0.12 The scope of contract (which encompasses the scope of supply and scope of analysis) provides the boundary of the safety activities to be conducted as part of that contract. It is negotiated during the early phases of a project where the scope of supply and the scope of analysis are determined.

0.13 Tailoring of the requirements to satisfy the scope of contract may be delivered through UK MOD Regulations. Tailoring shall be applied at Invitation To Tender (ITT) or in the contract in the form of a compliance matrix.

Note. Tailoring enables the removal, etc. of requirements that conflict with domain specific regulations or that are not applicable to the scope of contract. For example, requirements pertaining to safety engineering when only a service is being acquired, or requirements pertaining to in-service support when a system is being acquired but not operated by the contractor.

0.14 The requirements are grouped into three main areas as follows:

a) **Safety Management.** Chapter 2. The requirements for organisational and general processes to ensure that risk to life is managed effectively.

b) **Safety Engineering.** Chapter 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.** Chapter 4. The requirements for managing safety where a contractor is supporting the UK MOD by providing a service, which might include operating a PSS.

0.15 The UK MOD and contractors are subject to UK Law for activities in this country. These laws do not apply overseas. However, it is the Secretary of State for Defence's policy that when overseas the UK MOD will, in addition to complying with law of the host nation, achieve outcomes so far as reasonably practicable that are at least as good as those required by UK legislation. Contractors are expected to comply with the Secretary of State's policy statement. Generally, defence contractors cannot benefit from any disapplication, exemption or derogation from statutory requirements granted to Defence where they control activities, but, there may be exceptions to this and where this is the case, the responsibilities for complying with defence regulations shall be specified in contractual arrangements. Significantly though, defence contractors cannot claim Crown Immunity from prosecution. Contractors who supply PSS to the UK MOD are subject to legal duties, which might vary with the place of manufacture, supply and operation. The UK MOD shall have regard to the needs of contractors to discharge their legal duties when interpreting and applying the requirements of this standard.

0.16 This standard is based upon a definition of safe, which addresses fatality, physical or psychological injury or damage to the health of people, including UK MOD employees and the general public; in this standard we use the term risk to life in this sense. This standard is only intended to be applied to address operational effectiveness, survivability and reliability of PSS, and the management of environmental issues, where risk to life results.

0.17 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. Defence Standard 00-056 Part 2 Issue 6 is extant with this issue of Part 1.

0.18 This standard identifies requirements for the achievement and demonstration of safety by a contractor who is required to have safety management system in place.

Contents

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 UK 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 might 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 UK 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 UK MOD considers all Defence Lines of Development (DLOD) for PSS, but this might not be included in the scope of contract, eg concepts and doctrine would consider risk to life and would be a UK MOD responsibility.

Note. DLOD is a term used within the UK MOD to refer to all aspects of an acquisition or operation, not just the equipment. It covers: training, equipment, personnel, information, concepts & doctrine, organisation, infrastructure, logistics and interoperability. These are further described within the Knowledge in Defence website (https://kid.mod.uk/).

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 accountable person, beyond the deliverable PSS.

b) Full, where the contractor carries out safety engineering and safety management for the deliverable PSS, including interfaces to other 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 UK MOD acquisition scenarios.

1.4 Whilst contract life might 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 shall 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 might need to cover the full CADMID/T cycle.

1.4.4 All requirements of this standard shall apply regardless of the PSS lifecycle adopted.

1.5 This standard applies to PSS that have been identified as requiring accountable persons, supported by safety committees and relevant stakeholders. That being PSS for which there is an associated risk to life.

1.5.1 For all PSS to which this standard is applied, a UK MOD nominated accountable person will retain responsibility and accountability for the risk to life. The scope of contract is agreed between the UK MOD and the contractor and would identify accountable persons and relevant stakeholders who are responsible for managing safety of the PSS. The relevant stakeholders may include representatives from the UK MOD and Industry (for other related PSS) that might impact the PSS safety interfaces.

1.5.2 The mechanism for governing safety is through the safety management system and agreed safety committees. Terms of Reference and membership of safety committees will be specific to the scope of contract.

Notes:

1. This standard is specifically about safety and there is expectation that requirements will be set by the UK MOD and be included in the project documentation, eg capability, performance and reliability criteria, Concept of Use / Employment / Operations (CONUSE / CONEMP / CONOPS) and, User and System Requirements Documents (URD / SRD).

2. These clauses are an indicative commitment from the UK MOD to the contractor and a limitation on the scope of this standard. The contractor must assume that the UK MOD has a Safety Management System (SMS) for their PSS responsibilities, eg a safety committee exists prior to ITT. Agreeing a scope of contract is intended to clarify responsibilities between the UK MOD and the contractor. As the PSS evolves through life the scope of contract might need to be revisited and might need to be re-negotiated.

3. The interface and degree of support/cooperation between the UK MOD SMS and the contractor's equivalent would form part of the UK MOD/contractor agreed scope of contract. This standard defines the requirements placed on the contractor. For information on UK MOD processes and responsibilities, contractors can refer to the UK MOD publications and procedures, eg regulatory publications such as the Military Aviation Authority Regulatory Publications (MAA03), which are available through the Defence Gateway or GOV.UK websites, the UK MOD Project-Oriented Safety Management System (POSMS) manual, which can be accessed from the UK MOD Acquisition Safety and Environmental Management Systems (ASEMS) website http://www.asems.mod.uk or UK MOD policies within Joint Service Publications, which can be access via the Government publications website https://www.gov.uk/government/collections/joint-service-publication-jsp.

4. One of the main mechanisms of the UK MOD SMS is governing 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.

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

6. If an incremental rather than sequential lifecycle is adopted all requirements remain extant, but some requirements, such as those pertaining to creating a safety management system and planning supply and change management, will likely require some upfront activity. Other requirements, however, may also be applied in a continuous fashion, such as those for engineering safety requirements and undertaking hazard and risk analysis.

2 References

2.1 Normative References.

2.1.1 This standard does not contain any normative references.

2.2 Informative References

2.2.1 Informative references in this standard are to Relevant Good Practice (RGP), sources of additional guidance and context to provided Notes. It is expected that where any such standard is applied, the latest version should be used. The following are detailed:

ASEMS	DE&S Acquisition Safety and Environmental Management System (http://www.asems.mod.uk)
Def Stan 00-055	Requirements for Safety of Programmable Elements (PE) in Defence Systems
Def Stan 00-251	Human Factors Integration for Defence Systems
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
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

IET COPCSRSP	Code of Practice for Competence for Safety-Related Systems Practitioners
IET COPISA	Code of Practice for Independent Safety Assessors
ISO 26262	Road Vehicles – Functional safety
ISO 9001	Quality Management Systems
JSP440	The Defence Manual of Security Part 1 and Part 2
JSP 815	Defence Safety Management System
KiD	Knowledge in Defence (https://kid.mod.uk/)
MAA02	MAA Master Glossary (https://www.gov.uk/government/collections/maa-regulatory-publications)
MAA03	MAA Regulatory Process (https://www.gov.uk/government/collections/maa-regulatory-publications)
MCSRP	Managing Competence for Safety-Related Practitioners
RTCA DO-178	Software Considerations in Airborne Systems and Equipment Certification
SAE Aerospace Recommended Practice (ARP) 4754	Guidelines for Development of Civil Aircraft and Systems.
STPA Handbook	STPA Handbook
White Book	An Introduction to Safety Management in the UK MOD

Notes:

1. Defence Standards (Def Stans) can be downloaded free of charge from the UK Defence Standardization (DStan) web site by visiting https://www.gov.uk/guidance/uk-defence-standardization.

2. Many UK MOD policies which include safety are codified within JSPs or defence regulatory publications that can be accessed via the GOV.UK website. Some regulations and JSPs, such as JSP 440, are subject to restrictions on distribution. Where relevant, this material will be provided by the contracting authority.

3. In the Defence Air Environment (DAE), the MRPs define Air Safety Management Systems requirements through Regulatory Articles, https:/www.gov.uk/government/collections/maa-regulatory-publications. MRPs referenced in Part 1 of this standard are in the context of the DAE only.

3 Definitions

3.1 Terms and Definitions

3.1.1 Terms and definitions are detailed in Section 3.

Note. UK MOD regulatory publications, a contractor's Safety Management System (SMS), this standard and open standards may use terms and definitions that are diverse. Where there is divergence, the contractor will need to agree a glossary with the UK MOD which will need to be documented, eg in the Safety Management Plan (SMP).

