Ministry of Defence

Defence Standard 00-056 Part 02

Issue 6 **Date: 14 October 2023**

Safety Management Requirements for Defence Systems

Part: 02 : Guidance on Establishing a Means of Complying with Part 1

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 2 Issue 6 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.

There has been a substantial format change (issue 6 uses a different template to issue 5 and DStan do not allow the use of appendices). A major change to part 2 is the introduction of a generic tailoring and compliance matrix. There are many minor changes to part 2, the briefing pack available from DStan for this update provides an overlay document that details all changes conducted from issue 5 to issue 6.

HISTORICAL RECORD

This standard supersedes the following:

Def Stan 00-056 Pt 2 Iss 5

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 2: Guidance on Establishing a Means of Complying with Part 1

0 Introduction

0.1 The purpose of this part of the standard is to provide guidance for Part 1. It aims to support acquisition organisations in setting safety requirements on contractors that enable procurement of Products, Services and/or Systems (PSS) compliant with safety legislation, regulations and policy.

Notes:

1. Defence Standard 00-056 Part 1 Issue 8 is extant with this issue of Part 2.
2. Abbreviations used in this standard, eg PSS, are to be considered as singular or plural in context with their use in the text.

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

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

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

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

0.2 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. In accordance with general guidance provided by the Health and Safety Executive (HSE), and as defined in Defence Safety Authority (DSA) Joint Service Publication (JSP) 815, Defence Safety Management System, the UK MOD will discharge this duty by ensuring that all identified risks to life are reduced to levels that are As Low As Reasonably Practicable (ALARP) and tolerable, unless legislation, regulations or UK MOD policy imposes a more stringent standard.

0.3 Contractors who supply PSS to the UK MOD are subject to legal duties, which may vary with the place of manufacture and supply or operation.

0.4 The requirements are grouped into three main areas, safety management, safety engineering, and safety in-service. The safety management clauses should always apply, but the other clauses will depend on the scope of contract. Safety engineering clauses will apply to projects involving design and development work, but would also be expected to be applied (at least in part) to support contracts which involve design and development, eg upgrades.

0.4.1 The clauses can be tailored at a more detailed level, depending on the scope of contract, standards or the approach to regulation in a particular sector. Guidance is given on tailoring in Annex A to this part, but this is likely to be project dependent. Tailoring can be done only by the UK MOD, or as proposed by industry and with the agreement of the UK MOD; and must reflect the relevant domain DSA regulations and publications.

0.4.2 An essential element of safety management systems is the recording of evidence in support of safety cases (or safety assessments) that must be retained for audit and assurance or as a legal or regulatory requirement. Some data will be documented in the Safety Management Plan (SMP) and other data retained as part of the information set. Throughout this standard, unless otherwise specified, the data to be recorded or documented must be retained within the information set.

0.5 Part 1 of this standard may be applied to address the damage to (or loss of) PSS, environmental damage elements, or the management of environmental issues where risk to life results. Safety management must include the safety issues relating to the environment (eg health and safety risk from use or spillage of hazardous materials). There must also be consideration of any common issues by cross-referencing the results of hazard identification and environmental features identified from the environmental management system.

0.5.1 On UK MOD procurement projects, a common approach is usually taken with safety and environmental management systems and, in many cases evidence or plans are compiled into a single document, eg a safety and environmental management plan. For clarity, this standard refers only to safety management. Environmental management is addressed within Defence Standard (Def Stan) 00-051.

0.6 This part of the standard provides guidance on establishing a means of compliance with the requirements for achievement, assurance and management of safety, including overarching objectives and principles.

0.7 This standard is applied to all PSS procured to meet diverse capabilities across all Defence systems and may necessitate tailoring. The UK MOD may tailor the application of clauses and sub-clauses of this standard or, in consultation with the contractor, agree tailoring to reflect the scope of contract which includes:

a) Scope of Supply; the deliverable PSS and information. The introduction of scope of supply is intended to identify what is delivered and not delivered to the UK MOD.

b) Scope of Analysis; safety relevant activities to be undertaken, which may apply to more than or less than, the scope of supply. The introduction of the scope of analysis is intended to facilitate the clear definition of contractor's responsibilities.

0.7.1 This standard must cover a broad range of contractual scenarios, including contracts providing support to operations eg a PSS delivered and maintained by contractors in an operational environment. For all PSS to which this standard applies, an accountable person will retain responsibility and accountability for the risk to life, and would take account of this contracted PSS delivery, in the risk analysis. The use of Contractors on Deployed Operations (CONDO) is a concept of utilising contractors during operations and exercises to support and augment the capability of UK's Armed Forces as part of the civilian component of the military force. The policy and processes to be followed in the deployment of CONDO are covered by other publications and standards, such as Def Stan 05-129.

0.7.2 To address a broad range of scenarios, Part 1 of this standard sets out safety requirements which require application in any given situation. The Part 2 guidance helps to analyse the different circumstances which can arise and to provide rationale for compliance with the standard.

0.7.3 Guidance on tailoring is in Annex A which supports the application of Part 1 of this standard to capture the safety requirements for a specific project. It can be particularly effective where there is an urgent operational need for contractors to supply or modify PSS.

0.8 This standard identifies requirements for the achievement and demonstration of safety by a contractor who has a safety management system in place. A Safety Management System (SMS) provides the framework for the contractor's organisation to direct and control its safety management activities, including the organisational structure, processes, procedures, techniques and methodologies.

Contents

1 Scope and Applicability

1.1 Def Stan 00-056 Part 1 specifies the requirements for achieving, assuring and managing the safety of PSS defined by the scope of contract.

1.1.1 Part 2 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 Part 2 also provides guidance on tailoring and contracting with a matrix enabling acquisition staff to tailor the requirements to meet their PSS profile (Annex B).

2 References

2.1 Normative References

2.1.1 This standard is for guidance, therefore 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.
DEF STAN 00-051 2.	Environmental Management Requirements for Defence Systems, Part 1 and
DEF STAN 00-055	Requirements for Safety of Programmable Elements (PE) in Defence Systems.
DEF STAN 05-057	Configuration Management of Defence Materiel.
DEF STAN 05-129	Contractors on Deployed Operations.
DEF STAN 05-138	Cyber Security for Defence Suppliers.
IEC 61511	Functional safety - Safety Instrumented Systems for the Process Industry Sector.
ISO 9001	Quality Management Systems.
ISO 26262	Road Vehicles – Functional Safety.
ISO 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.
JSP 815	Defence Safety Management System.
MAA01	MAA Regulatory Principles.
MAA02	MAA Master Glossary.
MAA03	MAA Regulatory Process.
MRP	MAA Regulatory Publications.
MIL-STD-882-E	Department of Defense Standard Practice - System Safety.
SAE ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.
SAE ARP 4754	Guidelines for Development of Civil Aircraft and Systems.

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 definitions that are diverse. Where there is divergence, the contractor will need to agree a glossary with the UK MOD and document the outcome, eg in the Safety Management Plan (SMP).

3.2 Mandatory Requirements

3.2.1 Part 2 of this standard is primarily for guidance only. Though "shall" and "should" are detailed throughout this document they are not used in the same context as for Part 1 and are used interchangeably. Therefore "shall" and "should" in part 2 are not to be interpreted for precedence or necessity.

3.2.2 Where, in Part 2, a clause contains "mandatory" (e.g. Tailoring matrix) or within a clause it explains that it is to be "mandated", the rationale for proposed deviation from the guidance is to be included within the tailoring proposed for the associated Part 1 clause(s), for subsequent approval by the Authority.

4 UK MOD Policy

4.1 The role of Def Stan 00-056 is to place requirements on contractors to enable UK MOD to meet its obligations for safety management as defined by the Secretary of State's policy statement and amplified by the Defence Safety Authority publication JSP 815, Defence Safety Management System. UK MOD policy requires compliance with relevant legislation, policy, regulation and standards, both civilian and military. Codes of practice, mandated procedures, advice and guidance are also provided to support UK MOD staff in delivery of safe PSS.

4.2 The contractor is expected to derive safety requirements arising from relevant UK MOD policy. The UK MOD will assist the contractor to identify relevant UK MOD policy, including standards and regulations. DE&S mandates the Acquisition Safety and Environmental Management System (ASEMS) that includes the Project Oriented Safety Management System (POSMS) which is available from the UK MOD ASEMS website http://www.asems.mod.uk. POSMS contains guidance on defining safety requirements.

4.3 This standard requires contractors to meet their obligations with relevant aspects of legislation and regulation, and to document the applicable legislation and regulation in the SMP.

Note. It is assumed that a competent contractor will either already be aware of such legislation and regulations, or is in a position to identify it, particularly where they are selecting options for the PSS solution.

5 Products, Systems and Services

5.1 Most UK MOD acquisitions result in a delivery of an article which is intended to be operated; this standard refers to such artefacts as products. Products will range in size and type. Example products are: a chemical sensor, a winch, a software application and a ship. However products usually need additional elements, such as supplies, crew, weapons, etc. in order for them to be considered as an in-service/operational system.

5.2 Military systems are composed of elements such as products, services and possibly other systems. A system also includes Defence Lines of Development (DLOD), ie training, equipment, personnel, information, concepts and doctrine, organisation, infrastructure, logistics and interoperability. Military systems will usually be operated by military personnel, although civilian supported operation also occurs. A system is usually intended to be operated in a defined environment, to achieve a particular capability. An example system is a warship.

5.3 A military service is provided by the operation or use of a system. Thus a contractor may operate a system and provide a service, eg a network service. In this case, the contractor may have some responsibility for supporting in-service safety, ie the availability of the service has to be considered in the risk to life and health of UK MOD and civilian personnel. However, when this standard is applied, it will always be the case that there is a UK MOD accountable person who has ultimate responsibility for risk to life. As the range of scenarios for providing PSS is very large, there may be conflict between the legal obligations on contractors, eg under the Health and Safety at Work etc Act 1974, and the

operational imperative. This standard expects that the scope of contract will define contractual clauses which will be agreed between the UK MOD and the contractor to ensure these issues are managed.

5.4 It is important to note that:

a) The UK MOD sometimes uses contractors on deployed operations to provide operational support. This standard does not define rules or procedures for such cases as these are addressed by other UK MOD procedures and policies.

b) The distinction between different PSS impacts on the safety engineering and management processes. For any PSS, a contractor will be able to identify and manage some hazards, eg the possibility of trapping hands in a winch. Other hazard identification will depend on the way the PSS is used or employed. The contractor will be reliant on the defined requirements in the scope of contract, eg Concept of Use/Employment/Operations (CONUSE/CONEMP/CONOPS) or User/System Requirement documents (URD/SRD).

6 Summaries, Information Sets and Safety Cases

6.1 The UK MOD generally acquires PSS which are intended to form part of more complex systems, ordinarily described by the UK MOD within associated Concepts of Employment / Use / Operations (CONEMP/CONUSE/CONOPS). The system integrator will need to be provided with relevant information to enable them to assess the overall risk to life. Such information could include the failure modes associated with the use of the PSS, as well as usage constraints. This relevant information may be captured in the information set and summarised in an Information Set Safety Summary (ISSS) but not used in the primary PSS safety case. An ISSS captures a snapshot of the information set at a given point in time for a given purpose. Similarly, a safety case report and command summary are a snapshot of the PSS safety case at a given point in time for a given purpose.

6.2 This standard has introduced the information set, which identifies the totality of information produced in support of the PSS. However, it would be impractical to deliver all such information to all relevant Stakeholders. Hence, the standard introduces the concept of an ISSS, to represent the extracted safety information, required by the contract, to be delivered by the contractor to the UK MOD and other Stakeholders.

6.3 Together the ISSS, safety case report and command summary represent the deliverables that communicate safety information to the relevant stakeholders. The safety case report and ISSS address distinct purposes and may not both be required depending on the scope of contract. The intent of these deliverables are:

a) The command summary is intended to provide essential safety information on the PSS for the individual who has to manage in-service/operational risk. The command summary draws on information in the safety case report.

b) The ISSS is intended to provide sufficient information to enable PSS to be safely integrated into a higher level PSS, or interfaced to a peer PSS. The ISSS summarises the technical properties of the PSS that are relevant to safe integration/interface where the contractor cannot directly assess risk to life. The ISSS would be used by the integrator of the higher level PSS to support their safety assessment and contribute to the top level safety case.

c) The safety case report is intended to summarise the arguments and evidence of the safety case for a given application in a given operating environment, for a given period of time.

6.4 For some Products and Services an ISSS may be sufficient to support the overall system safety case. As an example, a commercial off the shelf (COTS) winch ISSS may contain sufficient information relevant for Risk of Life in the wider context. This would include Hazards, eg trapping hands, failure modes, eg locking or sticking and technical information, eg load limits. In general, the ISSS could be used to help define limitations of use for a defined capability.

6.5 A system safety case needs to place the COTS winch in context for the specific in-service use, eg replenishment at sea or deployment of a lifeboat. The ALARP principles would then be applied in the system context that may lead to a safety guard fitted around the winch to mitigate a trapped hands hazard. In this case there may only be a safety case report for a lifeboat system, supported by a number of ISSSs, one of which will be for the COTS winch.

Note. In the DAE, the aviation Duty Holder or Accountable Manager (Military Flying), as defined in MAA02 and RA1020/RA1024, are the designated posts who can accept risks as being ALARP and tolerable.

6.6 This standard places requirements on contractors to collaborate with stakeholder interfaces (eg integration/system of systems), as defined in the scope of contract, and may also place requirements on the contractor to collaborate in risk management with these stakeholders.

6.7 The scope of contract may include requirements on contractors to design multiple PSSs to be operated in a system of systems, eg in the case of a Naval support vessel controlling a set of different unmanned vehicles (eg surface, sub-surface and air). Technical requirements would apply to each system (vessel and different unmanned vehicles). This would inform the ISSS and safety case report for each system, ie each type of unmanned vehicle integrated with the support vessel. Therefore, for a particular configuration of unmanned vehicles which are integrated with a support vessel, a safety case and safety case report could be constructed for the deployed system of systems.

7 Invitation to Tender and Response

7.1 Guidance on how the UK MOD approaches the compilation of an ITT for generation of the top level safety requirements can be found in POSMS. Prior to ITT, the UK MOD will carry out any necessary tailoring of the standard. Bidders would then respond to the ITT. Following the selection, the potential contractor may negotiate with the UK MOD and agree further tailoring compliant with this standard. The resulting acceptable means of compliance of the selected contractor will be documented in the scope of contract and detailed in the SMP.

7.2 In the lead up to a project ITT, the UK MOD will identify the required capability for the deliverable PSS, eg in the URD/SRD. Other key information that the UK MOD may provide the contractor, to assist in the production of a tender response, will be guided by POSMS. This information will also include the initial definition of the scope of contract.

7.3 The ITT will require the contractor to provide a compliance statement or matrix against the tailored requirements. Guidance on tailoring, and use of the tailoring compliance matrix, is given in Annex A.

7.4 Contractors must note that only the UK MOD has the authority to tailor this standard; although this does not prevent the contractor proposing alternative means of compliance during the pre-contract negotiations. It must be understood that a detailed and unambiguous compliance matrix may be a significant discriminator in selection of a preferred bidder and subsequent contract award.

7.5 A key safety document is the contractor's draft SMP; this is normally included in the ITT response. A draft SMP is an excellent method of indicating a contractor's safety management capability, understanding and competence.

