Ministry of Defence

Defence Standard 00-055 Part 1

Issue 4 **Date:** **29 April 2016**

Requirements for Safety of Programmable Elements (PE) in Defence Systems

Part 1: Requirements and Guidance

Contents

Foreword

REVISION NOTE

Defence Standard 00-055, this Standard, has been raised to Issue 4 to update its content to include a Data Safety Annex and its' references, minor grammatical and textural errors and alignment with Defence Standard 00-056. Both these Standards incorporate government policy on Open Standards Principles.

The primary difference between Issue 3 and Issue 4 is the inclusion of a Data Annex; re-referencing to Def Stan 00-056 Parts, and minor text and grammar amendments.

IMPACT ON CONTRACTING

The Data Annex identifies that PE includes data and that Data Safety Requirements are a subset of the PE Safety Requirements. It sets requirement on the Contractor to ensure that the derived Data Safety Requirements demonstrate that the generation and use of data has achieved the PE Safety Objectives.

The impact on Contracting from Issue 3 to Issue 4 is minimal. It is expected that a systems engineering approach (scope of analysis) for PSS and PE delivery by a Contractor would have taken into account data. Annex E, Data Integrity, ensures that evidence supporting the achievement of the PE Integrity Objectives when generating or using data is documented.

This Standards' title number amendment, to comply with the revision by Defence Standardization on the Defence Standard numbering format (2 to a 3 digit) system, should have no effect on contracting to Issue 4 from Issue 3 this Standard.

HISTORICAL RECORD

This Standard supersedes the following:

Interim Defence Standard 00-55 Part 1 Issue 3, dated 12 Dec 2014

Defence Standard 00-55 Part 1 Issue 2, dated 01 Aug 1997

Defence Standard 00-55 Part 2 Issue 2, dated 01 Aug 1997

Interim Defence Standard 00-55 Part 1 Issue 1, dated 05 Apr 1991

Note. Issue 2 (Part 1 and 2) were declared Obsolescent on 29 Apr 2005 and withdrawn 12 Dec 2014

a) This Defence Standard (Def Stan) provides requirements and guidance for the achievement, assurance and management of safety of Programmable Elements (PE) within Products, Services and Systems (PSS). It can be applied to any MOD project and can be applied in any phase of a project's life. Defence Contractors shall use this Standard as required by Contract. This Standard also provides guidance for establishing a means of complying with the requirements for the management of safety of PE. The effective application of this Standard requires close co-operation between all parties, as the responsibility for the management of the PE contribution to PSS Risk to Life is shared.

Notes:

i. The **Notes** in this Standard provide a guide to establishing a means of complying with the requirements for the management of safety of PE. These **Notes** are not mandatory.

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

b) This Standard has been produced on behalf of the Ministry of Defence (MOD) by the Safety Standards Review Committee (SSRC) on behalf of the sponsor, Director Technical, MOD QSEP SEP. This Standard has been produced as an independent document to:

1) Meet the recommendation of the SSRCs' Software Safety Working Group (Subordinate to SSRC, selected PE subject matter experts).

2) Meet the Government Mandate for the implementation and use of Open Standards.

3) Capture the software specific requirements for Safety including consideration of Cyber security.

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

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

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

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

g) Further safety assurance reference material, which may be relevant to this Standard, may be found on the MOD Acquisition System Guidance (ASG). Published materials are subject to continuous review and development. Access to the ASG is via the Defence Gateway or Gov.uk websites.

0 Introduction

0.1 The Risk to Life associated with the failure or unintended behaviour of PE in PSS, including its integration, must be managed. This Standard uses the concept of Design Integrity to provide MOD with a means of determining whether the PE are fit for purpose for use in specified environments and applications.

Notes:

i. Def Stan 00-056 defines PE as; 'PSS that is implemented in software or programmable hardware, which includes any device that can be customised, eg ASICs, PLDs and FPGAs'. The terms, definitions and terminology used throughout this Standard are taken from Def Stan 00-056. Additional definitions can be found in Annex A.

ii. It can be argued that PE does not fail, rather that requirements are not correctly identified or implemented. Hence, the definition of failure mode from Def Stan 00-056 includes the term 'unintended behaviour' and has been introduced to ensure that where PE requirements have not been correctly identified or implemented, then the resulting functionality can validly be referred to as unintended behaviour.

iii. This Standard is concerned with the overall behaviour of PE; including cases where the use of data may lead to unintended behaviour.

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

Note. To enable safe operation of PSS, component PE will need to meet the required Design Integrity and fulfil the PE Integrity principles defined in Def Stan 00-056 Integrity and Open Standards Annex. PE cannot be safe or unsafe in itself, only in context of its role in a PSS; however the term PE Safety has been adopted as shorthand for 'the properties of PE which define its role in safety of the PSS'.

0.3 Lack of Design Integrity can lead to the unintended behaviour, or intentional misuse of PE. These may result in a hazard or impair mitigation of a hazard within the PSS and hence the MOD considers PE Design Integrity to be a significant safety issue. This Standard will allow the MOD to ensure appropriate Authorities are aware of the impact of PE unintended behaviour.