3.2 Mandatory Requirements

3.2.1 The use of the word "shall" indicates a requirement, whereas "should" indicates a recommendation. A requirement is an expression in the content of this document conveying objectively verifiable criteria to be fulfilled and from which no deviation is permitted other than through agreed tailoring. Whereas a recommendation is an expression in the content of this document conveying a suggested possible choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others.

Note. In contracts for PSS in the DAE, as defined in the Military Aviation Authority (MAA) Glossary MAA02, the "should" term is the permissive verb to allow the regulated community to consider an alternative approach in meeting the regulatory requirement. Any alternative approach to MAA regulation or this standard (via tailoring) must be agreed with the UK MOD in accordance with MAA03, the MAA regulatory processes.

3.3 Notes

3.3.1 The Notes in this standard are provided to support the meeting of its mandatory requirements.

Safety Management Requirements

4 Safety Management System

The contractor shall operate an SMS that defines a framework that ensures the contractor's organisation directs, controls and monitors its safety management activities. This shall cover occupational safety and may also cover PSS safety.

Notes:

1. Safety culture and SMS 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. The standard does, however, strongly encourage a positive safety culture since they provide a major contribution to PSS safety. UK MOD guidance on safety management and safety engineering such as POSMS and An Introduction to Safety Management in the UK MOD (White Book) are available via the http://www.asems.mod.uk website.

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

3. The UK 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 UK MOD, depending on the project requirements.

4.1 Safety Management Plan

4.1.1 The contractor shall define and implement a coherent approach towards the management of all safety-relevant activities, throughout the life of the contract and document their approach in an SMP.

4.1.2 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.

4.1.3 The contractor shall show that use of civil, open or other standards or good practice is appropriate for their contract.

4.1.4 The contractor shall analyse the civil, open or other standards or good practice which they intend to apply to the contract; identify any divergences from this standard; applicable regulations and legislation; and document the results of the analysis and their proposed means of resolving any divergences between them in the SMP.

4.1.5 The contractor shall 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.

4.1.6 The contractor shall 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.

4.1.7 Where the contract includes provision of a service the contractor shall agree with the UK MOD the balance between the activities managed through the service SMP and through other relevant plans. This will draw on the service SMP as the key plan for the safety aspects of the delivery, prior to commencement of the service.

4.1.8 Where the contractor has an appropriate pre-existing organisational SMS in place, the SMP shall draw on that system for occupational safety and may draw on it for PSS safety.

4.1.9 Where the contractor does not have an appropriate pre-existing organisational SMS in place, the SMP shall address the core principles of both occupational and PSS safety management.

4.1.10 Where the UK MOD, contractor and / or sub-contractors each operate an SMS, the SMP shall document, in accordance with the scope of contract, the interfaces between them (including how to resolve any differences in methodlogy and terminology) and the boundaries of responsibility and accountability applicable to each.

Notes:

1. It is mandatory for contractors to operate an SMS. In exceptional circumstances, the UK 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 UK MOD regulators. Information on the UK MOD's Acquisition Safety and Environmental Management Systems is available from the KiD. The White Book and the KiD contains guidance on acquisition safety management in a systems engineering context.

2. The SMP defines the safety-relevant activities to be undertaken, and these are agreed with the UK 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.

3. The UK 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.

4. A Data Item Description (DID) for the SMP is provided in the Annexes to Part 2 of this standard.

5. For failure modes of new and novel technologies in particular, it might be that the contractor needs to draw on emergent standards and practices that might have been developed for a different context (eg automotive rather than airborne domains) and / or that do not fully address the requirements of this standard.

4.2 Agreement

4.2.1 The contractor shall define an SMP as part of the tendering process, and formalise the plan with the UK MOD at contract award.

4.2.2 The contractor shall agree their SMP with the UK MOD

Notes:

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

2. The detail in a draft SMP might not be complete at the ITT stage, for example because the tenderer might 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 might be substantive work to be undertaken in formalising the SMP during contract negotiations and from contract award. The SMP must be agreed with the UK MOD before any safety work is undertaken.

4.3 Review and Update

4.3.1 The contractor shall review and update the SMP to reflect changes throughout the life of the contract.

4.3.2 The contractor shall review the SMP on a regular basis, including changes in the phase of the contract and on significant events, eg stage gate reviews, change in supplier, introduction of a new technology or changes to risk mitigation strategy.

4.3.3 Changes required to the SMP that are identified during its review shall be agreed with the UK MOD before implementation.

4.3.4 When the contract includes support, the contractor shall ensure that all changes in design and their implementation are managed in accordance with the SMP, and other relevant plans, together with mechanisms for safe and effective distribution and installation of those changes.

4.4 Progress Reports

4.4.1 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.

4.4.2 The contractor shall ensure that progress reports highlight all safety issues and proposed remedial actions, as well as documenting progress against planned tasks.

Notes:

1. The DID for the progress report is provided in the Annexes to Part 2 of this standard.

2. This covers all safety issues arising, including those identified during contractors' internal tasks against which progress is not formally reported; such as safety issues encountered during informal testing activities.

5 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.

5.1 Deviation from Requirements

5.1.1 Any deviations from the requirements of this standard shall be formally agreed between the UK MOD and the contractor prior to their implementation, and documented in the SMP.

5.1.2 Where there are conflicts between the requirements of this standard and other requirements, a means of resolving the conflicts shall be agreed between the UK MOD and the contractor.

5.1.3 In the response to an ITT, the tenderer shall specify how they intend to meet the requirements of this standard.

5.1.4 The tenderer shall 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.

5.1.5 For any intended deviations, the tenderer shall indicate how their approach will meet the intent of this standard or explain why compliance is not considered to be necessary.

Notes:

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

2. 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 UK MOD and contractor and might result in contract amendment.

3. The ITT may identify tailoring of the standard as required by the UK 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 UK MOD, eg during contract negotiation.

4. Part 2 of this standard includes tailoring principles and contracting guidance and provides a clause-by-clause tailoring and compliance matrix template.

5.2 Legislation, Regulations, Standards, Policy and Approved Codes of Practice

5.2.1 The contractor shall identify and document all relevant safety legislation, regulations, standards and approved codes of practice applicable to the scope of supply and scope of analysis for the duration of the contract.

5.2.2 The contractor shall work with the UK MOD to identify and agree relevant UK MOD policy appropriate to the scope of supply and scope of analysis, addressing the domain and the technology used.

5.2.3 The contractor shall agree with the UK MOD, all legislation, regulations, standards and approved codes of practice applicable to the scope of supply and scope of analysis, addressing the domain and the technology used.

Notes:

1. Legislation and standards will be documented in a legislation register which is fundamental to any SMS, eg the UK MOD POSMS Project Safety Initiation procedures identify a legislative register as an integral part of the safety case. Adherence to and compliance with legislation, regulations, standards, policy and approved codes of practice is expected to form part of the safety case.

2. The contractor has responsibility for identifying relevant UK and International legislation. Currency must be maintained as legislation may change during the life of the contract. Relevant legislation will be dependent on the contractor's chosen solution, eg where the legislation is technology related, the UK MOD will expect the contractor to be fully aware of their obligations to deliver compliant PSS.

3. The UK MOD is subject to UK Law for activities in the UK. They don't apply overseas. However, it is the Secretary of State for Defence's policy that overseas the UK MOD will apply UK standards where reasonably practicable in addition to complying with host nations' standards. Contractors are expected to comply with the Secretary of State's policy statement. It is noted that generally, defence contractors cannot benefit from any disapplication, exemption or derogation from statutory requirements granted to Defence where they control activities, but, there may be exceptions to this and where this is the case, the responsibilities for complying with defence regulations shall be specified in contractual arrangements. Significantly though, defence contractors cannot claim Crown Immunity from prosecution.

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

5. Approved Codes of Practice (ACOPs) are guidance that has been approved by the UK Health and Safety Executive. Defence Codes of Practice (DCOPs) published by the Defence Safety Authority provide similar guidance on compliance with defence regulations. Although other guidance and codes of practice exist, such as those published by regulators eg DCOPs and professional bodies, the HSE ACOPs are those which have a special legal status with respect to demonstrating compliance with the law.