7.6 The level of detail to include in a draft SMP or ITT response will be dependent on the scope of contract and the top level safety requirements. POSMS provides guidance on what the UK MOD may require. Where necessary, the ITT response or draft SMP could also identify:

a) Where there is uncertainty as to the applicable legislation and regulations, eg new materials;

b) Where the contractor cannot disclose required information, eg intellectual property rights or international traffic in arms regulation, the contractor will need to define how such aspects are to be addressed.

c) Where Government Furnish Information / Equipment / Services / Facilities (GFX) will need to be incorporated, the contractor's requirement for access to relevant safety information.

7.7 The UK MOD may request other preliminary deliverables to support an ITT response, such as:

a) Draft hazard log report: particularly if the PSS is established, eg using Military off-the-Shelf (MOTS) or COTS.

b) Draft safety case report: where an outline safety argument and type of evidence is a key discriminator for selection.

c) Risk register: where uncertainties regarding the identification and satisfaction of safety requirements might significantly impact contract timescales or cost are identified.

7.8 It will be for the UK MOD to determine if a contractor's ITT response to safety would be considered acceptable.

8 Scope of Analysis

8.1 This standard recognises that, in modern acquisition scenarios, there may be a difference between what PSS the contractor delivers and what they are required to analyse. The introduction of the scope of analysis in this standard is intended to enable this difference to be articulated.

8.2 The scope of analysis defines the contractor's responsibilities with regards to the application of the safety analysis processes, ie scope of hazard and safety analysis. The scope of analysis will typically cover everything which can affect the safety of the PSS, including any ancillary material which could influence safety; eg operating procedures. This standard identifies three levels of analysis:

a) Full, where the scope of analysis is for the PSS, plus safety-relevant ancillary material. This is appropriate where the contractor has sufficient knowledge and visibility of the in-service operation of the PSS to be able to carry out the full safety process up to, but excluding, acceptance of risk to life, which can be undertaken only by the UK MOD.

b) Enhanced, where the scope of analysis exceeds what the contractor is supplying. This may occur when the contractor is a system integrator, or where the UK MOD specifically contracts for additional elements, such as legacy systems to be analysed. In some cases, the contractor may undertake the complete safety analysis of a PSS which they did not produce.

c) Reduced, where the scope of analysis is less than what the contractor is supplying. This might occur if it is more efficient for the UK MOD to contract a system integrator to undertake the overall system safety management of a number of PSSs, not all of which are being developed by the contractor.

8.3 At the ITT stage, the UK MOD will identify the level of expected scope of analysis but the level may change as it is partly dependent on the contractor's knowledge and response to the ITT. The contractor will need to ensure that this is reflected in the safety activities documented in the SMP. It may be necessary to modify the scope of analysis as the contract matures, and this may require amendment to the contract.

9 Scope of Supply, Documentation

9.1 This standard mandates certain safety-related documentary deliverables; these form a major element of the scope of supply. The UK MOD will specify deliverable documents, and their links to project milestones, in the ITT or contract. The SMP must detail the form and content of the deliverables and the delivery schedules.

9.2 The Data Item Descriptions (DIDs), that includes description, purpose and format of safety document deliverables, are at Annexes C to K inclusive. These DIDs may be tailored by the UK MOD either to meet PSS requirements or where an agreed alternative, acceptable means of compliance is offered by the contractor.

9.3 Under certain circumstances, such as an emerging operational requirement for the PSS, the UK MOD may require additional documentary deliverables. It may be possible for these to be extracted from the information set. An example is a Failure Modes and Effects Analysis for a low-level component such as a valve or a human factors analysis for a new operating procedure. It would be expected that the UK MOD will ask for additional safety-related documentary deliverables only where they have a clear role in supporting safety of the defence activity, eg for a system integrator or a training facility.

10 Use of Other Standards

10.1 The UK MOD may allow contractors, as part of an agreed means of compliance, to use alternative standards.

10.2 It is likely that other standards will not address the UK MOD's specific requirements. It will therefore be necessary for the UK MOD and/or contractors to undertake a gap analysis for the adoption of standards that they intend to use against the requirements of this standard. It would then be necessary to identify how any requirement shortfalls, termed Military Deltas, would be addressed in the SMP. Guidance on open standards and Military Delta is given in Annex L. The Military Delta could include:

a) Omissions; such as the absence of a key safety requirement, eg independent safety audit.

b) Conflicts; where some standards may require safety features to be incorporated which conflict with operational necessity and where degraded functionality would be unacceptable.

c) Additions; where other standards impose safety requirements over and above those required by this standard, due to the limited way the military deploys the PSS, that could result in unnecessary effort and cost.

Note. Def Stan 00-055, Part 1, contains guidance on addressing the unique military risk requirement. Although this particularly references Programmable Elements (PE) issues, the principles may be relevant to this standard.

11 Tailoring

11.1 This standard has to address a wide range of PSS acquisition scenarios. As a consequence, there may be some clauses of this standard which are not applicable in a particular scenario, or there may need to be additional information on how to interpret this standard, for a given contract. This is referred to as tailoring. Guidance on tailoring is given in Annex A, with a Compliance Matrix being provided in Annex B and may also be delivered through UK MOD Regulations and applied at ITT or in the contract.

Annex A
Tailoring Guidance

A.1 Introduction

A.1.1 Tailoring is the process of identifying the range and depth of safety activities that should be carried out. It depends on the scope, size, complexity, lifecycle phase and contractual arrangements of any given project. This standard has to address a wide range of acquisition scenarios and as a result there will be clauses of this standard which require tailoring. Whilst tailoring is the prerogative of the UK MOD, it may be influenced by a contractor's Alternative Acceptable Means of Compliance (AAMC) for a given contract.

A.1.2 It is expected that the proposed tailoring compliance matrix will be documented in the scope of contract at ITT. This would then be captured in a draft SMP or agreed between the preferred bidders and the UK MOD prior to contract award. Guidance is given here on how this standard might be tailored by the UK MOD, or where such tailoring could be proposed by a contractor during their contract negotiations.

A.1.3 This standard may be tailored by the UK MOD in the following ways:

a) **Alternative**: replacing a clause with an AAMC that meets the original safety requirement, i.e. where the contractor's SMS covers a particular requirement.

b) **Partial**: revise a clause for partial compliance in order to address a particular acquisition scenario where full compliance cannot be achieved.

c) **Waive**: waiver of a clause or clauses from the contract; this is likely to be at the whole paragraph level, eg to remove the requirement for the In-Service Data Analysis where safety in-service is out of scope of the contract. Smaller scale waivers of clauses and sub-clauses are possible but all must be justifiable.

d) **Additional**: additional requirement clauses or sub-clauses may be added to this standard. This may be particularly relevant where there are domain regulatory requirements, however, these clauses should be documented in the SMP and documentary deliverables as appropriate.

A.1.4 The clauses in the standard should remain extant and tailoring will be reflected in the Tailoring Statement or Level of Compliance fields of the Tailoring and Compliance Matrix, and will be defined by the UK MOD and reflected in the contract.

A.1.5 Where contractors supply a draft SMP, delivered in response to the ITT, it is important that it incorporates the contractor's responses to any UK MOD tailoring and their compliance with this standard as reflected in the ITT. The tailoring compliance matrix could be used to identify compliance by the bidder. The bidder should indicate Full, Full (AAMC), Partial or Waiver against each clause with reasoning, justification or proposed alternative means of compliance and their rational documented in a draft SMP. Post bid selection, the rationale for tailoring and the acceptable means of compliance, agreed by the UK MOD, will be documented in the SMP, ISSS and safety case report.

A.1.6 Annex B provides a Tailoring and Compliance Matrix which advises the level of tailoring allowed for each clause. Where a clause is stated as being mandatory, there will need to be a robust, justified reason for tailoring, eg compliance with domain regulatory requirements or adherence to contractual requirements.

Annex B
Tailoring and Compliance Matrix

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
Safety Management Requirements							
	Safety Management System						
4	Clause Extant	Mandatory.					
4.1	**Safety Management Plan**						
4.1.1	Clause Extant	Partially Tailorable. Safety Management Plan might already exist.					
4.1.2	Clause Extant	Tailorable. The UK MOD might agree use of other standard.					
4.1.3	Clause Extant	Tailorable.					
4.1.4	Clause Extant	Tailorable.					
4.1.5	Clause Extant	Tailorable.					
4.1.6	Clause Extant	Tailorable.					
4.1.7	Clause Extant	Tailorable.					
4.1.8	Clause Extant	Tailorable.					
4.1.9	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
4.1.10	Clause Extant	Tailorable					
4.2	**Agreement**						
4.2.1	Clause Extant	Mandatory.					
4.2.2	Clause Extant	Tailorable.					
4.3	**Review and Update**						
4.3.1	Clause Extant	Mandatory.					
4.3.2	Clause Extant	Tailorable.					
4.3.3	Clause Extant	Tailorable.					
4.3.4	Clause Extant	Tailorable.					
4.4	**Progress Reports**						
4.4.1	Clause Extant	Mandatory.					
4.4.2	Clause Extant	Tailorable.					
5	**General Requirements**						
5.1	**Deviation from Requirements**						
5.1.1	Clause Extant	Mandatory.					
5.1.2	Clause Extant	Tailorable.					
5.1.3	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
5.1.4	Clause Extant	Tailorable.					
a)	Clause Extant	Tailorable.					
b)	Clause Extant	Tailorable.					
5.1.5	Clause Extant	Tailorable.					
5.2	**Legislation, Regulations, Standards, Policy and Approved Codes of Practice**						
5.2.1	Clause Extant	Tailorable. This may be undertaken by the UK MOD or another 3rd Party.					
5.2.2	Clause Extant	Mandatory.					
5.2.3	Clause Extant	Tailorable. This may be undertaken by the UK MOD or another 3rd Party.					
5.3	**Sub-Contracting**						
5.3.1	Clause Extant	Mandatory.					
5.3.2	Clause Extant	Tailorable.					
5.3.3	Clause Extant	Tailorable.					
5.3.4	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
5.4	**Multiple Deliverables**						
5.4.1	Clause Extant	Mandatory					
5.4.2	Clause Extant	Tailorable					
5.4.3	Clause Extant	Tailorable					
5.5	**Information Management**						
5.5.1	Clause Extant	Mandatory.					
5.5.2	Clause Extant	Mandatory.					
5.5.3	Clause Extant	Mandatory.					
5.5.4	Clause Extant	Mandatory					
5.5.5	Clause Extant	Mandatory					
5.5.6	Clause Extant	Mandatory					
5.5.7	Clause Extant	Mandatory					
5.5.8	Clause Extant	Tailorable					
5.5.9	Clause Extant	Tailorable					
5.5.10	Clause Extant	Tailorable					
5.5.11	Clause Extant	Tailorable.					
5.5.12	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
5.6	**Documentary Deliverables**						
5.6.1	Clause Extant	Tailorable. The UK MOD might agree another set of deliverables					
a)	Clause Extant	Mandatory.					
b)	Clause Extant	Mandatory.					
c)	Clause Extant	Tailorable.					
d)	Clause Extant	Tailorable.					
e)	Clause Extant	Mandatory.					
f)	Clause Extant	Tailorable.					
g)	Clause Extant	Tailorable.					
h)	Progress Reports.	Tailorable.					
5.6.2	Clause Extant	Mandatory.					
5.6.3	Clause Extant	Tailorable.					
5.6.4	Clause Extant	Tailorable.					
5.7	**Agreement of Deliverables**						
5.7.1	Clause Extant	Mandatory.					
5.7.2	Clause Extant	Tailorable.					
5.7.3	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
5.7.4	Clause Extant	Tailorable.					
6	**Roles and Responsibilities**						
6.1	**Safety Organisation**						
6.1.1	Clause Extant	Partially Tailorable. The UK MOD might not require identification of individuals.					
6.1.2	Clause Extant	Mandatory.					
6.1.3	Clause Extant	Mandatory.					
6.1.4	Clause Extant	Tailorable.					
6.1.5	Clause Extant	Tailorable.					
6.2	**Safety Committees**						
6.2.1	Clause Extant	Partially Tailorable. There might not be any existing safety committees.					
6.2.2	Clause Extant	Partially Tailorable. There might not be any existing safety committees.					
6.2.3	Clause Extant	Partially Tailorable. There might not be any existing safety committees.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
6.2.4	Clause Extant	Partially Tailorable. There might not be any existing safety committees.					
6.2.5	Clause Extant	Tailorable.					
6.2.6	Clause Extant	Tailorable.					
6.2.7	Clause Extant	Tailorable.					
6.2.8	Clause Extant	Tailorable.					
6.2.9	Clause Extant	Tailorable.					
6.3	**Competencies**						
6.3.1	Clause Extant	Mandatory.					
6.3.2	Clause Extant	Tailorable.					
6.3.3	Clause Extant	Tailorable.					
6.3.4	Clause Extant	Tailorable.					
6.3.5	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
7	**Interfaces**						
7.1	**Organisational Interfaces**						
7.1.1	Clause Extant	Mandatory.					
7.1.2	Clause Extant	Tailorable.					
7.1.3	Clause Extant	Tailorable.					
7.2	**Technical Interfaces**						
7.2.1	Clause Extant	Mandatory.					
7.2.2	Clause Extant	Mandatory.					
7.2.3	Clause Extant	Mandatory.					
7.2.4	Clause Extant	Tailorable.					
7.3	**External Interacting Interfaces**						
7.3.1	Clause Extant	Mandatory.					
7.3.2	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
8	**Safety Audits**						
8.1	**Audits and Reports**						
8.1.1	Clause Extant	Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
8.1.2	Clause Extant	Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
8.1.3	Clause Extant	Tailorable.					
8.1.4	Clause Extant	Tailorable.					
8.2	**Contractor Safety Auditor Independence**						
8.2.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
8.3	**Independent Safety Audit**						
8.3.1	Clause Extant	Mandatory.					
8.3.2	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
8.4	**Remedial Action**						
8.4.1	Clause Extant	Mandatory.					
8.4.2	Clause Extant	Tailorable.					
8.4.3	Clause Extant	Tailorable.					
SAFETY ENGINEERING							
9	**Safety Requirements, Hazard and Risk Analysis**						
9.1	**Hazards and Accidents**						
9.1.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.1.2	Clause Extant	Tailorable.					
9.1.3	Clause Extant	Tailorable.					
9.1.4	Clause Extant	Tailorable.					
9.1.5	Clause Extant	Tailorable.					
9.1.6	Clause Extant	Tailorable.					
9.1.7	Clause Extant	Tailorable					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.2	**Hazard Tracking**						
9.2.1	Clause Extant	Mandatory.					
9.2.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.2.3	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities					
9.2.4	Clause Extant	Tailorable.					
9.3	**Safety Requirements**						
9.3.1	Clause Extant	Mandatory.					
9.3.2	Clause Extant	Mandatory.					
9.3.3	Clause Extant	Mandatory.					
9.4	**Safety Requirements Management**						
9.4.1	Clause Extant	Mandatory.					
9.4.2	Clause Extant	Tailorable.					
9.4.3	Clause Extant	Tailorable.					
9.4.4	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.5	**Design for Safety**						
9.5.1	Clause Extant	Mandatory.					
9.5.2	Clause Extant	Mandatory.					
9.5.3	Clause Extant	Partially Tailorable. The UK MOD may agree different strategies.					
a)	Clause Extant	Tailorable.					
b)	Clause Extant	Tailorable.					
c)	Clause Extant	Tailorable.					
d)	Clause Extant	Tailorable.					
e)	Clause Extant	Tailorable.					
f)	Clause Extant	Tailorable.					
9.5.4	Clause Extant	Mandatory.					
9.5.5	Clause Extant	Mandatory.					
9.5.6	Clause Extant	Tailorable.					
9.5.7	Clause Extant	Tailorable.					
9.5.8	Clause Extant	Tailorable.					
9.5.9	Clause Extant	Tailorable.					
9.5.10	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.6	**Safety Analysis**						
9.6.1	Clause Extant	Mandatory.					
9.6.2	Clause Extant	Mandatory.					
9.6.3	Clause Extant	Tailorable.					
9.6.4	Clause Extant	Tailorable.					
9.6.5	Clause Extant	Tailorable.					
9.7	**Failure Modes**						
9.7.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.7.2	Clause Extant	Partially Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.3	Clause Extant	Partially Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.7.4	Clause Extant	Partially Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.5	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.7.6	Clause Extant	Tailorable.					
9.7.7	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.8	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.9	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.7.10	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.11	Clause Extant	Tailorable.					
9.7.12	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.13	Clause Extant	Tailorable.					
9.7.14	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.15	Clause Extant	Tailorable.					
9.7.16	Clause Extant	Tailorable. Alternative techniques that do not specifically identify Failure Modes may be agreed with the UK MOD. See 9.7 Note 2.					
9.7.17	Clause Extant	Tailorable.					
9.7.18	Clause Extant	Tailorable					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.8	**Risk Estimation**						
9.8.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.8.2	Clause Extant	Tailorable.					
9.8.3	Clause Extant	Tailorable.					
9.8.4	Clause Extant	Tailorable.					
9.9	**Risk and Compliance Evaluation**						
9.9.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.9.2	Clause Extant	Tailorable.					
9.9.3	Clause Extant	Tailorable.					
9.9.4	Clause Extant	Tailorable.					
9.9.5	Clause Extant	Tailorable.					
9.10	**Satisfaction of Requirements**						
9.10.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
9.10.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
9.10.3	Clause Extant	Tailorable.					
9.10.4	Clause Extant	Tailorable.					
10	**Safety Reporting**						
10.1	**Information Set Safety Summary**						
10.1.1	Clause Extant	Mandatory.					
10.1.2	Clause Extant	Mandatory.					
10.1.3	Clause Extant	Mandatory.					
10.1.4	Clause Extant	Mandatory.					
10.1.5	Clause Extant	Tailorable.					
10.2	**Safety Case**						
10.2.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
10.2.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
10.2.3	Clause Extant	Mandatory.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
10.2.4	Clause Extant	Mandatory.					
10.2.5	Clause Extant	Mandatory.					
10.2.6	Clause Extant	Mandatory.					
10.2.7	Clause Extant	Mandatory.					
10.2.8	Clause Extant	Tailorable.					
10.2.9	Clause Extant	Tailorable.					
10.2.10	Clause Extant	Tailorable.					
10.2.11	Clause Extant	Tailorable.					
10.2.12	Clause Extant	Tailorable.					
10.2.13	Clause Extant	Tailorable.					
10.2.14	Clause Extant	Tailorable.					
10.3	**Safety Case Reports**						
10.3.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
10.3.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
10.3.3	Clause Extant	Mandatory.					
10.3.4	Clause Extant	Mandatory.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
10.3.5	Clause Extant	Mandatory.					
10.3.6	Clause Extant	Tailorable.					
10.3.7	Clause Extant	Tailorable.					
11	**Supply and Change Management**						
11.1	**Build State Definition**						
11.1.1	Clause Extant	Mandatory.					
11.1.2	Clause Extant	Mandatory.					
11.1.3	Clause Extant	Tailorable.					
11.1.4	Clause Extant	Tailorable.					
11.2	**Change Control**						
11.2.1	Clause Extant	Mandatory.					
11.3	**Planning for Change**						
11.3.1	Clause Extant	Mandatory.					
11.3.2	Clause Extant	Tailorable.					
11.4	**Safety of Changes**						
11.4.1	Clause Extant	Mandatory.					
11.4.2	Clause Extant	Mandatory.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
11.4.3	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.4.4	Clause Extant	Tailorable.					
11.4.5	Clause Extant	Tailorable.					
11.4.6	Clause Extant	Tailorable.					
11.5	**Safe Update**						
11.5.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.5.2	Clause Extant	Mandatory.					
11.5.3	Clause Extant	Mandatory.					
11.6	**Monitoring Change**						
11.6.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.6.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.6.3	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
11.7	**Incorporating Change**						
11.7.1	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.7.2	Clause Extant	Partially Tailorable. The UK MOD may contract a 3rd party to undertake or manage such activities.					
11.7.3	Clause Extant	Tailorable.					
11.7.4	Clause Extant	Tailorable.					
11.7.5	Clause Extant	Tailorable.					
11.7.6	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
SAFETY IN-SERVICE							
12	**Supporting Systems In-Service**	This section only applies when in-service support is contracted.					
12.1	**Management of Safety-Related In-Service Data**						
12.1.1	Clause Extant	Mandatory.					
12.1.2	Clause Extant	Tailorable.					
12.2	**Monitoring, Reporting and In-service Data Analysis**						
12.2.1	Clause Extant	Mandatory.					
12.2.2	Clause Extant	Mandatory.					
12.2.3	Clause Extant	Mandatory.					
12.2.4	Clause Extant	Mandatory.					
12.2.5	Clause Extant	Tailorable.					
12.2.6	Clause Extant	Tailorable.					
12.2.7	Clause Extant	Tailorable.					
12.2.8	Clause Extant	Tailorable.					
12.2.9	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
12.3	**Remedial Action**						
12.3.1	Clause Extant	Mandatory.					
12.3.2	Clause Extant	Tailorable.					
12.3.3	Clause Extant	Tailorable.					
13	**Service Provision**	This section only applies when service provision is contracted.					
13.1	**Safety Case Report**						
13.1.1	Clause Extant	Mandatory.					
13.1.2	Clause Extant	Mandatory.					
13.1.3	Clause Extant	Tailorable.					
13.1.4	Clause Extant	Tailorable.					
13.2	**Service Provision Planning**						
13.2.1	Clause Extant	Mandatory.					
13.2.2	Clause Extant	Tailorable.					
13.2.3	Clause Extant	Tailorable.					
13.2.4	Clause Extant	Tailorable.					
13.2.5	Clause Extant	Tailorable.					
13.2.6	Clause Extant	Tailorable.					