Notes:

i. Whilst this Standard expects unintended behaviour of PE to be reported, Contractors may not always be aware of PE unintended behaviour in operation. This can be addressed by ensuring suitable mechanisms for sharing information between MOD and the Contractor are captured within the scope of contract, which is likely to depend upon a number of factors including required Design Integrity and complexity of the PE and PSS.

ii. For the assessment of intentional misuse of PE, the concepts identified in Def Stan 05-135 and Def Stan 05-138 provide additional guidance to the Contractor.

0.4 This Standard sets MOD requirements on Contractors that enable the acquisition of PE that is compliant with safety legislation, regulations, and MOD policy. The intent is that compliance with these requirements will support the MOD in discharging its obligations with regard to the management of Risk to Life associated with the operation of military PSS.

0.5 Under UK law, all employers have a duty of care to their employees, the general public and the wider environment. For the MOD this includes, but is not limited to, an obligation to manage the Risk to Life associated with operation of military systems. In accordance with general guidance provided by the Health and Safety Executive, and as defined in Defence Safety Regulatory Publications (DSRP), 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 at least tolerable, unless legislation, regulations or MOD Policy imposes a more stringent standard.

0.6 Contractors who supply PE to the MOD, either as stand-alone PE or as part of a PSS, are subject to legal duties, which may vary with the place of manufacture and supply or operation. MOD shall have regard to the needs of Contractors to discharge their legal duties when interpreting and applying the requirements of this Standard.

0.7 Programmed logic or data in PE does not degrade in the same way as mechanical or chemical elements, it is susceptible to a range of systematic failures and it is usually not possible to subject it to exhaustive testing or analysis. As a result PE may not reveal certain unintended behaviour until particular combinations of system states and histories occur in service.

Notes:

i. The need to maximise the possibility of finding unintended behaviour could lead to prolonged analyses that may make the PE cost prohibitive. Therefore the analyses must be commensurate to the Design Integrity of the PE and apply the principles of ALARP. A number of Open Standards already cover this issue and further guidance regarding the choice of such standards is contained in Annex B.

ii. For PE development, this may be achieved by careful use of software and electronic engineering, Quality Assurance and Safety Management processes appropriate to the Design Integrity. For pre-existing PE, it is possible that this work has already been undertaken and where this is not the case, the Contractor will need to propose how the pre-existing PE unintended behaviour can be identified.

iii. Issues relating to the random hardware faults and physical reliability of a device, eg wear out or degradation of device memory, are not covered by this Standard. Application of this Standard may result in the identification of random hardware reliability considerations and may lead to additional PSS activities and new Derived Safety Requirements (DSRs).

0.8 PE is vulnerable to inappropriate intentional and unintentional change due to its ease of access and modification, particularly when in the supply chain and during maintenance. In this Standard, PE vulnerabilities are treated as potential causes of unintended behaviour, in safety-related PE. This vulnerability includes functionality change or enabling access to critical data.

0.9 This Standard has 5 objectives derived from the 5 PE Integrity principles defined in the Def Stan 00-056 Integrity and Open Standards Annex. Achievement of these objectives and the mandatory Requirements in this Standard provide the means of assurance and management of Design Integrity for PE acquisition and through-life support. This Standard also provides guidance on establishing an acceptable means of compliance for these requirements. However, it is not the intent of this Standard to describe or outline specific types of analysis or evidence.

0.10 The strategy of this Standard is to enable the application of an Open Standard that demonstrably satisfies the objectives and clauses of this Standard. Open Standards may not meet the full military requirements defined in this Standard and the Military Delta may need to be identified and satisfied. Examples of PE Open Standards, with Military Deltas identified, can be found in Appendices to Annex B. Essentially this Standard enables the use of Open Standards as an acceptable means of compliance.

Requirements for Safety of Programmable Elements (PE) in Defence Systems - Part 1: Requirements and Guidance

1 Scope

1.1 This Standard specifies the requirements for achieving, assuring and managing the Design Integrity of PE in PSS. This includes PE used by, or on behalf of, the MOD, and covers the whole-life support of the PE, as defined by the scope of contract.

Note. The Standard can be applied to a single or multiple PE as defined in the scope of contract.

1.2 Whilst Contract life may be limited, this Standard considers the whole life of the PE including disposal. The disposal procedures are defined in the Defence Logistics Framework, available through the Defence Gateway. Earlier phases in the life of the PSS need only be considered if explicitly included within the scope of analysis. Applicability relates to all situations and scenarios, including but not limited to trials, operations and training for operations as defined in the scope of contract.

1.3 This Standard provides for the application of Open Standards supported by Recognised Good Practice (RGP) as an acceptable means of managing compliance of the PE with its Safety Requirements, within the scope of contract.

Notes:

i. Many definitions of the term Open Standard exist. For the purpose this Standard, the criteria provided in Annex 1, Section 2 of Open Standards Principles apply.

ii. Guidance regarding the choice of standards or the adoption of a PE Open Standard is covered in Annex B to this Standard.

iii. The preferred route of compliance is the application of RGP through an adopted PE Open Standard, with proven pedigree, that meets the objectives and requirement of this Standard. Although this Standard defines RGP, it is the responsibility of the Contractor to propose and justify the use of RGP as an acceptable means of compliance.