6. For new and novel technologies (where legislation, regulations, standards, policy and codes of practice might still be developing at pace), steps will need to be taken to monitor their progress throughout the development lifecycle. Where changes occur that might affect PSS use (particularly through legislative change) then changes to the PSS might need to be agreed with the UK MOD.

7. Although this standard is primarily concerned with safety legislation, etc. the contractor has a broader responsibility to identify and comply with all relevant legislation applicable to their scope of supply; be that safety or otherwise.

5.3 Sub-Contracting

5.3.1 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.

5.3.2 The contractor shall identify their requirements to sub-contractors, appropriate to the contractor's scope of supply and scope of analysis.

5.3.3 The contractor shall place requirements on sub-contractors to ensure that the contractor's compliance to the relevant requirements of the standard are met.

5.3.4 The contractor shall 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:

1. Many of the requirements of this standard relate to the relationship between the UK MOD and the contractor. It is the contractor's responsibility to meet the requirements of this standard.

2. 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.

5.4 Multiple Deliverables

5.4.1 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.

5.4.2 The contractor and the UK MOD shall discuss and agree where it is necessary to apply specific requirements of the standard across each deliverable PSS.

5.4.3 Safety case reports and Information Set Safety Summaries (ISSS) shall be produced for each related PSS so that they are "self-contained" from a safety perspective.

Notes:

1. 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.

2. In the case of services interfacing to other PSS, as part of the contract, there might be a need for separate safety case reports for each interfacing PSS. For example, a demonstration may necessitate some additional hazard analysis and safety analysis.

3. 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 case reports, in the DAE they are referred to as safety assessments and safety assessment reports unless specifically referring to the air system safety case.

4. Guidance on the concept, use and applicability of safety case reports and ISSS are provided in Part 2 to this standard. Their relevant DIDs are provided in the Annexes to Part 2.

5.5 Information Management

5.5.1 The contractor shall provide the UK MOD with visibility of the safety engineering, support and safety management activities throughout the life of the contract.

5.5.2 The contractor shall define and agree with the UK MOD an information set which is sufficient to enable all safety relevant design and analysis activities to be reviewed and repeated.

5.5.3 The contractor shall ensure that the information set is kept up to date as the design and analysis evolves, and that suitable configuration management is applied (eg as per the requirements of Def Stan 05-057).

5.5.4 The contractor shall maintain consistency between the information set and the configuration of deliverable PSS.

5.5.5 The contractor shall preserve the information set for the period or periods specified in the contract and as required by law.

5.5.6 The contractor shall ensure that the information set remains accessible as techniques, methodologies and tools change, through the life of the contract.

5.5.7 The contractor shall pass information in an easily accessible form to the UK 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.

5.5.8 The contractor shall define the information set such that all information that might have a safety role are included.

5.5.9 The contractor shall define, and agree with the UK 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.

5.5.10 Where the contractor anticipates difficulties, or very high costs, in preserving access to parts of the information set they shall discuss approaches and options with the UK MOD.

5.5.11 The contractor shall consider obsolescence of the technologies used for preserving the information set.

5.5.12 The contractor shall consider security risks to the information set to ensure its confidentiality, integrity and availability can be maintained.

Notes:

1. 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.

2. Contractors will need to ensure that the information set is manageable, and that there is no unjusten in maintaining this information for extended periods. Technology changes due to obsolescence might make continued information accessibility infeasible, or prohibitively expensive, and the contractor will need to consult with the UK MOD about the cost-benefit trades. PSS with large and fast changing data sets (eg those containing Machine Learning components) will present particular challenges and early planning and engagement with the UK MOD regarding accessibility will be essential for effective information set management.

3. It must be assumed that an ISA, if appointed, would need access to data from the information set used as evidence to substantiate the safety case.

4. Technologies used for the preservation of the information set include both hardware and software aspects. This does not necessarily require the technology to remain static; however, if the technology used to preserve the information changes, the integrity of the information must remain intact.

5.6 Documentary Deliverables

5.6.1 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.

5.6.2 The contractor shall agree with the UK MOD the format and content for all contracted safety-related deliverables in the scope of supply, and document this information in the SMP.

5.6.3 In defining deliverable formatting and content, the contractor shall take into account the DIDs and the requirements of any civil, open or other standards being used, as identified in the SMP.

5.6.4 The contractor shall develop and update the deliverable plans, reports and summaries at appropriate stages of the contract as defined in the SMP.

Notes:

1. DIDs for deliverables are provided in the Annexes to 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.

2. The safety-related deliverables within the scope of supply of a contract are to be agreed with the UK MOD and documented in the SMP. This should be performed with cognisance of domain specific policy or regulations.

3. The safety management plan describes the approach to managing safety for the duration of the contract. The safety audit plan and associated safety audit report, detail independent reviews that confirm realisation of the safety management approach throughout the contract. The hazard log identifies all safety hazards associated with the PSS. An information set captures all safety related data. A safety case is a sub-set of the information set and consists of a structured argument, supported by a body of evidence that provides a case that a system is safe for a given application in a given environment. The full information set and safety case may not be deliverables in their own right. Rather, the safety case report, information set safety summary and command summary present key elements of the safety argument and provision of evidence from the safety case, at a given point in time. These are tailored toward a specific audience in support of their associated responsibilities with regards to managing risk to life and ALARP and tolerablility judgements. The safety case report informs acquisition accountable persons, the information set safety summary informs integrators and operators, whereas the command summary informs in-service accountable persons.

5.7 Agreement of Deliverables

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

5.7.2 The contractor shall define the PSS and its given application, including its boundaries, environment and any known interfacing or interacting PSS, whether extant or planned.

5.7.3 The contractor shall define the PSS to include all relevant elements across the DLOD, as contracted.

5.7.4 The contractor shall 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.

Notes:

1. 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.

2. PSS with a high rate of design change (for example, autonomous systems, or those with agile lifecycles) will benefit from agreeing on how contractor and UK MOD acquisition lifecycles and deliverables will be aligned.

6 Roles and Responsibilities

6.1 Safety Organisation

6.1.1 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.

6.1.2 The contractor shall identify the normal point of contact for safety matters within the safety organisation.

6.1.3 The contractor shall demonstrate how responsibility is delegated to ensure safety is treated with appropriate authority within the organisation and on the contract.

6.1.4 The contractor shall keep the definition of roles and responsibilities of those individuals responsible for safety up to date.

6.1.5 The contractor shall identify and record, in the information set, competency requirements for each role.

Notes:

1. In practice, responsibilities will be shared between UK MOD and Industry and the safety committee is the primary mechanism to ensure coordination and interfaces with other organisations and stakeholders.

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

3. POSMS, Project Safety Initiation procedures, suggests a methodology to ensure that the safety management process is commenced on a firm basis by identifying basic information, interfaces and responsibilities. This might 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.

6.2 Safety Committees

6.2.1 The contractor shall contribute to safety committees and other liaison activities to ensure effective coordination of safety with the UK MOD and other stakeholders.

6.2.2 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.

6.2.3 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.

6.2.4 The contractor shall support the safety committee in any additional roles/tasks as agreed with the UK MOD and recorded in the SMP.

6.2.5 Where there is an appropriate UK MOD safety committee, the contractor shall participate in its work.

6.2.6 Where there is no appropriate safety committee, the contractor shall work with the UK MOD to establish a safety committee that includes relevant stakeholders and define the constitution and terms of reference in the SMP.

6.2.7 Where appropriate the safety committee may delegate work to subsidiary committees or working groups. The contractor shall identify the safety committee organisation in the SMP and state its policy on delegation of responsibility and escalation of issues.

6.2.8 Where the contract involves support, the contractor shall ensure the safety committee approves proposed changes to all PSS before they are implemented.

6.2.9 The contractor shall record all their support given to the safety committee and safety-related meetings.

Notes:

1. Governance and management of safety is a collaborative activity between the UK 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 UK MOD's in-service knowledge of operations, other interacting PSS, and the acceptability of risk. The contractor's and the UK 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 cooperative approach to all aspects of managing safety; this is indicative of a positive safety culture.

2. Normally the UK MOD will have already established a safety committee or a similar construct that satisfies this role, such as a safety panel or working group. The obligations on the contractor will be discharged through engagement in the safety committee. In the unlikely situation that there is no established UK MOD safety committee, the contractor must liaise with the UK MOD to establish such a committee.

3. 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 might also include producing formal records of safety committee meetings.