Para	Def Stan 00-056 Part 1	Mandatory/ Tailorable/ Informative	Tailoring Statement	Level of Compliance			
				Full	Full (AAMC)	Partial	Waiver
13.2.7	Clause Extant	Tailorable.					
13.3	**Risk Management**						
13.3.1	Clause Extant	Mandatory.					
13.3.2	Clause Extant	Mandatory.					
13.3.3	Clause Extant	Mandatory.					

Annex C
Data Item Descriptions

C.1 The Def Stan 00-056 DIDs are intended to assist contractors in determining the scope of supply of the project documentation; they have a similar purpose to the DIDs in MIL-STD-882 but should not be considered as directly equivalent.

C.2 The format, content and frequency of deliverable DIDs will be agreed with the UK MOD and form part of the scope of supply. Domain specific regulations may expand or reduce the intent of the DIDs, eg a safety case report and ISSS may be replaced by a safety assessment report. Where possible, contractors should use civil, open and other standards as a basis of meeting the intent of the DIDs. The SMP will define the relevant deliverables and agreed DID tailoring.

C.3 DIDs are at the Annexes as follows:

a) Annex D Command Summary.

b) Annex E Information Set Safety Summary.

c) Annex F Safety Audit Plan.

d) Annex G Safety Audit Report.

e) Annex H Safety Case/Safety Assessment Report.

f) Annex I Hazard Log Report.

g) Annex J Safety Management Plan.

h) Annex K Progress Reports.

Annex D
DID - Command Summary

D.1 Purpose

D.1.1 This DID sets out requirements for a command summary in support of Def Stan 00-056. This DID is intended to identify the scope and content of the command summary.

D.1.2 The command summary is a stand-alone summary of the safety case/safety assessment report that provides a focused report for commanding officers or managers.

D.1.3 The purpose of a command summary is to inform the commanding officer, manager or accountable person of:

a) The safe operating envelope of the PSS.

b) Any in-service limitations imposed by design parameters, certification, and risk assessment.

c) The safety implications of any unusual aspect of the PSS's design.

d) Information that may assist in making balanced, risk-based decisions should there be an unforeseen requirement to operate the PSS outside the design envelope.

e) Information that may assist in making balanced, risk-based decisions about the safety risks associated with a larger system of systems incorporating this PSS. This should include, but not be limited to known Concept of Operations and Statements of Operating Intent and Usage.

D.2 Scope of Applicability

D.2.1 The command summary should be produced in accordance with the SMP together with the safety case/assessment report when:

a) The scope of analysis for the PSS either impacts or is impacted by in-service use.

b) Tasked by the accountable person (or their agent).

c) When required by the contract for the scope of supply.

D.2.2 It will capture key information necessary to enable in-service commanding officers and managers to have an understanding of key safety risks regarding the PSS being used.

D.2.3 Other areas may also be addressed in the summary, for example the environmental case which might then lead to a title of 'Command Safety and Environmental Summary' or another variation.

D.2.4 Commanding officers and managers need not be given the full safety case or even the full safety case report, since they should not need to know all the information contained in it.

D.2.5 In the DAE, the Release To Service documentation (eg RTS, ALWRC & AERC) must not be subverted by a command summary. In the provision of services, a command summary may be appropriate.

D.3 Application/Interrelationship

This DID contains the content and instructions for preparing a command summary as specified within the SMP and in conjunction with the safety case report and Information Set Safety Summary.

D.4 Preparation Instructions

D.4.1 The command summary should address the following topics:

a) Scope (PSS and in-service use).

b) In-service Limitations.

c) Assumptions made in the Safety Case.

d) Unusual Aspects of the PSS's Design.

e) Safety risks in-service and recommended minimisation techniques.

f) Level of safety provided.

g) Emergency responses.

D.4.2 The command summary may be prepared under an alternative heading provided that it addresses the content and controls required by this DID.

D.4.3 Scope (PSS and in-service use)

D.4.3.1 The command summary should clearly and exactly identify the PSS and operations within its scope including their version and modification status.

D.4.3.2 A command summary may address more than one PSS and/or more than one version/modification state provided that the scope is clear.

D.4.4 In-Service Limitations

D.4.4.1 The command summary should clearly and exactly identify the operating environment and/or operations within its scope. This requires the provision of intended in-service scenarios such as Concept of Operations or a Statement of Operational Intent and Usage.

D.4.4.2 The command summary should explicitly identify any in-service scenarios that are out of scope and purposefully not addressed within it.

D.4.4.3 The command summary should identify any in-service limitations on the PSS from any authoritative source, eg a safety committee.

D.4.5 Assumptions made in the Safety Case/Safety Assessment.

All assumptions used within the safety case/safety assessment should be identified and recorded in the command summary.

D.4.6 Unusual Aspects of the PSS Design

The command summary should clearly identify any aspects of the PSS's design that affect safety in a manner that could be regarded as unusual or unanticipated, eg cyber-attack.

D.4.7 Safety Risks In-Service and Recommended Minimisation Techniques

D.4.7.1 The command summary should address all key safety risks of the PSS when used in respect of the in-service limitations and provide recommendations for minimising those risks.

D.4.7.2 The command summary should provide information that may assist in making balanced, risk-based decisions should there be an unforeseen requirement to operate the PSS outside the design envelope.

D.4.7.3 The command summary should provide information that may assist in making balanced, risk-based decisions about the safety risks associated with a larger system of systems incorporating this PSS.

D.4.8 Level of Safety Provided

D.4.8.1 These aspects should be addressed in a concise but comprehensive manner using text, illustrations, tables, etc to convey the level of safety to a commanding officer or manager.

D.4.8.2 The command summary should clearly identify requirements to be met under all foreseeable circumstances and provide recommendations that will generally reduce safety risk.

D.4.9 Emergency Response

D.4.9.1 The command summary should provide information for addressing foreseeable emergency situations.

D.4.9.2 The command summary should provide plans that cover emergency situations including, but not limited to, defining standard operating procedures, resourcing and oversight.

D.5 Control Requirements

D.5.1 The command summary should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

D.5.2 Approval of the command summary should be as defined within the SMP.

D.5.3 The command summary should be a formally controlled document, or part of a formally controlled document, with an issue number and date of issue.

D.5.4 The command summary should be updated whenever the safety case or safety assessment report is re-issued through the life of the PSS.

Annex E
DID - Information Set Safety Summary

E.1 Purpose

E.1.1 This DID sets out requirements for an Information Set Safety Summary (ISSS) in support of Def Stan 00-056. This DID is intended to identify the scope and content of the ISSS. The concept, use and applicability of ISSS and its relationship with safety case reports are included in Chapter 2 Para 6.

E.1.2 The ISSS draws on the content of the information set to provide a justification of the safety performance of a PSS, within bounds that are reasonable, given the scope of contract and other factors set out in this DID.

E.1.3 The ISSS is intended to provide sufficient information to enable PSS to be safely integrated into a higher level PSS, or interfaced to a peer PSS. The ISSS summarises the technical properties of the PSS that are relevant to safe integration/interface where the contractor cannot directly assess risk to life. The ISSS would be used by the integrator of the higher level PSS to support their safety assessment and contribute to the top level safety case.

E.1.3.1 The ISSS supports the production of a safety case/safety assessment when the PSS is integrated into a (larger) system, or a system or service integrated into a system of systems, eg for the DAE in the air system safety case. It may also supplement the safety case/safety assessment report which is a more specific safety report for a particular in-service use of a PSS.

E.1.3.2 The ISSS is constrained by the scope of analysis on the information set. A contractor‘s analysis is constrained to the limits of their visibility of the intended in-service operation of their PSS, and features that are inherent in their chosen design approach.

E.1.3.3 In compiling an ISSS, it is recognised that whilst a contractor may not be able to determine in isolation the acceptability of overall safety performance of their PSS, they have a responsibility to provide sufficient information for others to integrate their PSS in accordance with the contractor’s design intent to produce a system that can be operated safely.

E.2 Scope of Applicability

E.2.1 An ISSS is required where the contract includes the supply of product or service that is to be installed, or integrated, into a larger PSS.

E.2.2 There will be cases where a contractor can assess safety only in terms of the inherent characteristics of their PSS, such as the use of hazardous materials, risk of electric shock, control of moving parts. There will be other cases where the contractor has sufficient knowledge of the intended use that they can assess safety risks arising from the in-service operation of the PSS. The application of the DID will require adapting to ensure that the balance of inherent/intrinsic and external/extrinsic risks is appropriate for the contract/PSS context. The agreed scope of supply should be documented in the SMP.

E.3 Application/Interrelationship

This DID contains the content and instructions for preparing an ISSS as specified within the SMP and in conjunction with the safety case/safety assessment report and command summary.

E.4 Preparation Instructions

E.4.1 The ISSS should address the following topics:

a) Scope.

b) Identified accidents, hazards and failure modes.

c) Assumptions, dependencies and limitations.

d) Context of in-service use.

e) Unusual aspects of the PSS’s design.

f) Safety justification.

E.4.2 The ISSS may be prepared under alternative topic headings provided that it addresses the content and controls required by this DID. The content required by the DID may be provided under a number

of documents, or incorporated with other deliverables, provided that the purpose set out above is achieved in a clear and unambiguous way.