1.4 It is MOD policy to use civil standards where possible and military standards only as necessary. Due to the specialised operational environment in which the MOD uses PSS, the application of PE Open Standards and RGP may not meet all Design Integrity requirements. Where there is a shortfall in achieving PE Design Integrity requirements, this Standard makes provision for the use of enhanced RGP or augmented PE Open Standards to ensure compliance with Design Integrity requirements. A number of PE Open Standards provide alternative means of compliance, this Standard allows for these alternatives to augment the chosen PE Open Standard to address the identified PE Design Integrity shortfall.

Note. Guidance addressing the unique military risk requirement and impact on PE Open Standards (Military Delta) is contained at Annex C.

1.5 PE may be developed separately from the non-PE components of a PSS or supplied as Off the Shelf (OTS), and hence there is a risk of incompatibility and a need for careful consideration of the overall integrated system functionality. It is essential that sufficient PSS information is available to enable PE Failure Assessment to be undertaken.

Notes:

i. Undertaking PE Failure Assessment is essential for determining the behaviour of the PE that may contribute to PSS hazards and thereby help identify required Design Integrity. This cannot be undertaken without knowledge of the PSS. If the PE will not credibly contribute to a hazard or impair mitigation to a hazard, then the Contractor, with the agreement of the MOD, need take no further action in this Standard.

ii. This Standard is intended for all PE acquisition and its clauses are applicable to developmental as well as OTS PE.

iii. Where knowledge of the PSS is incomplete, it is likely that assumptions will be made. Such assumptions will need to be documented and where possible, validated. This may be accomplished through the use of independent assessment.

iv. It is possible that the PSS system integrator has already undertaken a risk assessment and the resulting PE Design Integrity is provided as Derived Safety Requirements (DSRs).

v. The risk of incompatibility between the PE and PSS can be mitigated by maintaining good communications between the Contractor and the PSS system integrator to enable sufficient access to PSS information. Requirements for the sharing of information are derived from the interfacing clauses of Def Stan 00-056 Part 1 and are covered in more detail in this Standard.

1.6 The aim of this Standard is to be technology agnostic and it is intended to be applied to all current and emerging PE related technologies.

1.6.1 Where PE technologies are not covered by this Standard, a mitigation strategy based on the sensible application of the assurance requirements will be used to satisfy the Design Integrity shortfall.

Notes:

i. For this Standard to be truly technology agnostic, all current and emerging technologies should be in scope. It is unlikely that this can ever be fully achieved, but this Standard has been written with this aspiration and will be reviewed in accordance with current DStan policy.

ii. Any mitigation strategy will be agreed by the Safety Committee.

2 Warning

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

3 Normative References

3.1 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 3.2, 3.3 & 3.4 below for further guidance), if you are having difficulty obtaining any referenced standard please contact the DStan Helpdesk in the first instance.

ARP 4754A	Guidelines for Development of Civil Aircraft and Systems
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
Def Stan 00-056	Safety Management Requirements for Defence Systems
Def Stan 00-970	Design and Airworthiness Requirements for Service Aircraft
Def Stan 05-057	Configuration Management of Defence Materiel
Def Stan 05-135	Avoidance of Counterfeit Materiel
Def Stan 05-138	Cyber Security Considerations for Defence Suppliers
DO-178	Software Considerations in Airborne Systems and Equipment Certification
DO-254	Design Assurance Guidance for Airborne Electronic Hardware
DO-333	Formal Methods Supplement to DO-178C and DO-278A
DSRP	Defence Safety Regulatory Publications
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
ISO 26262	Road Vehicles - Functional Safety
ISO 9001	Quality Management Systems - Requirements
JSP 440	The Defence Manual of Security
MIL-STD-882	Department of Defence Standard Practice - System Safety
Data Safety Guidance	Data Safety Guidance (ISBN 9781519533579)
Open Standards Principles	Open Standards Principles: For software interoperability, data and document formats in government IT specifications

Notes:

i. When this Standard is used, the Def Stan 00-056 reference is to the extant published Issue.

ii. For other references the latest version should be used, unless the clause specifically identifies a legacy version.

iii. As many PSS will be procured from international sources, international standards have been referenced. National equivalents will be identical, eg BS EN 61508 or BS ISO 26262.

3.2 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 supersessions might be made. For some standards the most recent editions shall always apply due to safety and regulatory requirements.

3.3 In consideration of clause 3.2 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.

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

4 Definitions

4.1 Terms and Definitions

For the purposes of this Standard, the terms and definitions detailed in Def Stan 00-056 apply, together with specific definitions for this Standard, which are provided at Annex A.

4.2 Mandatory Requirements

A requirement which uses the word ‘shall’ identifies the clause or sub-clause as mandatory. Sub-clauses using the word ‘should’ allows the Contractor the opportunity to consider an alternative approach in meeting the sub-clause.