4. Where the mandatory (shall) requirements 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.

5. Where there is concurrent work on interfacing or interacting PSS, the safety committee will collaborate with other safety committees to manage interfaces, and will refine the scope of analysis if necessary to minimise gaps in analysis, or overlaps and duplication of effort.

6.3 Competencies

6.3.1 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.

6.3.2 The contractor shall record the evidence of competence, on an individual, team and organisational basis, in the information set.

6.3.3 The contractor shall undertake competence management, for all project staff, drawing on publicly available competence frameworks, where possible.

6.3.4 Contractors shall 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.

6.3.5 The contractor shall ensure competence evidence is updated as and when staff leave or take up posts that affect safety and when posts that affect safety are in themselves changed.

Notes:

1. 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 the Maintenance Approved Organisation Scheme and the Design Approved Organisation 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.

2. It is expected that the contractor will provide sufficient evidence of competence of personnel undertaking tasks to meet contracted Safety requirements. This should include schemes to manage ongoing personnel competence. There are external body schemes for assessing safety competency. Examples of safety practitioner competence schemes are: Managing Competence for Safety-Related Practitioners (MCSRP), developed by the HSE, the Institution of Electrical Engineers and the British Computer Society; and the IET Code of Practice for Competence for Safety-Related Systems Practitioners (COPCSRSP). The UK MOD also provides guidance on UK MOD safety-related competence through the KiD. The KiD contains the Acquisition Safety and Environmental Management System (ASEMS) which is supported by Safety and Environmental Protection (S&EP) leaflets.

3. For new and novel technologies, available competency sets might be limited (for example, formal training in the technology might not yet have been developed). Where this is the case, the competence requirements still apply, but contractors may place greater emphasis on transferable competencies from related technologies and may seek external advice to supplement the contractor competency set.

4. Personally identifiable competence statements and evidence might be subject to data protection legislation. This should not forego the ability to satisfy the competency related requirements, but some additional considertation of how such personally identifiable information is lawfully collected, stored, maintained, used and disposed of, might be required.

7 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 UK 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.

7.1 Organisational Interfaces

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

7.1.2 The contractor shall identify all stakeholders relevant to safety for the scope of contract, including the authority, contractor, sub-contractors, suppliers, operators and those of interfacing or interacting PSS. These stakeholders and the processes for managing organisational interfaces between them, shall be documented in the SMP.

7.1.3 The contractor shall 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 might be an urgent need for timely communication between stakeholders, eg to manage an emergent risk that impacts in-service safety.

7.2 Technical Interfaces

7.2.1 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.

7.2.2 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.

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

7.2.4 The contractor shall define and manage the technical interfaces to each element which can be operated in a system of systems.

Notes:

1. 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.

2. 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.

3. 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 contractors' PSS are brought together to form a system of systems.

4. 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.

5. The information on assumptions must always be included in the ISSS. A DID for the ISSS is provided in the Annexes in Part 2 of this standard.

6. This standard identifies the need for safety case reports and ISSS 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.

7. Systems designed to operate in highly uncertain environments (eg autonomous systems) might pass uncertain data across technical interfaces. For example, the interfacing system might use Artificial Intelligence and pass probabilistic data to the PSS. This will place greater emphasis on the information provided in the Command Summary.

7.3 External Interacting Interfaces

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

7.3.2 The contractor shall reconcile assumptions made at boundaries with other PSS to ensure safe operation of the whole, recognising that changes might need to be made in PSS still under development, to cater for limitations of other system elements.

Notes:

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

2. Information about interfacing or interacting products might need to be analysed, and might therefore 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.

3. Changes to resolve incompatibilities will need to be agreed with the UK MOD as they might 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.

8 Safety Audits

Notes:

1. These clauses cover both audit by the contractor, and enabling independent safety audit. Guidance on indepenent safety audit has been provided by the IET ISA Working Group (https://www.theiet.org/impact-society/thought-leadership/expert-panels/independent-safety-assurance-isa-working-group/). ISAs, as referred to in this Standard, are appointed by the UK MOD, not by the contractor. 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.

2. Additionally, organisations with a strong safety culture would use their safety audits (both contractor and ISA led) as opportunities for improvement.

8.1 Audits and Reports

8.1.1 A contractor appointed Contractor Safety Auditor (CSA) shall carry out safety audits as specified in the SMP, to assure the implementation of the SMP.

8.1.2 A safety audit report shall be produced, following each safety audit, which fully describes the findings of the safety audit.

8.1.3 All audit findings shall be assessed for significance and the need for remedial action identified.

8.1.4 The contractor shall ensure that all sub-contract activity is audited, in accordance with the SMP.

Notes:

1. 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 supply chain.

2. Commercial advice should be sought on the best way to flow audit requirements to subcontractors in a proportionate manner.

3. It might be helpful for the CSA to make recommendations on remedial action to the contractor and, where appropriate, the UK MOD.

4. Safety Culture is an important but not contractually enforceable contributor to system safety. The Auditor is encouraged to reflect on the audited party's approach to foster continued development of good Safety Culture practices.

8.2 Contractor Safety Auditor Independence

8.2.1 The contractor shall ensure the CSA is independent from those areas within the contractor's organisation, or any sub-contractors, that are subject to contractor safety audit.

Note. Good practice for CSA 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.

8.3 Independent Safety Audit

8.3.1 The contractor shall allow an ISA, if one is appointed, reasonable access to the information set.

8.3.2 Where restrictions on access to elements of the information set, required for safety audit, are unavoidable, eg foreign export controls, the contractor shall identify and communicate them to the UK MOD at the earliest opportunity.

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

8.4 Remedial Action

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

8.4.2 The contractor shall agree the remedial actions with the UK MOD through the safety committee, and any other relevant stakeholders, as appropriate.

8.4.3 The contractor shall update the SMP, if appropriate, to reflect the agreed remedial actions.

Notes:

1. 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.

2. 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.

Safety Engineering

9 Safety Requirements, Hazard and Risk Analysis

Notes:

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

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

3. The standard is not prescriptive regarding the methods, tools and techniques to be used, the appropriateness of the adopted approach would be justified in the safety case. In some cases, eg where System-Theoretic Process Analysis (STPA, see the STPA Handbook for more information) is used, this might mean that the wording in Section 9 requirements require tailoring. Where this occurs, care is needed to ensure the intent of each clause is maintained.

9.1 Hazards and Accidents

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

9.1.2 The contractor shall employ justifiably appropriate systematic analysis processes for identification of hazards and accidents as defined in the SMP.

9.1.3 The contractor shall ensure that human factors are considered where they might be a contributory cause of a hazard or accident.

9.1.4 The contractor shall ensure that cyber security is considered where intentional or unintentional unauthorised electronic interactions might be a contributory cause of a hazard or accident.

9.1.5 The contractor shall ensure that systematic and random failures are considered where they might be a contributory cause of a hazard or accident.

9.1.6 The contractor shall ensure that the undesired impact of normal functions is considered; this is especially important for contractors carrying out systems integration.

9.1.7 The contractor shall ensure that where new or novel technologies are incorporated, the contribution of previously unseen failure modes to existing or new hazards are considered.

Notes:

1. There are established approaches to hazard analysis. Further guidance on techniques is available on the KiD (White Book), but other RGP might be available and appropriate. Where other approaches are to be adopted, the contractor would justify that RGP has been adopted in the safety case.

2. Safety risk management might be more effective when integrated with other risk management activities and communities (eg Human Factors and Cyber).

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

4. JSP 440 provides guidance for security.

5. Def Stan 05-138 provides guidance for the levels of cyber protection required to be achieved by defence suppliers.

6. Counterfeit materials might contribute to a hazard. It is expected that the contractor will have a policy for the avoidance of counterfeit materials. Def Stan 05-135 provides guidance on the arrangements that a contractor 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 UK MOD.

7. Def Stan 00-055 is concerned with the overall behaviour of PE including cases where the use of PE and data might contribute to a hazard or impair mitigation of a hazard at the system level.

9.2 Hazard Tracking

9.2.1 The contractor shall ensure that the status of the control of all hazards is visible throughout the contract.

9.2.2 The contractor shall implement a hazard log.

9.2.3 The contractor shall ensure that hazard log reports are delivered as defined in the SMP.

9.2.4 The contractor shall update the hazard log throughout the contract to ensure that it accurately reflects the status of the hazard analysis, design for safety, safety analysis and other relevant safety engineering activities.