E.4.3 The ISSS should be assumed to be deliverable unless otherwise stated within the scope of supply. Preliminary versions of the ISSS may be required as the maturity of the PSS develops. The timing and scope of preliminary versions should be agreed with the customer and defined within the SMP.

E.4.4 Scope

The ISSS should include a scope statement that defines the boundary of the PSS covered by the ISSS, taking into account the scope of contract, the scope of analysis and the PSS in-service operation. This may be supported by the relevant safety case/safety assessment report and command summary if they are available.

E.4.5 Identified Accidents, Hazards and Failure Modes

The ISSS should summarise all the potential accidents, hazards and failure modes in the information set that an integrator may need to take into account when performing the risk analysis during PSS integration. This should include those that have been sentenced as low risk and are not identified or recorded in the safety case report. For example: accidents, hazards or failure modes associated with a capability of the PSS that is not currently used in-service.

E.4.6 Assumptions, Dependencies and Limitations

E.4.6.1 The ISSS should summarise all the assumptions, dependencies and limitations identified in the information set including those not recorded in the safety case report.

E.4.6.2 This should include assumptions and dependencies related to valid configurations of the PSS but not currently used in-service.

E.4.7 Context of In-Service Use

E.4.7.1 The ISSS should summarise the current in-service use (the relevant command summary should be used to support this topic).

E.4.7.2 The ISSS should also summarise capabilities that are accessible but not used in-service. This should include capability that is inherent, eg functionality included but not used in a COTS PSS.

E.4.8 Unusual Aspects of the PSS's Design

The ISSS should summarise any aspects of the PSS that could be considered unusual, particularly those that are not covered by the safety case report, this may include:

a) Foreseeable misuse of the PSS capability, eg a PSS display function being used in an ad-hoc way to display information from another source.

b) A security vulnerability, control or mitigation that may lead to a safety issue when the PSS is placed in an environment outside the current in-service safety case.

c) Adoption of novel technology that has not frequently been used within safety related PSS previously.

E.4.9 Safety Justification

E.4.9.1 The ISSS should summarise safety performance of PSS. It should not be as extensive as the safety justification and analysis of the safety case report but include elements that may not be in the safety case report. This should include all the inherent/intrinsic risks not controlled by the PSS design but mitigated through limitations of use or assumptions about the usage environment.

E.4.9.2 The ISSS safety justification must summarise any safety specific functions of the PSS that operators or integrators can interface or interact with.

E.4.9.3 The ISSS safety justification is a summary and should be succinct and not extensive but must highlight/summarise all the safety properties identified in the information set, particularly those not in the safety case report. The ISSS should highlight any potential safety issues if the PSS has further capabilities or has limitations dependent on operating environment.

E.4.9.4 The PSS ISSS may provide an essential part of the body of evidence in a system safety case.

E.5 Control Requirements

E.5.1 The ISSS should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

E.5.2 The ISSS should be approved by a suitable authorised representative of the contractor, in accordance with the roles and responsibilities defined in the SMP and endorsed by the safety committee.

E.5.3 The ISSS may address information for more than one PSS type and/or more than one version/modification state of a PSS, provided that the information specific to the PSS version under contract is clear.

E.5.4 Reasonable access to the information set that underpins the ISSS should be provided to auditors and others identified by the SMP as having a legitimate need to access such information for safety purposes.

Annex F
DID - Safety Audit Plan

F.1 Purpose

F.1.1 This DID sets out requirements for a safety audit plan in support of Def Stan 00-056. In doing so, it also intends to identify the scope and content of the safety audit plan.

F.1.2 A safety audit plan should be produced for every project working to Def Stan 00-056. A safety audit plan should be updated regularly and following major project events, eg annual update or at Preliminary or Critical Design Reviews. Updates of a safety audit plan should be part of the scope of contract and defined in the SMP.

F.2 Scope of Applicability

F.2.1 The safety audit plan should identify the PSS items subject to safety audit and reference the relevant PSS SMP. The relevant PSS SMP should be developed such that they can be used to help compile the safety audit plan with the relevant scope and timing of the required safety audits. If there is no agreed contractor SMP then the safety auditor should use the requirements of this standard to help determine scope and timing of safety audits in the safety audit plan.

F.2.2 The safety audit plan should identify all safety audit requirements imposed through the contract and applicable legislation, regulations, and UK MOD policy and regulations. This should take into account all relevant jurisdictions; compliance with which may be determined during the safety audits.

F.2.3 The safety audit plan should also set out the assumptions being made by the safety auditor with regard to availability of documents, evidence, etc.

F.2.4 This safety audit plan DID can be used for contractor safety audits, or independent safety audits, or combined plans.

F.3 Application/Interrelationship

This DID contains the content and instructions for preparing safety audit plans. The contractor should consider the activities in the PSS Project Plans, SMP and related safety audit reports when compiling a safety audit plan.

F.4 Preparation Instructions

F.4.1 The safety audit plan should address the following topics:

a) Tailoring.

b) Applicable legislation and regulations.

c) Audit strategy.

d) Organisation and responsibilities.

e) Plans and milestones.

f) Analysis methods.

g) Interfaces.

h) Audit Reporting.

F.4.2 In general it is acceptable for contractors or Independent Safety Auditors (ISA) to use their own formats for safety audit plans, and to use the DID to check the scope and content of their safety audit plan.

F.4.3 A safety audit plan should be assumed to be deliverable unless otherwise stated within the scope of supply.

F.4.4 Tailoring

F.4.4.1 Should this DID require tailoring then such tailoring should occur at the contract tender/contract award stage. Any independent safety audit plan should be produced as agreed between the contractor, the UK MOD and the ISA; this might involve allowing the contractor to provide comments on a draft independent safety audit plan to ensure that the contractor understands the ISA's role, timescales and support requirements.

F.4.4.2 For small contracts the safety audit plan could be documented within the SMP rather than existing as a separate document; for larger contracts, a separate safety audit plan should be produced.

F.4.5 Applicable Legislation and Regulations

F.4.5.1 The safety audit plan should set out the goals of the safety audits, eg compliance with Def Stan 00-056. Where a Means of Compliance has been agreed by the UK MOD then the safety audit plan should show how it will determine that the approach has satisfied the intent of this standard.

F.4.5.2 The safety audit plan should identify all safety audit requirements imposed through contract and applicable legislation, regulations, and UK MOD policy and regulations. This should take into account relevant jurisdictions; compliance with which may be determined during the safety audits.

F.4.6 Audit Strategy

F.4.6.1 The safety audit plan should identify the strategy for meeting the safety audit goals and requirements, eg document selection, desk reviews, sample approach, etc. such that, for independent safety audits, the level of support required from the contractor organisations, in terms of personnel and access to information can be identified and agreed by the UK MOD and the contractor as part of the scope of contract.

F.4.6.2 Whereas a Contractor Safety Auditor (CSA) would be expected only to undertake safety audits of their own organisation and any sub-contractors, the ISA may also undertake safety audits of the relevant interfacing PSS through relevant UK MOD organisations.

F.4.6.3 For contracts at the early stages of the PSS lifecycle, eg concepts, the safety audit plan should show how the safety auditor will assess the contractor's intended safety strategy for the rest of the lifecycle.

F.4.7 Organisation and Responsibilities

F.4.7.1 The safety audit plan should identify the safety auditors, including the lead safety auditor if an audit team is proposed and justify how their areas of competence align with the PSS being developed / used by the contractor.

F.4.7.2 The safety audit plan should identify those contractor personnel needed to support safety audits; this should be on a role basis rather than naming individuals.

F.4.7.3 The safety audit plan should identify those within the contractor and UK MOD organisations with responsibility, authority and accountability for addressing safety audit findings.

F.4.7.4 The safety audit plan should identify roles outside the contractor's organisation that are relevant to the Safehty Audit activities, eg key suppliers and UK MOD Stakeholders (including regulators).

F.4.8 Plans and Milestones

F.4.8.1 The safety audit plan should provide a schedule for all safety audit activities and milestones, showing clearly the link between safety audit activities and other activities on the contract, eg major milestones such as Preliminary Design Review, Critical Design Review, etc.

F.4.8.2 The schedule should be updated after each safety audit, to take into account safety audit findings and the need for the safety auditor to assess how such findings have been addressed.

F.4.8.3 If the amount of safety audit effort is small then the contractor's safety audit schedule could be documented as part of the overall contractor's Project Plan.

F.4.9 Analysis Methods

F.4.9.1 The safety audit plan should identify, define and justify the methods to be used for the safety audits, especially if the safety audits will include assessment as well as audit activities.

F.4.9.2 The safety audit plan should record the safety criteria as specified by the UK MOD, rather than referencing the criteria as documented in the contractor's SMP. This is to address those cases where the UK MOD and contractor have not yet agreed the SMP or the safety criteria. In such cases the safety auditor should clearly document that this is the current state of affairs.

F.4.10 Interfaces

F.4.10.1 The safety audit plan should identify known interfaces to, and dependencies on, other Stakeholder organisations and define the methods for ensuring co-ordination across interfaces, including how safety audit findings are to be communicated to other organisations; this would normally be via the UK MOD.

F.4.10.2 The safety audit plan should identify the expected inputs to the safety audit activities which are to be made available by contractors, sub-contractors, the UK MOD, etc as well as when such inputs will be required.

F.4.10.3 Where relevant, the safety audit plan should also identify technical interfaces to existing or planned PSSs.

F.4.11 Audit Reporting

F.4.11.1 The safety audit plan should identify:

a) How long after a safety audit that safety audit reports are expected to be produced.

b) How the safety audit findings are to be recorded, categorized, and sentenced.

c) To whom the reports will be delivered and the roles and responsibilities with regard to responding to those safety audit findings.

F.4.11.2 Safety audit reports should record the safety criteria in place at the time of the safety audit. This is to address those cases where later amendments to the safety criteria are agreed between the UK MOD and the contractor, so that it is clear which safety criteria were applied during each safety audit.

F.4.11.3 Further guidance on the production of safety audit reports is contained in the DID for the safety audit report.

F.5 Control Requirements

F.5.1 The safety audit plan should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

F.5.2 The safety audit plan should be approved by a suitable authorised representative of the contractor (for internal plans) or safety committee (ISA plans), in accordance with the roles and responsibilities defined in the relevant management plan and endorsed by the safety committee.

Annex G
DID - Safety Audit Report

G.1 Purpose

G.1.1 This DID sets out requirements for a safety audit report in support of Def Stan 00-056. This DID is intended to identify the scope and content of the safety audit report.

G.1.2 At least one safety audit report should be produced for every project working to Def Stan 00-056, whether undertaken by a CSA or an ISA. The scope and number of safety audit reports will be defined in the safety audit plan.

G.2 Scope of Applicability

G.2.1 The safety audit report should identify the items subject to safety audit and reference the relevant safety audit plan and SMP. If there is no agreed safety audit plan or relevant SMP at the time of the audit then the safety auditor report should document how the requirements of this, or other standards were used to help drive the safety audit.

G.2.2 The safety audit report should also set out the initial assumptions made by the safety auditor with regard to availability of documents, evidence, etc.

G.3 Application/Interrelationship

This DID contains the content and instructions for preparing safety audit reports. The depth, scope, strategy and analysis methods for safety audits should be determined in the related safety audit plan. The contractor should consider the activities in the PSS Project Plans and SMP, as well as the related safety audit plan, when compiling a safety audit report.

G.4 Preparation Instructions

G.4.1 The safety audit report should address the following topics:

a) Tailoring.

b) Applicable legislation and regulations.

c) Audit implementation.

d) Organisation and responsibilities.

e) Plans and milestones.

f) Analysis methods.

g) Interfaces.

h) Safety audit findings.

i) Conclusions and recommendations.

G.4.2 In general it is acceptable for CSAs and ISAs to use their own formats for safety audit reporting and to use the DID to check the scope and content of their safety audit report.

G.4.3 At least one safety audit report is assumed to be a deliverable unless otherwise stated within the scope of supply.

G.4.4 Tailoring

G.4.4.1 Should this DID require tailoring for a contractor safety audit report, then such tailoring should be agreed at the ITT stage. Any independent safety audit report should be produced as agreed between the UK MOD and the ISA.

G.4.4.2 It would be expected that both the UK MOD and the contractor would be given visibility of draft safety audit reports, so as to allow the contractor and the UK MOD to provide comments, such as clarifying responses to safety audit findings, and to make the UK MOD aware of those safety audit findings as early as possible.

G.4.4.3 Where a number of safety audits are being undertaken on related items within a short period of time then it would be reasonable to produce a single safety audit report addressing all such audits; as long as this does not delay making major safety audit findings visible to the UK MOD and other stakeholders.

G.4.5 Applicable Legislation and Regulations

The safety audit report should record the goals of the safety audit, eg compliance with Def Stan 00-056. Where a means of compliance had been agreed then the safety audit report should document the approach used to satisfy the agreed means of compliance.

G.4.6 Audit Implementation

The safety audit report should record the audit implementation including those activities prior to the safety audit, eg document selection, desk reviews, sample approach, etc. The success, or failure, of all audit activities should be recorded. For example, an activity failed due a lack of necessary contractor support.

G.4.7 Organisation and Responsibilities

G.4.7.1 The safety audit report should identify the safety auditors who undertook the audits.

G.4.7.2 The safety audit report should identify those contractor personnel who supported the audits.

G.4.7.3 The safety audit report should identify those within the contractor and UK MOD organisations with responsibility, authority and accountability for addressing the safety audit findings raised as a result of the safety audit.

G.4.8 Plans and Milestones

The safety audit report should explain the context of the safety audit within the overall safety audit schedule defined in the safety audit plan. The safety audit report should identify if the safety audit plan needs amending in the light of the safety audit findings raised. This could include the need for additional follow-up audits in order to determine whether major safety audit findings are being addressed by the contractor, or the UK MOD.

G.4.9 Analysis Methods

G.4.9.1 Any additional analysis or assessment method not documented in the safety audit plan should be justified and documented in the safety audit report.

G.4.9.2 The safety audit report should identify relevant safety criteria applicable to the safety audit. This may be referenced through the relevant information in the relevant SMP or safety audit plan.

G.4.10 Interfaces

The safety audit report should identify whether the expected inputs to the safety audit activities, required to be made available by contractors, sub-contractors, the UK MOD, etc were provided during the audit. If not, then the reasons for their non-availability should be documented.

G.4.11 Safety Audit Findings

G.4.11.1 The safety audit report should document the safety audit findings, which should be categorized in accordance with the categorization scheme agreed between the contractor and the UK MOD and documented in the safety audit plan.

G.4.11.2 The safety audit report should record any discussions regarding the safety audit findings that may have taken place during the safety audit, such as potential remedial action. However, the safety auditor should be careful to ensure that their level of independence is maintained.

G.4.11.3 The safety audit report should clearly state the roles and responsibilities with regard to responding to the safety audit findings.

G.4.12 Conclusions and Recommendations

The safety audit report should include an overall conclusion of the findings of the safety audit together with a high level set of recommendations as to how the safety audit findings should be addressed.

G.5 Control Requirements

G.5.1 The safety audit reports should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. They should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

G.5.2 The safety audit reports should be approved by a suitable authorised representative of the contractor (for internal reports) or safety committee (ISA reports), in accordance with the roles and responsibilities defined in the relevant management plan and endorsed by the safety committee.