5 Abbreviations

AOF Acquisition Operating Framework
ALARP As Low As Reasonably Practicable
ASEMS Acquisition Safety and Environmental Management System
ASIC Application Specific Integrated Circuit
COTS Commercial Off the Shelf
Def Stan Defence Standard
DID Data Item Description
DSR Derived Safety Requirement
DSRP Defence Safety Regulatory Publications

DStan	UK Defence Standardization
FHA	Functional Hazard Analysis
FPGA	Field Programmable Gate Array
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
IP	Intellectual Property
IPR	Intellectual Property Rights
ITT	Invitation to Tender
ISA	Independent Safety Auditor
ISO	International Organisation for Standardization
ISSS	Information Set Safety Summary
JSP	Joint Service Publication
MOD	Ministry of Defence
MOTS	Modified/Military Off the Shelf
OTS	Off the Shelf - this included all variations of MOTS/COTS
PE	Programmable Elements
PESMP	Programmable Elements Safety Management Plan
PESS	Programmable Elements Safety Summary
PLD	Programmable Logic Devices
POSMS	Project Orientated Safety Management System
PSS	Products, Services and Systems
RGP	Recognised Good Practice
RTCA	Now RTCA, Previously Radio Technical Commission for Aeronautics
SIL	Safety Integrity Level
SMP	Safety Management Plan
SMS	Safety Management System

6 PE Safety Management

6.1 Relationship to Defence Standard 00-056

Where this Standard has been invoked in order to satisfy the requirements of Def Stan 00-056 Part 1; the Contractor shall ensure the PE Safety Requirements are met by their application of this Standard by inclusion or by producing PE specific documents.

Notes:

i. This Standard has been written to complement Def Stan 00-056 and allows for the use of existing documents and/or PE specific documents which might be an output from the application of chosen PE Open Standards.

ii. It is the responsibility of the owner of the Def Stan 00-056 scope of contract to ensure that any PE Safety Requirement is defined, and the owner of the PE scope of contract meets the PE Safety Requirement through the application of this Standard.

iii. The definition of a system in Def Stan 00-056 includes data as an element. In the context of this Standard Data Safety Requirements are a subset of PE Safety Requirements.

6.1.1 Where this Standard has been invoked without Def Stan 00-056, the Contractor shall ensure that the management of PE Safety is undertaken through:

a) An appropriate Safety Management System (SMS) which aligns with the safety principles of Def Stan 00-056, and;

b) An agreed scope of contract that addresses the management requirements of Def Stan 00-056.

Notes:

i. If this Standard has been invoked without Def Stan 00-056, then the Contractor can demonstrate equivalence in compliance to other safety standards, in addition to the requirements of this Standard.

ii. The scope of contract will address the following management sections of Def Stan 00-056, Part 1:

1) Section 2, - 7, General Requirements, clauses 7.1 to 7.5, and 7.7.
2) Section 2, - 8, Roles and Responsibilities, all clauses.
3) Section 2, - 9, Interfaces, all clauses.
4) Section 2, - 10, Safety Audits, all clauses.
5) Section 3, - 12, Health Monitoring and Reporting System.

6.1.2 The Contractor shall agree with the MOD the extent (scope of supply) and depth (scope of analysis) of the PE Safety Evidence.

Notes:

i. The PE and PSS interfacing boundaries will be identified in the scope of contract and may drive or constrain the depth of the required analysis to provide suitable and sufficient evidence.

ii. The scope of supply and scope of analysis will vary depending upon a number of factors that might include, but not be limited to, PE Design Integrity, choice of standard, and the needs of the MOD to maintain visibility of the PE through the acquisition process.

iii. PE Open Standards may advocate alternative techniques. This Standard allows for the use of additional RGP techniques to make good any shortfall in meeting Design Integrity requirements for PE.

iv. Where the PE includes the use of OTS elements, the Contractor may be required to identify appropriate evidence justifying the suitability of those elements.

6.1.3 As a minimum, the scope of analysis shall cover the identified hazards, or unintended behaviour, related to the PE.

Notes:

i. This clause specifically requires that the identified hazards or unintended behaviour is captured within the scope of analysis. As the design evolves or use of PSS changes PE Failure Assessment may impact the scope of analysis.

ii. Contractors are to be aware that this clause will be impacted by the choice of PE Open Standard, which may have specific analysis requirements.

iii. Contractors are to be aware that some PE Open Standards may not meet the Data Safety Requirements identified in Annex E.

6.1.4 The Contractor shall produce documentary deliverables relevant to PE Safety including a PE Safety Summary (PESS) report, with interim versions as defined within the scope of contract.

Notes:

i. The scope of contract will determine which documentary deliverables are required, which will in turn depend upon the chosen PE Open Standard and any use of existing documents invoked through Def Stan 00-056. The PESS report is the only mandatory documentary deliverable from this Standard and is intended to support or be incorporated into the Information Safety Set Summary (ISSS) from Def Stan 00-056. The PESS report as a deliverable is covered as a Data Item Description (DID) in Annex D to this Standard.

ii. Provision is also made in Annex D to this Standard for a PE Safety Management Plan (PESMP) DID. However, it is acceptable for the aspects of PE management to be contained within the Safety Management Plan (SMP) from Def Stan 00-056 or equivalent alternatives where mandated from the chosen PE Open Standard.

iii. Where the PE includes the use of OTS elements, the use of existing documentation may be considered appropriate to support but not replace the PESS report.