Notes:

1. Guidance on the management of a hazard log is available through the KiD (White Book). A hazard log is a record of all identified accident sequences including the hazards and causes. It ordinarily also defines the status of each hazard in terms of hazard probabilty targets and instantiated or outstanding corrective actions.

2. The DID for a generic hazard log report is provided in the Annexes in Part 2 of this standard.

3. A common contractor and UK MOD toolset for hazard tracking might facilitate communication of hazards, but any tool should foremost be fit for purpose to aid hazard management.

9.3 Safety Requirements

9.3.1 The contractor shall clearly identify, record and track safety requirements throughout the contract.

9.3.2 The contractor shall document the process for identifying, recording and tracking all safety requirements and derived safety requirements in the SMP.

9.3.3 The contractor shall identify and track all safety requirements (including top level safety requirements) and derived safety requirements, and record them in the information set.

Notes:

1. Safety requirements ordinarily prescribe controls, mitigations or absolute properties of causes (eg failures), hazards and accidents. These will usually seek to define and reduce the probability of occurrence of causes, hazards and accidents, or will seek to reduce the impact of them if they do arise.

2. Derived safety requirements may result from, among other sources: legislation, UK MOD policy, regulations and standards appropriate to the scope of supply and scope of analysis; the domain and the technology used, relevant to the contract; and safety engineering and safety analysis activities. They may seek to: eliminate or substitute hazards to remove or replace them; apply engineering or administrative controls (including design integrity targets, human factors and process based) to isolate

people from the hazard or change their way of working; provide personal protective clothes and equipment to protect people from the hazard; or put in place monitoring for preventative or corrective action to rectify once a hazard has arisen.

3. Top level safety requirements are normally imposed by the UK MOD on the contractor, eg URD/SRD. However, relevant standards, policy and legislation might change during the contract life, requiring revision of the top level safety requirements.

4. Derived safety requirements are drawn from policy, etc. as often the UK 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, should be met using recognised procedures and it is important that they are recorded for traceability.

5. There might be cases where compliance with regulations and standards, eg for UK Conformity Assessed (UKCA) 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 should be documented in the SMP (ideally at ITT stage) for agreement by the UK MOD. If this is the case, then many of the detailed safety engineering requirements might not apply.

6. Data safety requirements are a subset of Programmable Elements (PE) safety requirements (see Def Stan 00-055) which, during the systems engineering and safety assessment activities, might emerge as derived safety requirements where PE contributes to a hazard or impairs mitigation of a hazard.

7. In applications containing Machine Learning, it might not be possible to directly track requirements through to implementation (see Def Stan 00-055). In such cases the intent of the decomposed requirement must be maintained and the approach to be taken documented in the SMP.

8. The adopted approach might not use the exact terms used in this standard, eg STPA uses 'unsafe control actions' rather than 'failure modes' and these terms might not be exact equivalents but fulfil similar purposes. Furthermore, the adopted approach might be conceptually different whilst still achieving a safe outcome. Where the contractor elects to utilise an alternative approach to that outlined in this standard they must justify that the intent of this standard had still been achieved in the safety case.

9.4 Safety Requirements Management

9.4.1 The contractor shall maintain records to show bi-directional traceability between each individual safety requirement or derived safety requirement, and the individual source of those requirements.

9.4.2 The contractor shall record the evidence which shows that the information set of all safety requirements has been validated as complete and consistent and that each individual safety requirement (including derived safety requirements) has been validated as being correct and unambiguous.

9.4.3 The contractor shall record the evidence which shows in the information set that each individual safety requirement (including derived safety requirements) has been met. Any requirements not shown to be met should be highlighted and appropriate justification provided.

9.4.4 The contractor shall record the evidence such that it can be included in, or referenced from, the hazard log.

Notes:

1. Traceability is fundamental to requirements management. 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 or is imprecise 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) and should be demonstrated for each individual safety requirement (including derived safety requirements) and the individual hazard, failure, legislative or policy clause, or other individual source of that safety requirement.

2. Safety requirements must not only be shown to have been achieved but must be shown to be complete, consistent and unambiguous. This includes validating that the safety requirements fully address the hazards or other sources from which they trace.

3. In PSS containing Machine Learning it might not be possible to explicitly trace requirements through to the software implementation. In such cases, alternative arguments relating to the implementation of safety requirements must be provided so that the validity of the hazard log is not undermined.

9.5 Design for Safety

9.5.1 The contractor shall undertake the design of the PSS so as to meet the safety requirements.

9.5.2 The contractor shall identify mitigation strategies to reduce safety risk and meet safety requirements.

9.5.3 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) Substitution.

c) Engineering controls.

d) Administrative controls (including human factors).

e) Personal protective clothes and equipment.

f) Monitoring for preventative or corrective action.

9.5.4 The contractor shall evidence the effectiveness of each mitigation strategy, including the application of the ALARP principle so far as reasonable practicable within the scope of contract, and shall record the rationale in the information set.

9.5.5 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.

9.5.6 The contractor shall identify derived safety requirements which represent the partitioning and allocation of safety requirements to parts of the PSS.

9.5.7 Where safety requirements are allocated to parts of the PSS as an explicit safety function, ie a safety control or protective equipment, derived design safety requirements shall be defined commensurate with the associated hazard. This shall include the minimum derived design integrity safety requirement or probability of failure for the safety function.

9.5.8 Where there are identified shortfalls in meeting safety requirements, the contractor shall ensure that at least one mitigation strategy for each of the associated hazards is satisified, so far as is reasonably practicable.

9.5.9 Where the safety requirement shortfall is indirect, eg a non-conformance with an agreed process standard, the contractor shall use engineering judgement to identify the most appropriate mitigation strategies and agree them with the safety committee.

9.5.10 The contractor shall record the results of applying the mitigation strategies and ALARP principles, the evidence that safety requirements are met, and any residual shortfalls against safety requirements in the information set.

Notes:

1. 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 KiD (White Book).

2. 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.

3. All safety requirements, including derived safety requirements, should be traceable to a system-level hazard. Where no clear linked hazard exists, the contractor might need to re-visit the Hazard Analysis to identify the missing hazard(s).

4. 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.

5. The term ‘safety requirement’ includes design and functional safety. This broad perspective is applied throughout this standard.

6. Where an in-service monitoring system is used for preventative or corrective action, such as health and usage monitoring or failure reporting, there needs to be an agreed process of ownership and management for retrieval and analysis of reported data. Retrieval and analysis will ideally not rely on access to proprietary data formats or interfaces.

7. Some regulations and standards require defined recording systems, eg accident data recorders or voyage recorders, to monitor for preventative or corrective action.

8. A safety function is a specific safety control or mitigation implemented within a PSS for which a target probability of failure must be set to determine the likelihhod of a safety risk arising. Design Integrity is a generic term intended to cover the rigour of process used to develop mechanical components as well as complex electronics, in place of an absolute probability of failure. This standard does not impose an integrity scheme as the intent is to use civil, open or other standards so far as possible. Requirements and guidance on addressing the Design Integrity of PE, 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.

9.6 Safety Analysis

9.6.1 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.

9.6.2 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.

9.6.3 The contractor shall use the results of the safety analysis to identify derived safety requirements.

9.6.4 The contractor shall document the results of the safety analysis in the information set.

9.6.5 The contractor shall ensure that the safety analysis results remain consistent with the design.

Notes:

1. 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 might 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. The safety analysis is therefore undertaken early in the life of PSS and will ordinarily be iteratively re-visited and updated as the design matures.

2. Not all safety analysis approaches (for example those making use of STPA) use design decomposition to identify credible causes of hazards, accidents or failure modes that contribute to a hazard or accident. Where alternative approaches are adopted all of the requirements of 9.6 will still need to be demonstrated albeit not through decomposition.

9.7 Failure Modes

9.7.1 The contractor shall identify all potential failure modes that might contribute to a hazard in the PSS, or in any known interfacing or interacting PSS, whether extant or planned.

9.7.2 The contractor shall ensure that the status of control of all identified failure modes that contribute to a hazard is visible throughout the contract.

9.7.3 The contractor shall include, in the information set, information about all identified failure modes.

9.7.4 The contractor shall include in the ISSS, information on the status of all identified failure modes.

9.7.5 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.

9.7.6 The contractor shall identify and justify in the information set the units used for likelihood of occurrence estimates.