Annex H
DID - Safety Case/Safety Assessment Report

H.1 Purpose

H.1.1 This DID sets out requirements for a safety case report in support of Def Stan 00-056. This DID is intended to identify the scope and content of the safety case report. The concept, use and applicability of safety case reports and its relationship with ISSS are included in Chapter 2 Para 6.

H.1.1.1 In the DAE, each air system has its own safety case, “The Air System Safety Case”. It is supported by a number of structured arguments contained within equipment and commodity item safety assessments (defined in MAA02). Therefore, where the contractor is required to supply safety cases and safety case reports, in the DAE they are referred to as safety assessments and safety assessment reports. Where this DID refers to a safety case or safety case report, for the DAE it should be read as a safety assessment or safety assessment report (where those terms are in use).

H.1.2 The safety case report is a snapshot of the safety case at a given point in time. It documents that all of the safety issues relating to the PSS have been brought to a condition appropriate for the stage in the lifecycle, ie it provides the safety justification to support the major project milestones identified in the SMP. The safety case report draws on the content of the information set to provide a justification of the safety performance of a PSS, within bounds that are reasonable given the scope of supply and other factors set out in this DID. If there are shortfalls against safety requirements, the rationale for operating the PSS and the ways of mitigating the residual risk, will be justified.

H.1.3 The safety case report is intended to provide information to those with accountability for the safety of the PSS on the status of safety assessment and assurance, where the contractor can assess safety risk. This includes visibility of the structured argument justifying the suitability of the safety performance of the PSS. Depending on the scope of contract this may not represent a top level operational safety case assessment and may feed into higher level system or operational safety case assessment/assurance activities.

H.1.4 The safety case report supplements the ISSS at the PSS level. Whilst it is appropriate to have a focus on in-service use, it is also necessary to manage the technical detail that supports the design of the in-service PSS.

H.1.5 A contractor may not be able to determine in isolation the acceptability of overall safety performance of their PSS. However, they have a responsibility to provide sufficient information in the safety case report for others to integrate their PSS in accordance with the contractor’s design intent to produce a system that can be operated safely.

H.2 Scope of Applicability

H.2.1 A safety case report is always required where the scope of supply includes the supply of a system. A safety case report may be required where the product is an element of a larger PSS, dependent on the contracted scope of analysis.

H.2.2 There will be cases where a contractor can assess safety only in terms of the inherent characteristics of their PSS, such as the use of hazardous materials, risk of electric shock, control of moving parts. There will be other cases where the contractor has sufficient knowledge of the intended use that they can assess safety risks arising from the operation of the PSS. The application of the DID will require adapting to ensure that the balance of inherent/intrinsic and external/extrinsic risks is appropriate for the contract/PSS context. The agreed scope of contract should be documented in the SMP.

Note. For many simple products, an ISSS supported by an applicable command summary may be sufficient if the PSS is integrated into a more complex PSS with a safety case and associated safety case report.

H.3 Application/Interrelationship

A safety case report is a deliverable specified within the SMP. It may be used in conjunction with the ISSS and command summary. The safety case report is a presentation of the safety case which will be based on the evidence in the information set.

H.4 Preparation Instructions

H.4.1 The safety case report should address the following topics (these topics do not necessarily need to have their own explicit headings):

a) Scope.

b) Identified hazards and related accidents.

c) Assumptions, dependencies and limitations.

d) Context of use.

e) Unusual aspects of the PSS's design.

f) Safety justification.

H.4.2 The safety case report may be prepared under an alternative heading provided that it addresses the content and controls required by this DID. The content required by the DID may be provided under a number of documents, or incorporated with other deliverables, provided that the purpose set out above is achieved in a clear, concise and unambiguous way.

H.4.3 The safety case report may be combined with the ISSS and command summary. In this case there will be large areas of commonality in DID requirements, eg scope and context of use, however there should be a clear delineation between the topics addressing hazards that are addressed by the contractor, and those where the contractor is providing PSS and failure mode information in support of activities by another organisation, ie those areas covered uniquely by the ISSS DID.

H.4.4 The safety case report should be assumed to be deliverable unless otherwise stated within the contract. Preliminary versions of the safety case report may be required as the maturity of the PSS develops. The timing and scope of preliminary versions should be agreed with the customer and defined within the SMP.

H.4.5 Scope

H.4.5.1 The safety case report should include a scope statement that defines the boundary of the PSS covered by the safety case report, taking into account the scope of supply, the scope of analysis and the expected usage environment.

H.4.5.2 The scope statement should make clear the relationship to other reports, both extant and intended, that address the contractor's safety responsibilities and the intended use of the information contained within those reports. For example, this may include reference to a complementary ISSS, and the intention that these are supplied to support a broader safety case that addresses integration into a system and its in-service use (with in-service information in a command summary if required).

H.4.6 Identified Hazards and Related Accidents

H.4.6.1 The safety case report should identify the hazards that are within scope of contractor responsibility. It should also identify related accidents where these are within the contracted scope of analysis.

H.4.6.2 The safety case report may also identify hazards/accidents that are outside of the contracted scope of analysis but have been brought to the attention of the contractor. These are likely to be more relevant to the associated ISSS, and if included in this report should be clearly delineated to ensure there is no confusion regarding boundaries of responsibility.

H.4.7 Assumptions, Dependencies and Limitations

H.4.7.1 The safety case report should identify assumptions, at appropriate levels of abstraction, that have been used to progress the safety activities of the contractor. It should justify the reasonableness of such assumptions – in-service assumptions and limitations are particularly relevant to command summary.

H.4.7.2 The safety case report conclusions that rely on dependencies on information outside of the contractor's scope of supply or analysis should be identified, at appropriate levels of abstraction. This may include information supplied by the UK MOD on government furnished equipment, or information from interfacing PSS not within the contractor's scope of analysis.

H.4.7.3 The safety case report may include dependencies on information from sub-contractors or suppliers to the contractor. However, these should be clearly delineated from those from outside scope of contract as the responsibility for management of sub-contract/supplier information dependencies remains with the contractor.

H.4.7.4 The safety case report should identify limitations on use of the contractor's PSS that are necessary to ensure safety. Limitations may be aggregated together where it is appropriate to do so. Each limitation identified should detail the impact on safety should it not be enforced. This aims to aid judgements that may be necessary to balance risks arising from military operational imperatives. These limitations are considered a key aspect of the command summary if one is required.

H.4.8 Context of use

The safety case report should state the specified or intended context of use. This could include, but is not limited to: operating environment; integration considerations; competence of users; and concept of operation. This may also form part of the command summary if one is required.

H.4.9 Unusual Aspects of the Equipment's Design

The safety case report should highlight any aspects of the PSS that could be considered unusual, particularly where this may contribute to reasonably foreseeable misuse in operation or maintenance. This should including cyber security and human factors.

H.4.10 Safety Justification

H.4.10.1 The contractor is responsible for the safety performance of the PSS for inherent/intrinsic safety risks within their scope of supply. This responsibility may extend to aspects within the scope of analysis. The level of safety performance should be justified against that reasonably expected through relevant legislation, contract specification and good practice.

H.4.10.2 The safety case report should include evidence that the robustness of the justification has been challenged to provide an appropriate degree of assurance of its conclusions. This should include search for, and treatment of, potential counter evidence.

H.4.10.3 The safety case report should include the key elements of the safety case argument and references to evidence. From this argument and references it should be possible to trace all the evidence and detailed structured arguments that support the safety performance conclusions.

H.5 Control Requirements

H.5.1 The safety case report should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

H.5.2 The safety case report should be approved by a suitable authorised representative of the contractor, in accordance with the roles and responsibilities defined in the SMP and endorsed by the safety committee.

H.5.3 The safety case report may address information for more than one PSS type and/or more than one version/modification state of a PSS, provided that the association of the information specific to the PSS version under contract is clear.

H.5.4 Reasonable access to the information set that underpins the safety case report should be provided to safety auditors and others identified by the SMP as having a legitimate need to access such information for safety purposes.

Annex I
DID - Hazard Log Report

I.1 Purpose

I.1.1 This DID sets out requirements for a hazard log report in support of Def Stan 00-056. This DID is intended to identify the scope and content of the hazard log report.

I.1.2 A hazard log report is a snapshot of the hazard log status on a given date. The PSS hazard log is a continuously evolving record (database or document) which should be maintained with the PSS throughout its lifecycle.

I.1.3 Hazard log reports must be capable of showing the linkages between Causes, Hazards, Accidents and Controls, ie which failures lead to a hazardous condition arising that could result in a potential Accident, possibly with many-to-many relationships, and which controls relate to which causes, hazards and accidents. They must also differentiate between controls which are already in place and those which are being considered or planned.

I.1.4 Hazard log reports will be produced for the purpose of review (eg by the safety committee, the ISA or Stakeholders) to communicate current or changed status of the hazard log, as detailed in the SMP.

I.2 Scope of Applicability

I.2.1 Given that the PSS scope of contract may not match that of overall system for which the UK MOD hazard log requirements apply, it is essential that the relationship between the overall system level hazard log and the PSS hazard information maintained by the contractor is clearly captured and communicated.

I.2.2 The scope of contract may require the contractor to manage the complete hazard log for an overall system, in which case the requirements of POSMS Safety Management Procedures, including any domain specific aspects, will be applied.

I.2.3 Where the contractor is not the overall system hazard log manager, the contractor is required to supply hazard information to enable the UK MOD or their appointed hazard log manager to meet the POSMS requirements. The scope of information to be supplied will be dependent on the scope of contract and would normally be aligned to that addressed by the safety case/safety assessment report.

I.3 Application/Interrelationship

Hazard log reports are deliverables specified within the SMP. A hazard log report is used by stakeholders to assess the status of the PSS safety case at a particular point in the project. The hazard log is the full documentary evidence in the information set which draw from by reports such as the hazard log report and safety case report.

I.4 Preparation Instructions

I.4.1 The hazard log report should address the following topics to the degree agreed with the UK MOD and documented in the SMP (these topics do not necessarily need to have their own explicit headings). The level of detail provided against each heading should be tailored according to the agreed objective of each snapshot report:

a) Introduction.

b) Accident Data.

c) Hazard Data.

d) Risk Classification.

I.4.2 The hazard log report may be prepared under an alternative heading provided that it addresses the content and controls required by this DID. The content required by the DID may be provided under a number of documents, or incorporated with other deliverables, provided that the purpose set out above is achieved in a clear and unambiguous way. Repetition of information provided in other reports should be avoided by planning the purpose and content of such documents in advance and making appropriate cross reference.

I.4.3 The hazard log report should be assumed to be deliverable unless otherwise stated within the contract. By its nature, several versions of the hazard log report should be anticipated over the project lifetime. The timing and scope of versions should be agreed with the customer and defined within the SMP.

I.4.4 Introduction

I.4.4.1 The introduction should define the scope of information covered by the hazard log report and how this relates to any associated hazard logs, whether maintained by the contractor, the UK MOD or their agent.

I.4.4.2 The hazard log report should describe the PSS addressed by that scope, including relevant configuration information such as PSS identifier and standard.

I.4.4.3 The hazard log report should reference project safety information such as top level safety requirements and safety criteria. This information may be directly included rather than referenced where this aids interpretation of the accident, hazard and risk information in the hazard log report.

I.4.5 Accident Data

I.4.5.1 The hazard log report should include sufficient information to identify all relevant accidents and their sequences. It should link each accident with the hazards and causes which contribute to it, and any proposed or implemented controls or mitigations.

I.4.5.2 The hazard log report should include the accident severity category and probability targets to achieve an acceptable safety performance.

I.4.6 Hazard Data

I.4.6.1 The hazard log report should include sufficient information to identify all the hazards and their status, including any outstanding corrective action.

I.4.6.2 The hazard log report should include the hazard probability targets to achieve an acceptable safety performance.

I.4.7 Risk Classification

The hazard log report should include a statement of the risk classification of Accidents within scope of the hazard log report. It should be remembered that this may not be the complete set of accidents relevant to a system and therefore may represent only a lower bound on the risk classification of the related system.

I.5 Control Requirements

I.5.1 The hazard log report should be created, held and managed under an appropriate configuration management system, which should be specified in the SMP. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

I.5.2 The hazard log report should be approved by a suitable authorised representative of the contractor, in accordance with the roles and responsibilities defined in the relevant management plan and endorsed by the safety committee.

I.5.3 The hazard log report may address information for more than one PSS type and/or more than one version/modification state of a PSS, provided that the association of the information specific to the PSS version under contract is clear.

I.5.4 Reasonable access to the hazard log that underpins the hazard log report should be provided to auditors and others identified by the SMP as having a legitimate need to access such information for safety purposes.

Annex J
DID - Safety Management Plan

J.1 Purpose

J.1.1 This DID sets out requirements for a Safety Management Plan (SMP). The requirements should be viewed as a checklist, rather than as a contents list. This DID is intended to identify the scope and content of the SMP.

J.1.2 The SMP should be updated at a frequency defined in the contract, which should be commensurate with the project complexity and risk level and not more than 3 years; but it would be unusual if the SMP were not updated at least once per annum, and on major project events, eg a Preliminary or Critical Design Review.

J.1.3 In general, it is likely that the SMP would be produced by drawing on standard company practices, eg a Safety Management System (SMS), and on the project-specific information defined in the contract statement of work. The SMP should address the core principles of systems engineering and safety management.

J.2 Scope of Applicability

J.2.1 It is expected that the SMP would be a 'child' of the Project Management Plan which would identify the context of the Project. For some smaller projects the Safety Management aspects may be included within the Project Management Plan.

J.2.2 The SMP should identify the agreed scope of contract for the PSS, including the scope of analysis and supply. Where the UK MOD, contractor and / or sub-contractors each operate an SMS, the SMP should document, in accordance with the scope of contract, the interfaces between them and the boundaries of responsibility and accountability applicable to each.

J.2.3 It should identify both primary and ancillary PSSs, eg test equipment as well as the main deliverables, where they are safety-relevant. It should identify critical dependencies on externally supplied PSS, eg GFX.

J.2.4 The SMP should identify and cover the lifecycle of the PSS within the scope of analysis.

J.3 Application/Interrelationship

J.3.1 This DID contains the content and instructions for preparing the SMP. The SMP is a key plan and it should clearly identify important aspects such as responsibilities, plans, reports, interfaces, scope of contract, supply boundaries, requirements etc. The SMP should draw on the contractor's SMS for system engineering and safety management.

J.4 Safety Management Plan Preparation Instructions

J.4.1 The SMP should contain information on the following topics:

a) Applicable Legislation and Regulations.

b) Safety Strategy.

c) Safety Requirements.

d) Organisation and Responsibilities.

e) Plans and Milestones.

f) Analysis Methods.

g) Risk Assessment and Acceptance.

h) Development Methods.

i) Interfaces.

j) Information Management.

k) Safety Reporting.

l) Safety Auditing.

m) Change Management.

n) Deliverables.

o) Tailoring of Def Stan 00-056.

J.4.2 Coverage of the above topics is mandatory. However, tailoring may be acceptable subject to robust justification for the changes and agreement with the UK MOD.

J.4.3 Should this DID require more extensive tailoring then such tailoring should occur at the contract tender / contract award stage, not normally once the contract is under way.

J.4.4 The level of detail under each topic will depend on the scale of the project. For simple projects the SMP may contain detail for all of the above topics. For complex projects, the SMP is likely to contain detail for key elements of the above topics, and to refer out to other documents as appropriate, eg the disposal plan may be included in the SMP of the system into which the PSS is to be integrated.