6.1.5 Agreement of both scope of supply and scope of analysis shall be recorded formally and captured within the PESMP or SMP as appropriate.

6.1.6 The Contractor should define a PESMP and carry out a preliminary PE Failure Assessment as part of the tendering process and formalise and agree the plan and assessment findings with the MOD at Contract award.

Notes:

i. Def Stan 00-056 gives some guidance on tendering and other pre-contract activities necessary to agreeing a scope of contract at Contract award.

ii. The detail of the PESMP might not be complete at ITT stage. As a consequence there may be substantive work to be undertaken in formalising the SMP during Contract negotiations and from Contract award. The PESMP and assessment findings must be agreed with the MOD.

iii. The ITT PESMP may contain the preliminary PE Failure Assessment findings. An ITT PESMP or a preliminary PE Failure Assessment may not be required where this Standard has been invoked with Def Stan 00-056.

6.2 PE Safety Governance

The Contractor shall ensure that the management of PE Safety is undertaken within an appropriate SMS which identifies the organisation, roles and responsibilities suitable for achieving PE Design Integrity.

Note. Although this requirement is normally met through compliance with Def Stan 00-056, the need to apply Open Standards may result in a SMS that is both compliant with Def Stan 00-056 and the chosen PE Open Standard.

6.2.1 The Contractor shall justify and agree with the MOD an SMS that demonstrates suitable governance for the proposed PE Open Standard.

Notes:

i. Def Stan 00-056 expects an SMS to provide the framework for the Contractor's organisation to direct and control its safety management activities, including the organisational structure, processes, procedures, techniques, methodologies and interfaces with other organisations which will include the PSS system integrator.

ii. When using an agreed PE Open Standard use of the associated governance processes is encouraged.

6.2.2 The agreed means of governance shall be recorded within the scope of contract and captured within the SMP or the PESMP.

6.3 PE Information Sharing

The Contractor shall communicate, cooperate, and share PE information and documentation with MOD, other organisations and stakeholders responsible for each interfacing PSS regarding their integration into platforms and larger systems.

Notes:

i. This clause addresses potential management issues that can lead to incorrect implementation of PE requirements and re-emphasises the need to manage effective coordination of organisational and technical interfaces highlighted in Def Stan 00-056. This is especially important for PE, within a PSS, which very likely forms part of a larger PSS. The documentation defined within the scope of supply identifies which other organisations; stakeholders and MOD personnel can have access to the PE information and ensure it is shared in accordance with the scope of contract.

ii. Similarly, PSS information pertinent to the development of the PE will be available to the Contractor to enable effective management of the PE development. The Contractor can request PSS information to conduct PE Failure Assessment which may have an impact on the scope of contract where it is necessary to cover other sources of information.

iii. The extent of information for OTS PE may vary, which makes the need to share what information and documentation there is, very important and may warrant consideration of contract amendments (scope of contract) in order to access such information or documentation.

6.3.1 The Contractor shall communicate, cooperate, and share PE information and documentation with MOD Duty Holders, organisations and stakeholders responsible for each PSS regarding their operational use.

Notes:

i. PE operational use information, including limitations and assumptions can be documented in the PESS report.

ii. This clause equally applies for the use of other safety management standards. In such circumstances and unless specified in the scope of supply, the Contractor can either capture this information in an existing document or a dedicated report.

6.4 Fulfilling the Principles

To demonstrate that the PE Integrity principles defined in the Def Stan 00-056 Integrity and Open Standards Annex have been fulfilled, the Contactor shall ensure that the following PE Safety Objectives are achieved.

6.4.1 Objective 1

PE Safety Requirements shall be defined to manage the PE contribution to PSS hazards.

Notes:

i. This is met through activities that define PE Safety Requirements that are: unambiguous, comprehensible, internally consistent, feasible, valid and verifiable.

ii. PE Safety Requirements are usually allocated from the systems engineering and safety assessment activities, but may also emerge during the PE development lifecycle as DSRs. Where any OTS PE is to be used, the capability of the OTS PE to meet the PE Safety Requirements needs to be demonstrated to enable the satisfaction of all the PE Safety Objectives.

iii. PE Safety Requirements may also be derived from compliance with safety legislation, regulations, standards or MOD policy, and/or requirements. These requirements and their mitigation strategies can be realised by stating them in the Contract.

iv. PE Safety Requirements derived from PSS are usually validated at the PSS level. This validation is necessary to satisfy the PE Safety Objectives. The boundary of validation will be defined in the scope of contract**.**

6.4.2 Objective 2

PE Safety Requirements shall be maintained throughout requirements decomposition.

Note. This is met through activities that assure and demonstrate that the PE Safety Requirements have been established and preserved throughout requirements decomposition to the implementation.