9.7.7 The contractor shall employ systematic safety analysis processes for identification of failure modes which might contribute to a hazard in the PSS as defined in the SMP.

9.7.8 The contractor shall ensure that human factors are considered where they might be a contributory cause of a failure mode.

9.7.9 The contractor shall ensure that cyber security is considered where intentional or unintentional unauthorised electronic interactions might be a contributory cause of a failure mode.

9.7.10 The contractor shall ensure that systematic failures are considered where they might be a contributory cause of a failure mode.

9.7.11 The contractor shall ensure that the undesired impacts of normal functions are considered; this is especially important for contractors carrying out systems integration.

9.7.12 The contractor shall 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.

9.7.13 The contractor shall use qualitative estimates where it is not practicable to quantify likelihood.

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

9.7.15 The contractor shall consider human factors where they might provide risk mitigation.

9.7.16 The contractor shall consider cyber security controls where they might provide risk mitigation.

9.7.17 The contractor shall record the results of the failure mode assessment in the information set.

9.7.18 The contractor shall record all assumptions, data, judgements and calculations underpinning the failure mode assessment in the information set.

Notes:

1. 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).

2. Some approaches to identifying causes of hazards (eg those used when following STPA) may adopt different techniques to those listed in the Note above. Where this is the case, the contractor would still be required to meet the requirements of 9.7 albeit in the context of the adopted approach (eg in STPA it would be the identification of Unsafe Control Actions rather than Failure Modes).

3. 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 failure mode that does not contribute to a hazard, when used in different context, eg the PSS is 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.

4. All failure modes that have been identified must be documented (they form part of the information set), but they might 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 might be necessary to revisit the identified failure modes as the design progresses or requirements change.

5. 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.

6. New and rapidly advancing technologies have the potential to introduce novel failure modes; such systems might require closer monitoring and more frequent analyses to ensure early identification.

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

8. Def Stan 05-138 provides guidance for the levels of cyber protection required to be achieved by defence suppliers.

9. Def Stan 00-251 provides guidance for the achievement, assurance and management of human factors integration.

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

9.8 Risk Estimation

9.8.1 The contractor shall carry out risk estimation to determine systematically the severity of harm and likelihood of occurrence of PSS accidents, utilising the hazard analysis and safety analysis. This shall be recorded in the hazard log.

9.8.2 The contractor, with the agreement of the UK MOD, shall use justified qualitative estimates for reasonable worse case risk assessment, where it is not practical to quantify severity or likelihood.

9.8.3 The contractor shall determine residual risk once risk mitigation strategies have been realised, which might include human factors, cyber security controls or other failure mode mitigations.

9.8.4 The contractor shall 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 shall be done in terms of risk to life. It may be applied iteratively to refine the estimation of risk as the degree of uncertainty reduces throughout the life of a PSS. Use of risk criteria such as domain specific risk matrices might be required by UK MOD policy or regulation. Where the UK MOD identifies that a domain specific risk matrix should be used, the contractor shall employ this as applicable.

9.9 Risk and Compliance Evaluation

9.9.1 The contractor shall evaluate risk to life, for all identified hazards and accidents, and compliance with relevant legislation, standards, regulations and codes of practice, as defined in the SMP and record the results in the information set.

9.9.2 The contractor shall evaluate risks against the criteria agreed in the SMP.

9.9.3 The contractor shall record all assumptions, data, judgements and calculations underpinning the evaluations in the information set, such that they can be reviewed and reconstructed.

9.9.4 The contractor shall use the evidence produced to evaluate compliance with relevant legislation, standards, regulations and requirements derived from UK MOD policy.

9.9.5 The contractor shall 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 codes of practice, regardless of the scope of supply and scope of analysis.

9.10 Satisfaction of Requirements

9.10.1 The contractor shall carry out safety and systems engineering activities to provide evidence that all safety requirements, including derived safety requirements, have been met.

9.10.2 The contractor shall undertake systems engineering activities which are capable of detecting counter-evidence.

9.10.3 The contractor shall identify the most effective method, or methods, for showing satisfaction of requirements, or providing counter-evidence, and include this information in the SMP.

9.10.4 Whilst there might be general identification of techniques early in the process, the contractor shall ensure that the methods chosen are appropriate to the specific derived safety requirements identified.

Notes:

1. Ordinarily tests that evidence satisfaction of safety requirements are preferable. 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.

2. Counter-evidence indicates that the PSS might 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.

3. Some PSS, eg autonomous systems, might inherently display unexpected behaviour due to their design. It is important that when unexpected behaviour is observed that it is analysed to assess whether it is part of the design or counter-evidence (ie an unsafe behaviour).

10 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.

10.1 Information Set Safety Summary

10.1.1 The contractor shall produce an ISSS as defined in the SMP.

10.1.2 The contractor shall ensure that the ISSS contains sufficient information from the information set to enable a system integrator and a system operator to discharge their safety responsibilities.

10.1.3 The contractor shall ensure that the ISSS contains information on assumptions and limitations regarding the safe use of the PSS.

10.1.4 The contractor shall ensure that the ISSS includes a justification of the scope of the information provided.

10.1.5 The contractor shall ensure that the ISSS is delivered incrementally, as contracted and as defined in the SMP, to give the UK MOD visibility of progress in safety engineering and safety analysis.

Notes:

1. Guidance on the concept, use and applicability of ISSS and its relationship with safety case reports is included in Part 2 of this standard.

2. 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.

10.2 Safety Case

10.2.1 The contractor shall produce a safety case or safety cases for a PSS as defined in the SMP.

10.2.2 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.

10.2.3 The contractor shall ensure that the evidence for the safety case is drawn from the information set.

10.2.4 The contractor shall address safety throughout the life of the PSS within the safety case, to the extent required by the scope of contract.

10.2.5 The contractor shall provide evidence that supports claims for the verification and validation of all safety requirements, including evidence from sub-contractors.

10.2.6 The contractor shall provide evidence of compliance with relevant legislation, regulations, standards, policy and approved codes of practice.

10.2.7 The contractor shall ensure that the safety case identifies how to address any residual shortfalls in meeting safety requirements.

10.2.8 The contractor shall develop, maintain and refine the safety case as defined in the SMP. In developing the safety case the contractor shall address the full lifecycle (CADMID/T) of the PSS.

10.2.9 Where practicable, the contractor shall provide objective evidence.

10.2.10 The contractor shall provide diverse evidence, to ensure that that the overall safety argument is not compromised by errors or uncertainties in individual pieces of evidence.

10.2.11 The contractor shall demonstrate that the arguments and evidence in safety cases are sound, comprehensive and trustworthy.

10.2.12 The contractor shall justify the adequacy and suitability of the methods and techniques used for hazard analysis, design for safety, safety analysis and other relevant safety engineering activities.

10.2.13 The contractor shall develop, maintain and refine the safety case through the life of the contract.

10.2.14 The contractor shall 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:

1. Although only an accountable person is able to judge if risk is ALARP and tolerable, the safety case is to support this determination. 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).

2. The safety case might not be deliverable and, if the UK 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.

3. 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 case 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 UK MOD policy and DSA regulatory publications.

4. In developing the safety case, the contractor might 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 might need to be re-evaluated.

5. 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.

6. A single safety case approach might reduce complexity and thus improve comprehensibility. Conversely a single safety case might become oversized and as a consequence equally suffer from comprehensibility issues. A reasoned approach to the adoption of either a single case or multiple cases is advised. However, where possible, a single safety case approach is recommended.

10.3 Safety Case Reports

10.3.1 The contractor shall produce a safety case report or reports as defined in the SMP.

10.3.2 The contractor shall produce safety case reports that incorporate the key elements of the safety argument and provision of 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.

10.3.3 Where there are shortfalls in the evidence the contractor shall ensure safety case reports provide the rationale for operating the PSS, and the ways of mitigating the residual risk.

10.3.4 The contractor shall ensure that safety case reports contain information on assumptions and limitations regarding the safe use of the PSS.

10.3.5 The contractor shall produce command summaries, as contracted and as defined in the SMP, documenting the assumptions and limitations for safe in-service use of the PSS.

10.3.6 The contractor shall ensure that any related safety case reports or ISSS already in existence, and identified in the scope of analysis, are utilised and integrated as necessary.

10.3.7 The contractor shall deliver the reports incrementally, as contracted, to give the UK MOD visibility of progress in safety engineering and safety analysis. Early increments of the reports might not contain a complete argument for operation of a PSS, but will demonstrate intent and progress toward it.