J.4.5 Alternatively, for a simple project, the SMP would reference activities in the overall project management plan that are safety-related.

J.4.6 The topics may be viewed as a checklist for the supporting documentation, not just for the SMP itself. However, the level of detail in the SMP should be defined at the ITT and agreed prior to contract award, and should not normally be changed once the contract is under way.

J.4.7 Applicable Legislation and Regulations

The SMP should identify, or reference (eg reference to a legislation register), the legislation, regulations, standards and UK MOD policies that apply to the PSS, taking into account all theatres in which the PSS is intended to operate. It should also identify the relevant regulatory bodies, both civil and military, and the impact of their regulatory role on the PSS.

J.4.8 Safety Strategy

J.4.8.1 The SMP should identify a safety strategy that is both appropriate for the scope of analysis of the PSS, consistent with the project management plan and UK MOD policy and appropriate to the project risk profile.

J.4.8.2 The strategy should provide an overarching framework that will enable a PSS to be assured as safe within the scope of supply.

J.4.9 Safety Requirements

J.4.9.1 The SMP should identify all top level safety requirements imposed through contract and derived safety requirements applicable to legislation, regulations, and UK MOD policy.

J.4.9.2 The SMP should identify processes for identifying, and for managing safety requirements through the contract life, and especially the development process. The requirements should cover all of the DLOD within the scope of contract.

J.4.9.3 The SMP should identify processes for identifying, and for managing assumptions made when assessing the safety of the PSS.

J.4.10 Organisation and Responsibilities

J.4.10.1 The SMP should identify the key safety-related roles in the project organisation covering both individuals and committees. It should identify responsibility, authority and accountability for safety-related activities and decision-making, together with lines of reporting and communication. It should identify key staff with safety responsibility, and record their qualifications and experience. The SMP should document the Terms of Reference for the key roles.

J.4.10.2 The SMP should record how competency of staff in key safety roles is assessed and how it is managed.

J.4.10.3 The SMP should also identify roles outside the contractor's organisation, eg key suppliers, and UK MOD stakeholders, eg regulators.

J.4.10.4 The SMP should address all sub-contractors activities and responsibilities, including the mechanisms that the contractor will use for oversight of sub-contractor work, to ensure that the requirements of this standard are met.

J.4.11 Plans and Milestones

J.4.11.1 The SMP should identify the schedule for major safety activities and milestones, and clearly show the link between safety activities and the remainder of the activities on the contract, eg major milestones such as design reviews.

J.4.11.2 The SMP should identify other relevant plans, eg plans of significant service provision supporting the PSS, such as test rigs or trials that may warrant their own SMP and safety case.

J.4.12 Analysis Methods

J.4.12.1 The SMP should identify, define and justify the methods to be used for safety and hazard analysis, and which activities in the plan should use these methods.

J.4.12.2 The range of methods included will depend on the scope of analysis, but may include exploratory analyses, eg HAZOP, deductive techniques, eg Fault Tree Analysis, and inductive techniques, eg FMEA and Event Tree Analysis.

J.4.13 Risk Assessment and Acceptance

The SMP should identify and define the methods to be used for risk analysis, and which activities in the plan should use these methods. It should identify risk measures and acceptance criteria, eg hazard risk matrices, and the authorities for accepting risk in each category. It should also identify the organisations involved and protocols to be used for risk acceptance.

J.4.14 Development Methods

J.4.14.1 The SMP should identify, define and (where necessary) justify the methods to be used for the development of system components that perform a safety function or whose failure might result in a safety hazard, particularly in response to integrity requirements.

J.4.14.2 This should address the full lifecycle of all relevant technologies, eg software, and critical mechanical parts. Where appropriate the SMP should refer to external standards or sources of good practice.

J.4.14.3 The identification and definition of methods are necessary only where system components are being developed, eg may not apply to service provision.

J.4.15 Interfaces

J.4.15.1 The SMP should identify known interfaces to other stakeholder organisations and define the protocols for ensuring safety co-ordination across these interfaces, including identifying information to be shared and engagement in safety committees.

J.4.15.2 Where relevant, the SMP should also identify technical interfaces to existing or planned PSS within the scope of contract.

J.4.16 Information Management

J.4.16.1 The SMP should identify the scope of the information set and the formats, tools, etc, for recording the information set, together with the protocols for keeping the information set under configuration control.

J.4.16.2 The SMP should identify the procedures and tools for establishing and maintaining the hazard log to ensure that it accurately reflects the status of the design, hazard analysis, safety analysis and other safety engineering activities.

J.4.16.3 The SMP should identify mechanisms for preserving the information set through contract life.

J.4.17 Safety Reporting

J.4.17.1 The SMP should identify the frequency and nature of reports against the safety programme, and indicate how these will be linked into major programme milestones and reviews.

J.4.17.2 The SMP should identify the hazard log reports, ISSSs, safety case reports and Command Summaries to be produced, including preliminary reports and/or incremental delivery of the reports.

J.4.17.3 The SMP should identify the distribution lists for the reports and the forum in which the reports will be reviewed, discussed, and remedial action identified. If this is not specified, then the default is that the reports go to, and are handled by, the safety committee.

J.4.17.4 The SMP should identify mechanisms and procedures for recording and assessing incident data, and taking both immediate remedial action and longer-term corrective action. It should include processes for dissemination of information to all interested parties, which may include users of similar PSS, regulators, or other official bodies, eg the HSE.

J.4.18 Safety Auditing

J.4.18.1 The SMP should identify internal safety audit plans and reporting, including processes, terms of reference for audits, audit frequency, and audit of sub-contractors. This may refer to a dedicated safety audit plan.

J.4.18.2 The SMP should identify how safety audit findings (both internal and by an ISA, if appointed) will be sentenced, reported and managed, and the escalation route (in the defined organisation) if audit findings are not acted upon in a timely manner.

J.4.19 Change Management

J.4.19.1 The SMP should identify mechanisms and procedures for management of change for the PSS.

J.4.19.2 These mechanisms and procedures should address updates in-service, and the maintenance of clear records of materiel state, even for geographically dispersed PSS.

J.4.20 Deliverables

J.4.20.1 The SMP should identify all safety-related deliverables from the contract, and define formats for all documentary deliverables identifying where domain regulations and agreed civil standards replace DID formats.

J.4.20.2 The SMP should identify the review and acceptance process and timeframes for all deliverables.

J.4.21 Tailoring of Defence Standard 00-056

J.4.21.1 The SMP should contain a compliance matrix showing any tailoring of the requirements of Def Stan 00-056.

J.4.21.2 The SMP should contain results from identification and analyses of any divergences with Def Stan 00-056, and applicable regulations and legislation. The SMP should also contain the means of resolving the divergences.

J.4.21.3 The SMP should document the agreed deviations from requirements and Def Stan 00-056.

J.5 Control Requirements

J.5.1 The SMP should be created, held and managed under an appropriate configuration management system. It should be suitably secured to prevent information theft and to preserve information integrity, availability and accessibility.

J.5.2 The SMP should be approved by a suitable authorised representative of the contractor, in accordance with the roles and responsibilities defined in the relevant management plan and agreed by the UK MOD and the safety committee.

J.5.3 The SMP may address information for more than one PSS type and/or more than one version/modification state of a PSS, provided that the association of the information specific to the PSS version under contract is clear.

J.5.4 Throughout the life of the contract, the SMP should be subject to continual review and all changes agreed with the UK MOD and the safety committee

Annex K
DID - Progress Reports

K.1 Purpose

K.1.1 This DID sets out requirements for a progress report. This DID is intended to identify the scope and content of the progress report.

K.1.2 A progress report will normally record progress of safety management against the agreed SMP and will form a formal record which should stay with the PSS throughout its lifecycle. The progress report requirements should be viewed as a checklist, rather than as a contents list. It is desirable that the contractor uses their own formats for documents and to use the DID to check that the scope and content of the progress report.

K.1.3 The progress report should be updated at a frequency defined in the SMP. However, it would be normal for a progress report to be issued prior to significant safety meetings, eg a safety committee meeting.

Note. The progress report is not the method of recording safety committee minutes.

K.1.4 In general, it is likely that the progress report would be produced by drawing on standard company reporting practises.

K.2 Scope of Applicability

K.2.1 Progress reports record progress against the requirements of the SMP, eg schedule and status for major scope of supply deliverables such as a safety case/safety assessment report.

K.2.2 Progress reports may contain commentary or intermediate analysis on particular safety topics raised within the safety management committee or during other management activities. Progress reports may contain a response to a safety issue and form an important formal record, eg an analysis of data from an incident or clarification on the justification for adopting particular standards.

K.3 Application/Interrelationship

Progress reports are deliverables specified in the SMP. Progress reports are a record of intermediate contractor activities related to activities identified in the SMP or safety audit plan. Progress report may also contain responses to formal actions from stakeholders.

K.4 Progress Reports Preparation Instructions

K.4.1 Progress reports should address the following topics:

a) Progress against the SMP.

b) Progress against the safety audit plan.

c) Status of scope of supply Deliverables.

d) Analysis of Safety Issues.

e) Records of contractor activities in response to safety committee and stakeholder actions.

K.4.2 The above topics for a progress report are an indication of what areas a progress report may cover. Progress against the SMP and status of scope of supply deliverables are mandatory.

K.5 Control Requirements

All progress reports created should be held and managed under an appropriate configuration management system.

Annex L
Integrity and Open Standards

L.1 Introduction

L.1.1 Integrity is a general concept which applies across the entire system hierarchy, from the highest level, eg an aircraft carrier, to the lowest level, eg a bolt. This standard uses the concept of integrity, across a range of technologies, including structures and complex electronics.

L.1.2 Integrity is important from a safety perspective as loss of, or inadequate, integrity can contribute to hazards. A metal framework, eg an aerial mast, which has inadequate structural integrity, will fail under normal operating loads. Programmable Elements (PEs) which have inadequate integrity may have obscure failure modes that allow incorrect operation resulting in risk to life, eg Flight Control Software that allows an aircraft to exceed its operating envelope.

L.1.3 Hazards and failure modes are properties of PSS which can be observed. Integrity generally cannot be observed, but is a property of the way in which a PSS is designed, constructed and maintained.

L.1.4 This Annex provides guidance on the ways in which integrity requirements are determined, how they are managed through life, and how shortfalls in integrity are sentenced. The guidance specifically addresses where the standard requires the contractor to identify and record safety requirements to ensure integrity. In particular, it considers robustness to PSS elements which are not of high integrity (or are of unknown integrity) and impairments to integrity.

L.1.5 For some simple PSS elements, eg COTS/MOTS components, quality assurance, declaration of conformity and specifications may be sufficient to show that the elements are of sufficient integrity, eg have the requisite strength, reliability or performance. For more complex or critical PSS elements, or where simple PSS elements are to be integrated into a safety critical system, integrity needs to be more explicitly managed during the design and development process.

L.2 Integrity Requirements

L.2.1 Integrity requirements are a special case of derived safety requirements, and will generally be allocated and managed down to the level of individual elements which are designed and manufactured or acquired.

L.2.2 This standard encourages the use of civil, open or other standards or good practice. Open standards vary in how they decompose and allocate integrity requirements at a lower level. It is difficult to give general guidance as open standards use different strategies to manage integrity requirements, eg:

a) Aerospace Recommended Practice, ARP 4754/4761 initially allocating integrity requirements based on Hazard severity.

b) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, IEC 61508 risk reduction methodology.

c) Road Vehicles - Functional Safety, ISO 26262, influenced by controllability.

L.2.3 The general principle underlying decomposition is that there must be evidence that the elements to which the integrity requirements are allocated will fail independently. In particular, the aim is to ensure that there are no common-cause or common-mode failures between the elements. Mitigation strategies such as duality and diversity need to be designed in to the PSS, hence the use of the general term design integrity.

L.2.4 Recently, approaches to safety engineering have been developed that do not adopt a decompositional approach, eg STPA. Such approaches have been found to be useful for analysing complex systems where potential failures may not be obviously dependent leading to emergent hazard causes during operational use.

L.3 Design Integrity

L.3.1 Integrity is one of the key factors to take into account at the architectural design phase, and it feeds into design and architectural trade studies. Trade study techniques, such as Preliminary System Safety Analysis in ARP 4761, enable alternative architectures to be assessed based on their safety properties. One important aspect of the trade studies is to optimise the design to reduce the cost of achieving integrity, if possible, by placing the highest integrity requirements on simple elements, and avoiding reliance on elements which are complex.

L.3.2 Avoidance of single points of failure is a significant factor in design and architecture trade studies. These studies can lead to increased confidence in the selected architecture and reduce the possibility of over designed solutions.

L.3.3 If it is not possible to avoid single points of failure, then the critical PSS elements will have to be developed to the integrity level allocated to the most severe hazard associated with that failure. In many cases, there will be established means of developing or demonstrating the critical PSS elements to the appropriate level of integrity, eg design standards.

Notes:

1. In some cases, eg the main spar in an aircraft wing, it is not possible to avoid single points of failure.

2. In some cases, design standards are in the public domain. However, the safety case would also need to include an argument explaining why the design approach is adequate.

L.3.4 Duality, diversity and other forms of independence, use combinations of redundancy and disparate design and implementation solutions. Demonstrating independence may require analysis of mitigation strategies for the common-cause or common-mode failures, leading to a justification of the level of independence and overall integrity.

Notes:

1. There is more than one viewpoint when considering diversity in PSS, eg mechanistic and conceptual. Both views may have to be demonstrated as equivalent which may impact verification and validation.

2. An example of diversity for the same function is where an Inertial Navigation System and Global Positioning System use different communications methods, eg analogue and digital, on the same transmission line.

L.3.5 There is increasing trend for interdependencies in system design between previously separate elements of integrity, eg automated aircraft fuel distribution is used to alleviate stresses on wings. The failure of such an automated control system can place greater demands on the integrity of other parts of the system.

L.3.6 In some cases the design standards or approaches which have been used historically are no longer applicable or not considered sufficient, particularly when used out of their original context, and the design approach will have to address these interdependencies and document them in the safety case.

L.3.7 The intention of this standard is to identify design integrity requirements that address safety interdependencies and enable safe PSS.

L.4 Open Standards and Military Delta

L.4.1 It is UK MOD practice that Defence Standards are used only where civil or open standards cannot be effectively applied in a military context. One of the goals of this standard is that civil or open standards should be used as the basis for complying with its requirements. In practice, not all standards will fully address the requirements of this standard, so there needs to be a gap analysis and development of derived safety requirements to address shortfalls.

L.4.2 Meeting the requirements of this standard through the use of civil or open standards needs consideration and evaluation as their requirements relating to risk vary. Additionally, the set of techniques required, or implied, to meet the different standards also vary. These differences in detail are accepted in the context of this standard, as it seeks to conform to industry norms so far as practicable and guidance on adoption and application of PSS open standards is provided at Annex M. Adoption of a PSS open standard may lead to shortfalls in meeting the requirements of this standard. For example, civil or open standards may or may not require the use of Design Integrity where probabilities of failure cannot be assigned and may or may not require cyber security be considered as a potential cause of a failure mode.

L.4.3 Open standard shortfalls need to be sentenced, and will lead to derived safety requirements, addressed through the design and/or development process. These evidence shortfalls are gaps between civil and military needs arising from using open standards and are defined as a Military Delta (See Section 3 – Terms and Definitions).

L.4.4 Annexes N and O identify shortfalls for the PSS open standards IEC 61508 and MIL-STD-882E. The open standard shortfalls (Military Deltas) will need to be addressed by derived safety requirements identified by the contractor in their response to the UK MOD ITT.