6.4.3 Objective 3

PE Safety Requirement satisfaction shall be demonstrated.

Note. This is met by activities that generate and communicate evidence that all the PE Safety Requirements have been demonstrably satisfied.

6.4.4 Objective 4

Hazardous behaviour of the PE, including generation and use of data shall be identified and mitigated.

Notes:

i. This is met by activities that generate evidence that all PE unintended behaviour and emergent properties due to normal behaviour, that may have an impact on PSS Risk to Life, have been controlled and mitigated. This Standard's strategy is achieved by:

1) PE Failure Assessment to identify DSRs, either to mitigate the effects of the unintended behaviour, or to make them less likely to occur.

2) Applying RGP and the chosen PE Open Standard to meet the DSRs.

ii. It is recognised that the impact on PSS Risk to Life from PE Failure Assessment, can only be determined at the systems level. This will require the Contractor to have knowledge of or access to relevant PSS information.

iii. PE Failure Assessment determines whether any PE functionality does anything that is unsafe. These emergent causes of normal and unintended behaviour and/or properties may generate DSRs.

iv. PE Failure Assessment is likely to generate DSRs as the design evolves.

6.4.5 Objective 5

The confidence established in addressing the (other) PE Safety Objectives shall be commensurate to the contribution of the PE to PSS risk.

Notes:

i. This Standard enables confidence to be established through the undertaking of the following:

1) Identification of PE Design Integrity requirements, including the unique military risk, from PE Failure Assessment activities, and;

2) Choice and proposal of an appropriate standard commensurate to the PE Design Integrity requirements, including identification of the Military Delta, and;

3) The correct application of the chosen PE Open Standards or standard will produce appropriate evidence whose extent is commensurate with contribution of the PE to PSS risk.

ii. The confidence from the correct identification of PE Design Integrity requirements needs to be maintained throughout the lifecycle.

7 General Requirements

7.1 Requirements Definition

The Contractor shall ensure that PE Safety Requirements are correctly identified so that they are specified, unambiguous, comprehensible, internally consistent, feasible, valid and verifiable (Objective 1).

Notes:

i. In the context of PE any Safety Requirement has a number of possible components which may include:

1) Functional behaviour.

2) Integrity considering both random and systematic failures.

3) Independence from other elements.

4) The data consumed, processed and/or generated.

ii. Functional PE Safety Requirements derived from PSS are usually validated at the PSS level. Identified PSS level validation shortfalls, will become DSRs included in the scope of contract to ensure satisfaction of the PE Safety Objectives.

iii. It is particularly important that the requirements are verifiable to enable demonstration. The demonstration and satisfaction is addressed through PE Safety Evidence.

iv. PE Failure Assessment is the main mechanism for checking the feasibility and validity of PE Safety Requirements along with the selection of the appropriate PE Open Standard. The PE Failure Assessment also assists in confirming that the scope of contract is correct, or requires amendment.

7.2 PE Failure Assessment

The Contractor shall identify and assess the consequences of PE behaviour within the intended military operational environment (Objective 4).

Notes:

i. This requirement fulfils Objective 4 in terms of the identification of emergent causes or unintended behaviour and is essential to determine the presence of hazard causes and their impact upon PSS Risk to Life. This assessment applies to normal as well as unintended behaviour and is carried out to determine the PE Design Integrity requirement even if the parent PSS safety assessment has not allocated a Design Integrity requirement to the PE. This is to cover the circumstances where PE unintended behaviour leads to an emergent hazard, eg System of Systems impact.

ii. There may be a variety of means for identifying and assessing the consequences of PE unintended behaviour, and this Standard refers to these techniques as PE Failure Assessment. This requirement enables the Contractor to determine whether the PE is safety-related and is effectively a Def Stan 00-056 requirement.

iii. It is entirely possible that PE Failure Assessment has been undertaken through Def Stan 00-056 (or alternative safety standard) generating the DSRs (Objective 1). If so, the Contractor can refer to this evidence as fulfilment of this requirement. If not, the Contractor can employ a suitable technique for identifying the safety impact of PE within the context of the PSS, also ensuring that the Functional PE Safety Requirements are feasible and valid.

iv. PE Failure Assessment will need to be carried out as an iterative process whenever changes are made to the design or use of the PE.

v. There are numerous techniques that might be appropriate depending upon the complexity of the functionality within the PE and the knowledge and expertise of the safety analysts. This might include techniques such as Hazard and Operability Study (HAZOP) or Functional Hazard Assessment (FHA), although it is not the purpose of this Standard to mandate any one technique.

vi. PE Failure Assessment may identify PE unintended behaviour that impacts Cyber security or Mission performance. If this occurs, the impacts are to be reported to MOD. For Cyber security, the Contractor can be guided by the principles contained within JSP 440, Def Stan 05-135, and Def Stan 05-138.

7.2.1 The Contractor should request sufficient access to PSS information to enable PE Failure Assessment to be undertaken.