Notes:

1. Where there are shortfalls in evidence and if the contractor cannot provide a rationale, then this should be raised with the UK MOD and other stakeholders so that the relevant accountable person and safety committee can take the necessary steps to assist the contractor in addressing the shortfalls.

2. 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 Annexes to Part 2. Further guidance on the concepts of UK MOD safety cases and safety case reports are available through the KiD.

3. The DAE use of safety assessments and safety assessment reports to support the Air System Safety Case is defined in MAA02.

4. Detailed requirements for safety-related report and summaries might vary with domain regulatory requirements.

11 Supply and Change Management

11.1 Build State Definition

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

11.1.2 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.

11.1.3 The contractor shall 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. This should include a list of critical items whose related failure modes can result in serious injury or loss of life.

11.1.4 The contractor shall ensure that the build state definition is specific to each delivered instance of a PSS, so that specific instance is properly managed.

Notes:

1. 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 might migrate from the initial contractor to the support organisation as the PSS evolves through life; in some cases responsibility for the build state might rest with the UK MOD.

2. Def Stan 05-057 addresses configuration management, including providing domain-specific requirements.

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

11.2 Change Control

11.2.1 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 might 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.

11.3 Planning for Change

11.3.1 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.

11.3.2 The contractor shall consider all relevant change drivers, including modified operating requirements, the availability of new technologies, as well as supply chain issues 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:

1. Although the contractor might 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 might 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 UK MOD to judge which improvements can be implemented in order to comply with its obligations, and meet its operational commitments.

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

11.4 Safety of Changes

11.4.1 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.

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

11.4.3 The contractor shall review and update the safety case and safety case report, as defined in the SMP, to ensure that they remain valid.

11.4.4 The contractor shall update the design where there are agreed changes to the safety requirements, updating the information set accordingly.

11.4.5 The contractor shall update the hazard analysis and safety analysis as necessary for all changes, both intended and unplanned, updating the information set accordingly.

11.4.6 Following any change which has an adverse effect on safety, the contractor shall propose, agree and implement further revisions to the design so as to preserve safety.

Notes:

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

2. Some contractors might adopt fast-paced development lifecycles (eg DevOps). Change management in such environments requires greater emphasis to preserve safety.

11.5 Safe Update

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

11.5.2 The contractor shall supply appropriate installation instructions to enable changes to be made safely to the in-service PSS.

11.5.3 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.

Notes:

1. 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.

2. Automated or highly-efficient mechanisms for safe updating might assist with maintaining the fast pace of change expected in modern military systems.

11.6 Monitoring Change

11.6.1 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 might have undesired safety impacts.

11.6.2 Where undesired safety impacts are identified, the contractor shall notify the relevant stakeholders and, where practicable, recommend mitigation to control risk to life.

11.6.3 To ensure visibility of changes, the contractor shall agree with the UK MOD the monitoring channels to be used; these shall be recorded in the SMP.

Note. The contractor might 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 might 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.

11.7 Incorporating Change

11.7.1 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.

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

11.7.3 The contractor shall assess supplied PSS, together with installation instructions, and develop and implement plans for safe installation and maintenance.

11.7.4 The contractor shall 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.

11.7.5 Where temporary modifications have been made to manage risk the contractor shall ensure that they are removed once a permanent resolution has been implemented.

11.7.6 The contractor shall 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:

1. In many PSS cases the contract development and manufacture phases will overlap the in-service phase of the CADMID/T lifecycle. These clauses might 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 might 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.

2. 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 loss of accuracy in the safety argument if it is not updated, possibly leading to an incorrect estimation of risk.

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

4. UK MOD necessarily has control over in-service requirements. It will be the accountable person who makes decisions on implementation of mitigation and responsibility for risk to life.

5. 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.

Safety In-Service

Notes:

1. 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.

2. The boundary between what is provided in support of the in-service PSS and a contractor managed service will depend on the scope of analysis or scope of supply and the in-service/operational scenarios. This boundary will 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.

3. Regulators might 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.

4. Defence contractors should be aware that, in general, they cannot benefit from any disapplication, exemption or derogation from statutory requirements granted to Defence where they control activities, but, there might be exceptions to this and where this is the case, the responsibilities for complying with Defence Regulations shall be specified in contractual arrangements. Significantly though, defence contractors cannot claim Crown Immunity from prosecution.

12 Supporting Systems In-Service

12.1 Management of Safety-Related In-Service Data

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

12.1.2 The contractor shall 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:

1. 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 might be integrators or responsible for interfacing PSS.

2. Hazards on one PSS in a system might result in new hazards that manifest in another interfacing system. Interfacing with other stakeholders (UK MOD and other contractors) need to be agreed. This might require changes to the scope of contract and management through the SMP.

3. This standard cannot place requirements on the UK MOD. Any contractor requirements for data should be agreed in the scope of contract and captured in the scope of analysis. If, for example, a digital twin or health monitoring and reporting system is employed, then supply of data should be agreed at scope of contract.

12.2 Monitoring, Reporting and In-service Data Analysis

12.2.1 The contractor shall define and operate a process for collecting, analysing and documenting safety-relevant in-service data across all DLOD, which might include, but is not limited to: usage and environment; accident and incident reporting; and defect, error and failure data, including human errors.

12.2.2 The contractor shall review the safety case, in 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.

12.2.3 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 UK MOD, shall implement those actions within their sphere of responsibility.

12.2.4 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.

12.2.5 The contractor shall define and operate a process for collecting and analysing incident, accident and near miss reports, and comparable data from other operations available to the contractor or supplied by the UK MOD.

12.2.6 The contractor shall analyse all collected data, addressing both individual events and longer-term trends, to identify root causes which require action.

12.2.7 The contractor shall monitor and report changes to relevant safety legislation to ensure that PSS operation remains compliant or that appropriate remedial action is identified.

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

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

Notes:

1. These clauses require coordination between operations and support, regardless of whether the support is provided by UK 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 UK MOD.

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

3. Some PSS, eg those with Machine Learning components, might create significant amounts of data. Furthermore, some systems might operate remotely and it might not be obvious if and where an incident has occurred. In such cases the automated logging and analysis of data will be a vital tool in the effective monitoring and reporting of safety.

4. 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.

5. Examples of information sharing might include PSS failure rates encountered by other stakeholders. Such information might require sanitation but might still provide valuable In-Service data to support safety improvements.

6. Using common data standards and repositories will improve the opportunities for enhanced safety modelling (eg through digital twins) and thus provide greater efficiency and efficacy of in-service safety management.

12.3 Remedial Action

12.3.1 The contractor shall implement remedial actions to preserve or improve safety, agreed with the UK MOD and prioritised accordingly.

12.3.2 The contractor shall plan remedial actions taking into account the need for efficient change management, to enable updates to the in-service PSS with minimum disruption.

12.3.3 The contractor shall 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:

1. 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 accountable person.

2. 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.

3. The safety committee will prioritise remedial action. The organisational arrangements will be defined in the SMP.

13 Service Provision

Note. These clauses apply only when the contractor is supporting the UK MOD by providing a Service, which might 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 might be domain-specific requirements or regulations. These clauses will not be applicable if the scope of contract does not include service provision.

13.1 Safety Case Report

13.1.1 The contractor shall produce a safety case report and command summary and deliver them to the UK MOD for approval before commencement of services.

13.1.2 The contractor shall maintain the safety case, safety case report and command summary so they are accurate representations of the service.

13.1.3 The contractor shall produce command summaries so that each provision of the service can be properly assessed and controlled in terms of risk.

13.1.4 The contractor shall provide information to support domain specific processes providing essential information for the accountable person responsible for the service to manage risk to life.

Notes:

1. 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 might lead to the production of more than one command summary. A command summary might therefore, as an example, pass design (equipment) safety case information to the operators. This would state how to use it safely and detail what they need to know to further assess the operational safety.

2. The command summaries and safety case reports will be reviewed and accepted by the UK MOD, prior to commencement of operations. This may include regulators, accountable persons or other UK MOD stakeholders.

3. In the DAE, the operating duty holder is responsible and accountable for the Air System Safety Case. All duty holder facing organisations (ie those providing evidence of PSS safety to the duty holder) have a responsibility iaw RA1020 in the management of risk to life.

13.2 Service Provision Planning

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

13.2.2 The contractor shall 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.

13.2.3 The contractor shall 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 accountable person and relevant stakeholders.