L.5 PE Integrity

L.5.1 PSS dependent on software and complex electronic hardware have consistently challenged the UK MOD and Government projects. This dependency is increasing and impacted by emerging external challenges such as cyber security, data dependency and artificial intelligence.

Note. Def Stan 05-138 provides guidance for the levels of cyber protection required to be achieved by defence suppliers to protect project information, but not the PSS itself.

L.5.2 It is essential that contractors consider cyber security as a potential credible cause of Programmable Element (PE) failure modes contributing to a hazard. Additionally, UK MOD PE is increasingly being driven by external data which has led to a requirement to manage PE data integrity.

L.5.3 To meet the challenges of PE integrity, the following PE safety requirement principles have been developed from good practice:

a) Principle 1. PE safety requirements should be defined to address the PE contribution to system hazards.

b) Principle 2. The intent of the PE safety requirements should be maintained throughout requirements decomposition.

c) Principle 3. PE safety requirements should be satisfied.

d) Principle 4. Hazardous behaviour of the PE, including generation and use of data, should be identified and mitigated.

e) Principle 5. The confidence established in addressing the PE safety requirements should be commensurate to the contribution of the PE to system risk.

f) Principle 6. The safety-related consequences of adaptive PE behaviour should be addressed.

L.5.4 Def Stan 00-055 has been developed to meet these principles through measurable objectives and PE safety requirements. The implementation strategy for Def Stan 00-055 is through the application of PE open standards that demonstrably satisfy the Def Stan 00-055 objectives and identified Military Delta.

Note. PE open standards may not meet the full military requirements defined, eg cyber security, data safety and artificial intelligence are potential shortfalls for an open standard. Examples of adopted PE open standards, with Military Deltas are detailed in Def Stan 00-055.

L.6 Integrity Degradation

L.6.1 Integrity needs to be managed through life. There are a number of ways integrity can be impaired over time. Loss of integrity may be caused by:

a) Fatigue due to use of the PSS, eg a ship’s hull, which will weaken over time with stresses from normal operation;

b) Some technologies degrade over time, even if stored and not used due to corrosion or migration, eg tin-whiskers is a migration associated with thermal and chemical stresses, dendrites are migration associated with electrical field stress, silicon failures can be caused by doping migration;

c) Planned change, eg upgrading PSS due to obsolescence or legislative restriction, where the alternative component may not have the required performance or reliability so it reduces integrity;

d) The environment, outside the PSS, changes, eg includes new buildings/features affecting a terrain/map database;

e) The construction or development processes/tools changes, eg compilers used in the construction of PE of PSS;

f) New security vulnerabilities are discovered that highlight previously unconsidered causes of failure modes of PSS.

L.6.2 Management of integrity, through life, includes monitoring these and other factors which could undermine the integrity. It involves understanding both PSS usage, ie purpose and requirements, provenance of components and effective management of the supply chain.

Notes:

1. Health Monitoring and Reporting System is a tool that can assist in managing through life Integrity.

2. Integrity Management within the DAE is undertaken in accordance with RA5726.

Annex M
Adoption of Open Standards as an Acceptable Means of Compliance

M.1 Introduction

M.1.1 This Annex defines the adoption practices for the selection and use of an open standard proposed as an acceptable means of compliance for this standard. These are expressed in terms of considerations that a contractor should take into account and justifications expected to be produced to facilitate UK MOD acceptance of the proposal.

Note. There will be differences between UK MOD requirements associated with the unique military risk for PSS and civil requirements met by open standards. Open standards may not be specifically written for the development of military systems or for PSS used in a military context.

M.1.2 The term Military Delta refers to the evidence shortfall or gap between civil and military needs arising from the use of civil standards or Off-The-Shelf (OTS) solutions. The term includes any difference between UK and overseas military standards.

Note. An OTS solution may have been developed to a foreign military standard. In such cases the foreign military standard may be treated as an open standard. In such cases, there is likely to still be a difference between the standards.

M.1.3 Annex N and Annex O provide guidance on the adoption of a selection of open standards in common use. Inclusion should not be taken to imply a preference for use of those open standards, nor should exclusion be taken to imply that any other standard is unsuitable or unacceptable for adoption.

M.1.4 An open standard may not meet all the safety requirements necessary to meet Part 1 of this standard. contractors must complete the Compliance Matrices, as defined in the scope of contract, to justify the use of the selected open standard and identify the shortfalls.

M.2 Adoption Context

M.2.1 When adopting an open standard, the context of its application must be considered. This Annex addresses context where the PSS is developmental or un-modified Off-the-Shelf. Un-modified OTS PSS includes use in the context for which the PSS was designed, and alternate use of PSS without modification.

Note. For the purposes of this standard, OTS which is modified is to be considered developmental.

M.2.2 The scope of contract may cover multiple PSS. The considerations of this standard must be applied to each of these PSS, with particular attention paid to risks introduced by any proposed use of different open standards across different integrated PSS. In all cases this must be with reference to the higher system needs.

M.2.3 The contractor must ensure that the open 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 proposed open standard fails to fully address those safety requirements, the contractor must derive safety requirements that will address the shortfall.

Note. Open standards may have similar outcomes to this standard but could still generate shortfalls in meeting all the UK MOD safety requirements.

M.2.4 The contractor must ensure that the justification supporting the use of the proposed open standard is acceptable to the UK MOD.

M.3 Adoption Requirements

The contractor must ensure that shortfalls in evidence, supporting safety arguments, generated from the use of the open standard are addressed by considering the following top level adoption requirements.

M.3.1 Safety Requirements Definition

The contractor must ensure that application of the open standard will provide evidence that the PSS safety requirements are defined and justified.

Note. For the military context this will include:

a) Definition of boundaries and operating environment;

b) Definition of technical assumptions about interfacing systems (including systems-of-systems

c) Identification of relevant legislation, regulations, standards and policy;

d) Addressing the safety issues relating to the environment or loss of equipment;

e) Definition and traceability of technical safety requirements, derived safety requirements and design integrity requirements;

f) Appropriate application of safety requirements to multiple deliverables.

M.3.2 Safety Requirements Satisfaction

The contractor must ensure that application of the open standard provides evidence for the satisfaction of the safety requirements.

Note. For the military context this will include:

a) Availability and maintenance of evidence;

b) Production of all documentary deliverables;

c) Provision of diverse, comprehensive and trustworthy evidence;

d) Conducting contractor safety audits;

e) Access for UK MOD independent safety audits;

f) Analysis, documentation and treatment of shortfalls in the evidence;

g) Addressing design integrity principles.

M.3.2.1 The PSS risk assessment must provide sufficient evidence to enable the UK MOD to manage risk to life.

M.3.2.2 All hazards and associated potential accidents from all credible causes must be identified.

Note. A systematic safety analysis process must be adopted for military PSS, including but not limited to:

a) Addressing cyber security;

b) Carrying out human factors safety analysis;

c) Documenting hazards, related accidents and controls in the hazard log. (Some civil, open or other standards do not include use of a hazard log; in this case agreement will need to be reached with the UK MOD whether or not the intent of the standard is met).

M.3.2.3 The risk from the PSS must be reduced by the application of the ALARP principles during design, and a combination of mitigation strategies for hazards or failure modes that contribute to a hazard must be selected and implemented.

Note. This will include adoption of good practice and appropriate technical standards.

M.3.2.4 The status of all hazards and accidents must be visible to the UK MOD throughout the contract.

M.3.2.5 All assumptions and information necessary to enable safe integration or interoperation with other PSS must be recorded, including in a system-of-systems.

Note. This will include the definition and validation of technical interfaces with interfacing and interacting systems (including systems-of-systems), and the definition of the safety aspects of the interface in the ISSS.

M.3.2.6 Assurance must be provided that the relevant requirements of this standard are met throughout the supply chain.

M.3.2.7 Evidence must be provided that all safety requirements, including derived safety requirements, have been met.

M.3.3 Continued Satisfaction of Safety Requirements In-Service

The contractor must ensure that evidence is provided that the safety requirements can continue to be met in-service.

Note. Where the contractor is not employed through the in-service phase of the lifecycle, only para M.3.3.1 applies.

M.3.3.1 The contractor must ensure that the following are provided:

a) A command summary, providing essential safety information for commanders and managers;

b) Information on assumptions and limitations regarding the safe use of the PSS in-service;

M.3.3.2 Where the contractor supports the in-service PSS, they must ensure that the information set is maintained.

Notes.

1. This will include management of safety-related data in-service, and provision of a suitable configuration management framework to capture change. Def Stan 05-057 addresses configuration management, including giving domain-specific requirements.

2. This may require a monitoring, analysis and corrective action process to be agreed between the contractor and the UK MOD and, where relevant, other contractors.

M.3.3.3 Where the contractor supports the in-service PSS, they must provide evidence that safety analysis and risk assessment is carried out after any change that may affect the risk to life.

Note. Change can include change of use, change of operating environment or PSS modification.

M.3.4 Demonstrably Safe Service Provision

When the contractor is supporting the UK MOD by providing a service, they must ensure that evidence supports the argument that the service provision is safe.

M.3.4.1 safety case reports and Command Summaries are produced for the service.

M.3.4.2 Plans are developed for normal service provision, emergency situations and change to the service provision.

M.3.4.3 Service risk management processes are in place and meet ALARP principles.

Note. Where a service upon which a UK MOD military capability depends is provided by a contractor, 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 where the contractor has responsibility for a service and may necessitate demonstrable compliance with the ALARP principle.

M.4 Governance

The standard requires an agreed approach for governance which may vary between UK MOD regulatory domains. The approach must consider the proposed open standard and any requirements of the UK MOD policy or regulation. The governance must be agreed and formalised in the scope of contract.

Note. It is important to consider whether the governance arrangements for the proposed use of an open standard are compatible with the original intent.

M.4.1 The assessment of compliance for open standards can vary. When adopting an open standard, the assessment definition and measurement of compliance must be considered.

M.4.2 The contractor must support the safety committee, including any additional roles/tasks as agreed with the UK MOD.

Notes:

1. Safety activities must be coordinated with stakeholders by means of the safety committee.

2. Where the contract involves support, the safety committee must approve proposed changes to all PSS before they are implemented and ensure the proposed changes comply with domain regulatory requirements.

M.4.3 The contractor must provide the UK MOD with visibility of the safety engineering, support and safety management activities throughout the life of the contract.

M.4.4 The contractor must provide evidence of competence of individuals and organisations responsible for tasks that have a bearing on safety and their application in the military environment.

M.4.5 Whilst assurance will be covered in open standards, the UK MOD requires that independent safety audits are undertaken to provide assurance that safety activities comply with planned arrangements.

Notes:

1. The contractor will need to allow an ISA reasonable access to the information set.

2. Personally identifiable information, including contractor competence statements and evidence, may be subject to privacy law.

M.5 Applicability and Status

The contractor must provide a justification for the relevance of the open standard to the PSS in a military environment, and demonstrate that it represents current good practice.

Notes:

1. If a superseded or obsolete standard, or a standard that is not native to the domain, eg an automotive standard for avionics application, is proposed; it is likely to require more robust justification.

2. It may be necessary to supplement the open standard with additional process or governance to cover shortfalls, eg where the governing body has issued supplemental guidance or where the open standard is being applied outside its native domain.

M.6 Strategies for Managing Shortfalls

M.6.1 The contractor may propose mitigation strategies as a means of meeting shortfalls in evidence supporting the safety argument as a result of using the selected open standard (Part 1, 4.3 and 9.5).

Notes:

1. Adoption of an open standard may not mitigate the unique military risk.

2. Resulting shortfalls that introduce unacceptable risk may result in significant derived safety requirements that must be agreed with the UK MOD. This mitigation may include, but is not limited to:

a) Raising the design integrity, eg increasing integrity or assurance level within the chosen open standard;

b) Raising the level of assurance, eg by carrying out testing and analysis to more demanding coverage criteria;

c) Raising the level of scrutiny, eg by further independent review or scrutiny of the development artefacts;

d) Reducing dependence on critical components, eg by introducing redundancy or diversity within the PSS.

M.6.2 Where selected, the supplements to the open standard that address shortfalls should be expressed as derived safety requirements (Part 1, 9.5).

Annex N

Adoption of IEC 61508

N.1 Introduction

N.1.1 This Annex addresses the potential adoption of IEC 61508. IEC 61508 is an international standard for Electrical/Electronic/Programmable Electronic (E/E/EP) Safety-Related Systems. IEC 61508 is intended to be used pan-domain. It is the basis of many domain specific standards, eg ISO 26262 Road Vehicles Functional Safety. The contractor may propose standards derived from IEC 61508 with the agreement of the UK MOD using the adoption guidance in this Annex.

N.1.2 The guidance in this annex applies both where IEC 61508 is applied pre-development, and where a PSS that has already been developed to IEC 61058 is being procured by the UK MOD. In the latter case, retrospective work may be required to address all the requirements of this standard.

N.1.3 IEC 61508 is in seven parts, all of which are within the scope of this standard; however, Part 3, which specifically addresses software, can be applied through Annex C to Def Stan 00-055.

Note. This annex refers to the 2010 edition of IEC 61508 and identifies principles at the time of publication of this standard. Future updates to IEC 61508 may change details of the safety lifecycle and other clauses, and the contents of this annex will need to be interpreted accordingly.

N.2 Adoption Context

N.2.1 Apart from the exceptions detailed in the remainder of this Annex, IEC 61508 is deemed to address the contents of the following top-level adoption requirements:

a) Safety requirements definition;

b) Safety requirements satisfaction;

c) Continued satisfaction of safety requirements in-service.

N.2.2 IEC 61508 does not address Service Provision, and the contractor must undertake additional safety and engineering analysis to derive safety requirements and DLODs etc, to address the service provision requirement (Part 1, 16).

N.2.3 Key features of IEC 61508 are:

a) The adoption of an overall IEC 61508 system safety lifecycle for its technical framework. This contrasts with the requirements-based approach of this standard;

b) Functional safety assessment, to arrive at a judgement of the adequacy of the functional safety achieved by the IEC 61508 system, and to assess compliance with the standard.

N.2.4 IEC 61508 has no explicit requirement for a safety case, and the contractor must use the products of the safety lifecycle and functional safety assessment as the basis for constructing the safety case.

N.2.5 IEC 61508 uses a model of necessary risk reduction, which is the reduction of risk, from that posed by the basic Equipment Under Control (EUC) that has to be achieved to meet the tolerable risk for a specific situation.

N.2.6 This standard uses a top-down system engineering approach, apportioning the numerical risk to life to systems, sub-systems and components according to the ALARP principle. In contrast, IEC 61508 employs a bottom-up approach identifying an EUC, a control system, E/E/PE safety-related systems and other risk reduction measures. These distinctions are often not applicable to defence systems, although the concept of necessary risk reduction may be relevant to systems containing COTS, MOTS etc.

N.3 Adoption Requirements

N.3.1 Safety Requirements Definition

N.3.1.1 IEC 61508-1 Safety Lifecycle Boxes 1 to 5 and 9 are deemed to address the definition of safety requirements, including those safety requirements that contribute to the evidence of the safety of the PSS, provided that the contractor follows the guidance in the following paragraphs.