Notes:

i. PE Failure Assessment can be undertaken at the PSS level by an appropriate authority, with appropriate input from the Contractor, but will need to be revisited as the design evolves or use of the PSS changes. The scope of contract can be used to enable the Contractor to gain access to relevant PSS information, or be informed of the PE Design integrity, which can also identify the extent and how PSS information can be shared.

ii. There may be circumstances where there is insufficient information to determine what impact the PE unintended behaviour has upon hazards.

7.2.2 Where there is insufficient PSS information to determine the impact of PE unintended behaviour upon hazards, or to fully identify and assess the consequences PE unintended behaviour, resolution shall be sought through the Safety Committee.

Note. Where appropriate, the Safety Committee will agree and sentence remedial action, which may include PE Failure Assessment being undertaken by the appropriate authority at the PSS level.

7.2.3 The Contractor shall record the results of PE Failure Assessment in the PESS report (Objective 4).

Notes:

i. This requirement fulfils the first part of Objective 4. Identifying the consequences of PE behaviour is key to deriving the Design Integrity requirements such as:

1) Selection of a management framework eg Safety Integrity Levels (SIL), Design Assurance Levels, Software Levels, etc.

2) The standards and processes that will be used to gather the required evidence.

ii. Even if there is no hazardous behaviour that can credibly occur from PE, the Contractor will document the findings of PE Failure Assessment, recording this as evidence that there are no Design Integrity requirements and informing the MOD of this outcome.

iii. Once the MOD or its representative has accepted that the PE will not credibly contribute to a hazard or impair mitigation of a hazard and recorded the result in the PESS, then the Contractor need take no further action in this Standard. At the PSS level, the PESS may have to be referenced in the relevant Safety Cases.

7.3 Mitigation of Credible Hazards

Where PE Failure Assessment identifies that the PE behaviour could credibly result in a PSS hazard, or impairs mitigation of a PSS hazard, all clauses of this Standard shall apply (Objective 4).

Note. Having determined PE behaviour could credibly result in a PSS hazard or impair mitigation of a hazard; this requirement simply requires the rest of this Standard to be followed and fulfils the second part of Objective 4.

8 Standards Selection, Agreement and Design Integrity

8.1 Standards Selection

The Contractor shall propose PE Open Standard(s) supported by RGP for PE, and provide justification in the PESMP or SMP as appropriate.

Notes:

i. This Standard recognises that there are numerous PE Open Standards that can satisfy the majority of Design Integrity requirements to address Risk to Life for the military.

ii. It is for the Contractor to determine which PE Open Standard is appropriate for the domain in which the PE will operate and will enable the Design Integrity requirements to be met. Guidance on adoption and application of PE Open Standards is available in Annex B to this Standard.

iii. The proposal will need to contain justification for the appropriateness of the PE Open Standard together with evidence that the Contractor is suitably experienced in applying the PE Open Standard. The evidence may include previous examples of similar PE used in a similar context.

iv. It is anticipated that the proposal of one PE Open Standard will be sufficient for most cases, but if more than one PE Open Standard is proposed, the Contractor will need to justify the use of multiple standards and ensure the requirements of the proposed PE Open Standards do not conflict.

v. The choice of PE Open Standards may need to be supported by RGP in order to meet the Design Integrity requirements, some PE Open Standards offer options to achieve this. Although this Standard defines RGP, it is the responsibility of the Contractor to propose and justify the use of RGP as an acceptable means of compliance.

vi. Where the PE includes the use of OTS elements, the Contractor will be expected to justify the standards used in the development of those elements.

8.2 Agreement of Standards

The Contractor shall obtain formal agreement of the MOD that any proposed standards are an appropriate means of compliance with the PE Safety Requirements (Objective 5).

Note. It is expected that the Contractor will be competent to make an appropriate proposal regarding the choice of PE Open Standard, but the MOD still requires to agree, and retains the right to refuse that agreement if the proposal is considered inappropriate.

8.2.1 The PESMP, SMP or accepted alternative plan shall be used to record the justification and formal agreement of the use of the identified PE Open Standard(s).

Notes:

i. The PESMP as a deliverable is covered as a DID in Annex D to this Standard. However, it is feasible for the Contractor to use the SMP to record the choice of standard where this Standard is invoked with Def Stan 00-056.

ii. The chosen PE Open Standard may also mandate the use of a plan and as long as the intent of the PESMP DID is met, then such plans can be considered an acceptable means of compliance.

8.3 Capturing Design Integrity

The Contractor shall identify the Design Integrity requirements using the scheme specified in the selected PE Open Standard or standards and ensure that the PE Failure Assessment defines the required DSRs (Objectives 1, 4 and 5).

Notes:

i. This requirement enables the Contractor to determine the Design Integrity and is effectively a Def Stan 00-056 requirement. In some cases it is possible that this assessment will be confirming a previous Def Stan 00-056 analysis and identified DSRs for a particular PSS.

ii. Def Stan 00-056 covers a wider consideration of Design Integrity; whereas this Standard specifically relates to the Design Integrity of the PE.

iii. Where the PE includes the use of OTS elements, the Contractor will be expected to demonstrate the Design Integrity of those elements, or how any shortfall can be mitigated.

iv. The results from PE Failure Assessment are also a means of identifying unique legislation, regulations and standards for the candidate PE implementation technologies.

v. Some PE Open Standards do not identify data within their Design Integrity requirements, in these cases the PE Failure Assessment needs to consider Annex E.