13.2.4 The contractor shall 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.

13.2.5 The contractor shall ensure that the communications plan, detailed in the SMP, includes processes for delivery of in-service data and build state definition.

13.2.6 The contractor shall provide information to those not employed as part of the provision of the service about relevant undertakings, where this might affect their health and safety. How this will be achieved shall be included in the relevant plans.

13.2.7 The contractor shall provide access to health and safety advice relating to the service, and consultation on the risks to employees, contractors and any other people who could be affected by them.

Notes:

1. These plans may be part of the SMP or in a separate plan as agreed with the UK 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.

2. Various JSP may also be consulted for UK MOD policy and direction for safety within service provision of trials, ranges and more. For example, JSP 822 provides Defence direction and guidance for training and education, which includes Defence direction on the safe system of training.

13.3 Risk Management

13.3.1 The contractor shall support the UK 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 SMP.

13.3.2 The contractor shall cooperate with the accountable persons for interfacing or interacting services or operations to enable effective management of risk to life.

13.3.3 Where necessary and with the accountable person's agreement, the contractor shall implement immediate action to manage risks to life until a longer-term resolution is identified.

Notes:

1. As these requirements relate to a service upon which a UK MOD military capability might 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 UK MOD to do so). This is necessary and appropriate when the contractor has responsibility for a service that might contribute directly to the in-service risk to life and will necessitate demonstrable compliance with the ALARP principle. This will be agreed with the UK 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 UK MOD accountable person endorsed through the mechanism of the UK MOD SMS.

2. Guidance on ALARP in a military equipment context is available on the KiD.

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

4. 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.

Section 3

Normative References

1 The publications shown below are referred to in the text of this standard. Publications are grouped and listed in alpha-numeric order.

Note: 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.dstan.mod.uk>** for all other users. All referenced standards were correct at the time of publication of this standard (see 2, 3 & 4 below for further guidance), if you are having difficulty obtaining any referenced standard please contact the UK Defence Standardization Help Centre in the first instance.

Def Stans

Number	Title

STANAGs

Number	Title

Allied Publications

Number	Title

Other References

Standard Type	Standard Name

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 In consideration of clause 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 identification of standards is as defined in the ITT or contract.

4 DStan can advise regarding where to obtain normative referenced documents. Requests for such information can be made to the UK Defence Standardization Help Centre. Details of how to contact the Help Centre are shown on the outside rear cover of Defence Standards.

Definitions

For the purpose of this standard, ISO/IEC Guide 2 ‘Standardization and Related Activities – General Vocabulary’ and the definitions shown below apply.

Definition	Description
Accident	An event, or sequence of events, that: causes unintended harm, such that a person is killed or suffers an injury. An accident sequence will need to consider the functional safety of equipments/systems involved.
ALARP	"ALARP" is short for "as low as reasonably practicable". "SFAIRP" is short for "so far as is reasonably practicable". The two terms mean essentially the same thing and at their core is the concept of "reasonably practicable"; this involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled.
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	Encompasses all military and civilian organisations undertaking Defence Aviation activities on the UK Military Aircraft Register.
Derived Safety Requirement	A safety requirement which is derived from a design or analysis activity.
Design Integrity	The extent to which the design, including PE, 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 has a personal level duty of care for the personnel under their command; those who, by virtue of their activities, come within a Duty Holder’s area of responsibility, and the wider public who may be affected by their operations. They are thus legally accountable for the safe operation of systems in their area of responsibility and for ensuring that risks to life are ALARP and Tolerable.

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	An item, event, activity, or situation with the potential to cause: • injury, ill-health, or death; • damage to or loss of equipment or property; or • damage to the environment - (An intermediate state where potential for harm exists)
Hazard Analysis	The process of describing in detail the hazards and accidents associated with a system, and defining accident sequences.
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, accident sequences 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.
Human Factors	The interaction between; people and people, people and machine, people and procedures and people and the environment. The understanding and application of physical, physiological and behavioural factors in the design, operation, maintenance and management of systems to optimise safety, performance and capacity. It is multidisciplinary, and embraces individuals, teams and organisations.
Incident	The occurrence of an event that might have progressed to an accident but did not cause injury or damage but had the potential to do so.
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: a) Usually allocated from PSS systems engineering and safety assessment activities; b) Derived from the choice of standards to meet the PE Design Integrity, or; 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	Products, Services and/or Systems (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 to Life addresses fatality and injury, but excludes damage to assets or the environment where no harm results. People should only be exposed to risk of harm where some defined benefit is expected and where the risks are adequately controlled.
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	Process that encompasses systematic hazard identification; risk assessment; hazard risk matrix; risk reduction and risk monitoring, evaluation, and review.
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	A systematic and independent examination to determine whether safety related activities and related results comply with planned arrangements and whether these

	arrangements are suitable to achieve safety objectives and are implemented effectively. The Safety Audit may be used to make recommendations to improve the subject activity.
Safety Auditor	An individual or team that undertakes safety audits.
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 PSS is safe for a given application in a given environment. It is through-life, pan-Defence Lines of Development and addresses a combination of the physical components, procedures and human resources organised to deliver the capability.
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; this includes design and functional safety.
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.
Accountable Person	Accountable Person, is a person holding Accountability for the activity who is empowered to make safety-related executive decisions.

Abbreviations

Abbreviation	Description
ALARP	As Low As Reasonably Practicable
ARP	Aerospace Recommended Practice
ASEMS	Acquisition Safety & Environmental Management Systems
CADMID/T	Concept, Assessment, Demonstration, Manufacture, In-service, Disposal/Termination
CSA	Contractor Safety Auditor
DAE	Defence Air Environment
Def Stan	Defence Standard
DID	Data Item Description
DSA	Defence Safety Authority
DStan	UK Defence Standardization
ESL&S	Equipment, Services, Logistics and Support
FMEA	Failure Modes Effects and Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FPGA	Field Programmable Gate Array
FRACAS	Failure Reporting Analysis And Corrective Action System
GFX	Government Furnished Equipment (GFE) or Assets (GFA)
IET	Institute of Engineering and Technology
ISA	Independent Safety Auditor
ISAWG	Independent Safety Assurance Working Group
ISO	International Organisation for Standardisation
ISSS	Information Set Safety Summary
ITT	Invitation to Tender
JSP	Joint Service Publication
KiD	Knowledge in Defence
MAA	Military Aviation Authority
MIL-STD	Military Standard
MOD	Ministry of Defence

MRP	MAA Regulatory Publications
PE	Programmable Elements
PLD	Programmable Logic Devices
POSMS	Project Oriented Safety Management System
PSS	Products, Services and/or Systems
RGP	Relevant Good Practice
SRD	System Requirement Document
SMP	Safety Management Plan
SMS	Safety Management System
STPA	System Theoretic Process Analysis
UKCA	UK Conformity Assessed
URD	User Requirement Document
HSE	Health and Safety Executive
DLOD	Defence Lines of Development
DevOps	Development and Operations
ACOPs	Approved Code of Practice
DO	Document Order

Changes since previous issue

The changes incorporated in this issue are shown below. For more information please contact DStan through the UK Defence Standardization Help Centre. Details of how to contact the Help Centre are shown on the outside rear cover of Defence Standards.

Clause	Page	Change	Change Reason
All Part 1 Requirements	Part 1 inclusive	All clauses where previously "should", amended to "shall"	Avoid commercial ambiguity and promote due diligence and interpretation to be applied
Format Change	All	Requirements numbering has moved up 2 in number. For example 8.1 now reads 6.1	Issue 8 uses an updated template to Issue 7.
Part 1	All	Information pack containing Scope, triage of review feedback received and overlay document detailing changes from issue 7 to issue 8	DStan 00-056 briefing pack - available on request from DStan

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

UK Defence Standardization Help Centre

Please direct any enquiries via the Standardization Management Information System (StanMIS) Help Centre.

To access the StanMIS Help Centre please select either http://stanmis.gateway.isg-r.r.mil.uk/ (for MOD and industry users with MOD Core Network (MCN) access) or https://www.dstan.mod.uk/StanMIS/ (for all other users), and, after logging in, please follow the link to the Help Centre. If required, users can also register for an account from the login screen.

File Reference

The DStan file reference relating to work on this standard is 01410/2021.

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.gateway.isg-r.r.mil.uk/index.html, 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.