N.3.1.2 IEC 61508 defines Safety Integrity Levels (SILs) for specifying the target level of design integrity for the safety functions to be implemented by IEC 61508 safety-related systems. IEC 61508-5 provides examples of methods for the determination of SILs. The ALARP method (IEC 61508-5 clause B.2 and

Annex C) and quantitative method (IEC 61508-5 clause B.3 and Annex D) used together are deemed to comply with this standard. The risk graph, layer of protection analysis and hazardous event severity matrix methods are simplified methods that are unlikely to be suitable for PSS, except for simple, well-understood, low-risk systems, when they may be proposed with the agreement of the UK MOD.

N.3.1.3 The contractor must propose a generalisation of Safety Lifecycle Box 5 to address systems-of-systems and multiple deliverable PSS.

Note. The Safety Lifecycle boxes are simplified views, which is why further action is needed to capture systems-of-systems.

N.3.2 Safety Requirements Satisfaction

N.3.2.1 Safety Lifecycle Boxes 3 and 10 and clauses 6 and 8 of IEC 61508 are deemed to address evidence for the satisfaction of safety requirements provided that the contractor follows the guidance in the following paragraphs.

N.3.2.2 IEC 61508 contains a general requirement for documentation of the hazard and risk analysis, but the contractor must in addition comply with the requirements of this standard for the production of a hazard log and hazard log report.

N.3.2.3 IEC 61508 requires the production of a safety manual for compliant items, which covers many items of the ISSS. Where an ISSS is required under the terms of this standard, the safety manual for compliant items is deemed to be compliant with the addition of:

a) Context of in-service use;

b) Summary of the safety justification of the PSS.

N.3.2.4 The requirements of IEC 61508 on subcontracting are not compliant with the standard and will need to be revised and elaborated to ensure that the contractor can provide assurance that the relevant requirements of this standard are met throughout the supply chain, and to address the complexity of defence procurements, especially when systems-of-systems are to be developed.

Note. 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.

N.3.2.5 IEC 61508 contains detailed requirements on the safety management system and safety management plan that are deemed to be compliant with this standard provided that, within their IEC 61508 compliant SMS and SMP, the contractor ensures that:

a) The specific requirements of the SMP DID are addressed;

b) A point of contact responsible for safety is identified in the contractor's organisation;

c) Safety activities are coordinated with other contractors and government organisations;

d) Where there is no UK MOD safety committee, the contractor must establish governance that exercises, oversees, reviews and endorses safety management and safety engineering activities in the contractor's safety organisation;

e) The UK MOD safety committee is supported by contractor's personnel responsible for functional safety;

f) Governance arrangements are appropriate for the UK MOD regulatory domain, including identification of the designated posts within the UK MOD who can accept risks as being ALARP and tolerable and the process for referral of a risk that is not ALARP, on consideration of the risk to life, to an appropriate level within the UK MOD.

N.3.3 Continued Satisfaction of Safety Requirements In-Service

N.3.3.1 Safety Lifecycle Boxes 6, 14, 15 and 16 are deemed to comply with the requirements for continued satisfaction of safety requirements in-service in this standard provided that the contractor follows the guidance in the following paragraphs:

N.3.3.2 In addition to the in-service documentation required by IEC 61508, the contractor must produce a command summary in accordance with the requirements of this standard.

N.3.3.3 Incident reporting and analysis in accordance with IEC 61508 must be elaborated to address coordination between the contractor and the UK MOD operations and support authorities and other requirements of Clause 15 of Part 1 of this standard.

N.3.3.4 After modification or retrofit, the contractor must support the recertification process appropriate for the UK MOD regulatory domain.

N.4 Governance

N.4.1 IEC 61508 contains comprehensive requirements for functional safety assessment, which is an activity similar to the UK MOD's independent safety audit. The contractor must provide reasonable access by the UK MOD's ISA to the results of functional safety assessment. To avoid unnecessary duplication, the contractor may propose sharing the outputs from some activities carried out by its personnel and the UK MOD's ISA, provided this does not compromise the independence of the UK MOD's ISA.

N.5 Applicability and Status

N.5.1 For new development PSS, where IEC 61508 is proposed, the latest version should be used, together with relevant supplementary publications. Choice of an earlier version would require further justification identifying clear benefits of use of the version, and any perceived risks and their mitigation.

Note. Relevant supplementary publications in this context mean domain specific interpretations, eg IEC 61511 for Safety Instrumented Systems.

N.5.2 Versions of IEC 61508 before the 2010 version do not adequately address cyber security, and if an earlier version is proposed, the contractor must define additional means for meeting the requirements of this standard in this area.

N.6 Managing Shortfalls

N.6.1 The contractor must apply mitigation strategies as a means of meeting shortfalls in evidence as a result of applying IEC 61508.

Annex O
Adoption of MIL-STD-882E

O.1 Introduction

O.1.1 This Annex addresses the potential adoption of MIL-STD-882E. This is a US Department of Defense (DoD) system safety standard. It contains definitions and general requirements in Sections 3 and Section 4, which comprise the minimum mandatory definitions and requirements for an acceptable system safety effort for any DoD system. MIL-STD-882E Section 5 contains optional tasks covering management, analysis, evaluation and verification, which may be selectively applied in a specific contract to fit a tailored system safety effort.

O.1.2 The guidance in the Annex applies both where MIL-STD-882E is applied pre-development, and where a PSS that has already been developed to MIL-STD-882E is being procured by the UK MOD. In the latter case, retrospective work (eg conducting additional tasks) may be required to address all the requirements of this standard.

O.1.3 MIL-STD-882E addresses PE (eg in Section 4.4) as well as systems and hardware. The applicability of the PE requirements to UK defence procurement is considered in Def Stan 00-055.

O.1.4 MIL-STD-882E identifies tasks to support systems safety processes. The relevance of these tasks to compliance with this standard are identified in this adoption annex and where referenced must be applied.

Note. Where the contractor carries out other tasks in addition, the evidence generated by them may optionally be included in the safety argument.

O.1.5 The following MIL-STD-882E Tasks are referenced in this Annex:

a) Task 101 Hazard Identification and Mitigation Effort Using the System Safety Methodology;

b) Task 102 System Safety Program Plan - SSPP;

c) Task 104 Support of Government Reviews/Audits;

d) Task 105 Integrated Product Team/Working Group Support;

e) Task 106 Hazard Tracking System;

f) Task 108 Hazardous Material Management Plan;

g) Task 201 Preliminary Hazard List;

h) Task 202 Preliminary Hazard Analysis;

i) Task 203 System Requirements Hazard Analysis;

j) Task 204 Subsystem Hazard Analysis;

k) Task 205 System Hazard Analysis;

l) Task 206 Operating and Support Hazard Analysis;

m) Task 207 Health Hazard Analysis;

n) Task 208 Functional Hazard Analysis;

o) Task 209 System-of-Systems Hazard Analysis;

p) Task 210 Environmental Hazard Analysis;

q) Task 301 Safety Assessment Report;

r) Task 302 Hazard Management Assessment Report;

s) Task 303 Test and Evaluation Participation;

t) Task 401 Safety Verification.

O.2 Adoption Context

O.2.1 Apart from the exceptions detailed in the following paragraphs, MIL-STD-882E is deemed to address the contents of the following top-level adoption requirements:

a) Definition of safety requirements.

b) Achievement of safety requirements.

c) Continued satisfaction of safety requirements in-service.

O.2.2 MIL-STD-882E does not address service provision, and the contractor must undertake additional safety and engineering analysis to derive safety requirements, DLODs, etc to address the service provision requirement.

O.2.3 MIL-STD-882E is a process-based standard. Implementation of the standard should produce much of the evidence required to support the safety requirements, but without production of the safety case itself.

O.2.4 The contractor must carry out Task 301 and add a structured argument, supported by a body of evidence, to the safety assessment report to meet the requirement in this standard for a safety case.

O.2.5 In cases where an ISSS alone is sufficient, the contractor must propose a document based on the documentation defined by MIL-STD-882E Section 4 and Task 205, ensuring that it includes a safety justification.

O.2.6 The contractor must propose documentation based on Task 302 to meet the requirement for a safety case report.

O.3 Adoption Requirements

O.3.1 Definition of Safety Requirements

O.3.1.1 MIL-STD-882E Section 4 with Task 102 is deemed to comply with the requirements of this standard for the definition of safety requirements, provided that the contractor follows the guidance in the following paragraphs.

O.3.1.2 The contractor must ensure that safety requirements flowing from legislation, regulations, standards and policy relevant to the UK MOD are included in the safety requirements.

O.3.1.3 MIL-STD-882E does not address system design integrity requirements, and the contractor must propose a design integrity scheme that meets the requirements of this standard.

O.3.2 Achievement of Safety Requirements

MIL-STD-882E Section 4 with appropriate optional tasks is deemed to address the achievement of safety requirements, provided that the contractor follows the guidance in the following paragraphs.

O.3.2.1 MIL-STD-882E defines severity categories, probability levels and a risk assessment matrix for assessing and documenting risk. The contractor must revise and elaborate these for a system of risk estimation in terms of the risk to life and whether risks are ALARP and tolerable that can be used by the UK MOD as the basis for acceptance of risks.

Notes:

1. This system might include a risk class table, based on the risk assessment matrix that identifies broadly acceptable, tolerable, undesirable and intolerable risk classes.

2. Use of risk criteria such as domain specific risk matrices may be required by UK MOD policy or regulation.

O.3.2.2 The contractor must produce an SMP describing the systematic safety analysis process to be adopted. The adopted safety analysis process must be based on MIL-STD-882E Section 4 and Tasks 101, Task 102, Task 108 and Tasks 201 - 210, as required and tailored for the UK MOD procurement organisation.

O.3.2.3 The adoption of the optional analysis tasks must be commensurate with the complexity of the PSS.

O.3.2.4 The contractor must propose documentation meeting the requirements for a hazard log, which must be based on the Hazard Tracking System (HTS) described in MIL-STD-882E Section 4 and Task 106.

O.3.2.5 MIL-STD-882E does not directly address cyber security and the contractor must propose additional means for meeting the requirements of this standard for cyber security and data integrity.

O.3.2.6 The contractor must describe the safety aspects of the technical interfaces with interacting systems in the ISSS.

O.3.2.7 Sub-contracting is addressed in MIL-STD-882E Section 4 and Task 101 and Task 102. These must be revised and elaborated to ensure that the contractor can provide assurance that the relevant requirements of this standard are met throughout the supply chain.

Note. 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.

O.3.2.8 The contractor must ensure that, within their MIL-STD-882E compliant SSPP (Task 102):

a) The specific requirements of the SMP DID are addressed.

b) A point of contact responsible for safety is identified in the contractor's organisation.

c) Safety activities are coordinated with other contractors and UK government organisations.

d) Where there is no UK MOD safety committee, the contractor must establish governance that exercises, oversees, reviews and endorses safety management and safety engineering activities in the contractor's safety organisation (Task 104).

e) The UK MOD safety committee is supported by contractor's personnel responsible for safety (Task104 and 105).

f) Governance arrangements are appropriate for the UK MOD regulatory domain, including identification of the designated posts within the UK MOD who can accept risks as being ALARP and tolerable and the process for referral of a risk that is not ALARP, on consideration of the risk to life, to an appropriate level within the UK MOD.

O.3.2.9 The contractor must verify the achievement of the safety requirements by application of MIL-STD-882E Section 4, Task 401, Task 303, and safety audits in accordance with the SSPP (Task 102).

O.3.3 Continued Satisfaction of Safety Requirements In-service

O.3.3.1 The contractor must produce a command summary in addition to the MIL-STD-882E documentation.

O.3.3.2 The contractor must propose means to address the safety claim that the PSS is safely maintainable, which may be by management of life-cycle risk, MIL-STD-882E Section 4, and application of the optional tasks in accordance with MIL-STD-882E Appendix A, Table A-I.

O.3.3.3 The contractor must support a monitoring, incident reporting, analysis and corrective action system in place between themselves, UK MOD operations and support authorities and, where relevant, other contractors. This must be based on the relevant parts of Tasks 101, 102, 103 and 105.

O.3.3.4 The contractor must support recertification of the PSS after modifications by repeating the necessary parts of Section 4 and the optional tasks in accordance with MIL-STD-882E Appendix A, Table A I.

O.4 Governance

O.4.1 The contractor must propose, in their ITT, and agree with the UK MOD, a governance solution meeting all the criteria set out in Task 104 and Task 105. The support solution in Task 104 must include the UK MOD ISA (if appointed) and allow the UK MOD and ISA reasonable access to the information set.

O.5 Applicability and Status

O.5.1 For new development PSS, where MIL-STD-882E is proposed, the latest version should be used. Choice of an earlier version would require further justification identifying clear benefits of use of the version, and any perceived risks and their mitigation.

O.5.2 One specific issue is that the previous issue MIL-STD-882D does not define the optional tasks included in MIL-STD-882E. Some or all of these will be required to address aspects of the safety argument as described above, in which case the contractor will need to propose additional activities to cover the areas of the relevant optional tasks.

O.6 Managing shortfalls

O.6.1 The contractor must apply mitigation strategies as a means of meeting shortfalls in evidence as a result of applying MIL-STD-882E.

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.
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.
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.
AAMC	Alternative Acceptable Means of Compliance
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.
Military Delta	The evidence shortfall or gap between civil and military needs arising from the use of civil standards or OTS solutions.
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.
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
AERC	Airborne Equipment Release Certificate
ALARP	As Low As Reasonably Practicable
ALWRC	Air Launched Weapon Release Certificate
AAMC	Alternative Acceptable Means of Compliance
ARP	Aerospace Recommended Practices
ASEMS	Acquisition Safety and Environmental Management System
ASG	Acquisition System Guidance
ASIC	Application Specific Integrated Circuit
BS	British Standard
CADMID/T	Concept, Assessment, Demonstration, Manufacture, In-service, Disposal/Termination
CONDO	Contractors on Deployed Operations
COTS	Commercial Off The Shelf
CSA	Contractor Safety Auditor
DAE	Defence Air Environment
Def Stan	Defence Standard
DID	Data Item Description
DLF	Defence Logistics framework
DMR	Defence Maritime Regulator
DO	Document Order
DSA	Defence Safety Authority
DStan	UK Defence Standardization
EN	Norme Européenne
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 And Corrective Action System

GFX	Government Furnished Equipment (GFE) or Assets (GFA)
HSE	Health and Safety Executive
HTS	Hazard Tracking System
IEC	International Electrotechnical Commission
ISA	Independent Safety Auditor
ISAWG	Independent Safety Assurance Working Group
ISO	International Organisation for Standardization
ISSS	Information Set Safety Summary
ITT	Invitation To Tender
JSP	Joint Service Publication
MAA	Military Aviation Authority
MIL-STD	Military Standard
MOD	Ministry of Defence
MOTS	Modified/Military off the shelf
MRP	MAA Regulatory Publications
OTS	Off the Shelf - this included all variations of MOTS/COTS
PE	Programmable Elements
PLD	Programmable Logic Devices
POSMS	DE&S Project Oriented Safety Management System
PSS	Product, Services and/or Systems
RA	Regulatory Article
SRD	System Requirement Document
SMP	Safety Management Plan
SMS	Safety Management System
STPA	System Theoretic Process Analysis
URD	User Requirement Document
DLOD	Defence Lines of Development

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
Format Change	All	Requirements numbering has moved up 2 in number. For example section 7 now reads section 5. All appendices have been changed to Annexes.	Issue 6 uses an updated template to Issue 5
Part 2	All	Information pack containing Scope, triage of review feedback received and overlay document detailing changes from issue 5 to issue 6	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 01412/2021.

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.