8.3.1 Where there is a shortfall in evidence to support Design Integrity within the PE, the Contractor shall make use of replacement or enhanced PE Open Standards to enable satisfaction of those Design Integrity requirements (Objective 5).

Notes:

i. The purpose of this Clause is to address the potential shortfall of evidence when applying PE Open Standards, particularly in a military context (Military Delta). This Clause allows the Contractor to consider the use of alternative standards or enhanced standards to support additional Design Integrity requirements.

ii. Further guidance on addressing the Military Delta shortfall is provided in Annex C. Guidance regarding the choice and use of replacement or enhanced standards is provided at Annex B, Annex C, and Annex E.

8.3.2 When applying the chosen PE Open Standard to satisfy Design Integrity, the Contractor shall consider Cyber security and Mission performance with regard to inappropriate intentional and unintentional change to PE (Objective 4).

Notes:

i. This Clause partially meets Objective 4. The Contractor will need to evaluate normal and unintended behaviour of the PE and potential for misuse, considering at least the following:

1) Viruses or unauthorised code,

2) Unauthorised installation, change or deletion, or modification of its function by additional or modified physical devices or installed PE, and

3) The installation or use of unauthorised PE, (eg running games or office applications), if these risks are not already included in PE Failure Assessment or PSS safety assessment for the specific equipment or sub-system.

4) Intentionally or unintentionally malformed data.

5) Counterfeit PE, eg software libraries sourced from untrusted agencies.

ii. Although good practice in Configuration Management may prevent some of the above issues, the Contractor will have to consider the requirements in Def Stan 05-135 and 05-138 to manage shortfalls.

9 PE Management

9.1 Safety Requirement Traceability

The Contractor shall ensure, maintain and provide evidence of PE Safety Requirements traceability throughout the lifecycle and as defined in the scope of contract (Objective 2).

Notes:

i. Typically, PE Safety Requirements will progress from more abstract to more concrete implementation. Consequently these requirements will be refined, decomposed, allocated and interpreted. Contractors are to ensure that the safety intent is not lost through this process and that it is clear how these requirements drive design and how the design meets each requirement.

ii. The depth and thoroughness of traceability applied will be commensurate with the Design Integrity of the PE. Various approaches can be used to develop evidence of traceability, e.g. formal refinement.

iii. PE Safety Requirements traceability will need to be managed at all stages of the lifecycle to a rigour and depth determined by the PE Design Integrity.

9.2 PE Configuration

The Contractor shall capture, document and maintain the Configuration Status of the PE, and its relationship to the PSS configuration, throughout the life of the Contract.

Notes:

i. It is essential that the Configuration Status or build state of the PE is known throughout the life of the contract to ensure that PE Failure Assessment is conducted against an established and understood configuration of the PSS. This will include development configurations as well as in-service operational configurations.

ii. The Contractor needs to capture, document and maintain the Configuration Status of all evidence supporting the PESS report, PSS Safety Case or ISSS as specified within the scope of contract.

iii. Configuration Management will permit the capture and maintenance of the Configuration Status and ensure that the Configuration Management system is capable of accurately documenting that status. Def Stan 05-57 addresses configuration management and includes domain-specific requirements.

9.3 PE Risk Reduction and Mitigation

The Contractor shall ensure that, for each configuration of the PE, the PSS Risk to Life posed by the known impact of normal or unintended behaviour of the PE is addressed by;

a) Implementation and documentation of appropriate risk reduction or mitigation, and;

b) Provision of evidence that PE Safety Requirements are satisfied (Objectives 3 and 4).

Notes:

i. The PSS Risk to Life includes any risks that originate from the normal and unintended behaviour of the PE within its military environment. A changing PE configuration may result in a DSR on the PSS to mitigate the hazard.

ii. The normal behaviour of the PE may include the detection, reconfiguration and reporting of unintended behaviour to a health and monitoring system.

iii. Each new configuration may need to revisit the PE Failure Assessment to address the Risk to Life posed by the unintended behaviour of PE from changes from the previous configuration and be documented and justified in the PESS report.

iv. It is likely that the options for risk reduction may be limited and that evidence satisfaction, including the correct implementation and the absence of errors, may be difficult to obtain. This may be a consideration regarding the choice of OTS PE depending upon what alternative mitigation is provided.

9.3.1 If the Contractor determines there is no impact on the PSS from changes to the PE Configuration Status, then this shall be documented and justified in the PESS report.

9.3.2 The Contractor shall ensure selection or implementation of PE is managed to identify, assess and mitigate the impact of PE unintended behaviour so far as is reasonably practicable and as defined by the design integrity framework of the chosen PE Open Standard, addressing the risks and uncertainty arising from: (Objectives 2, 4 and 5).

a) Not fully implementing the PE Safety Requirements (normal behaviour);

b) Unintended behaviour, and;

c) The lack of evidence supporting a) and b) above.

Notes:

i. During the PE development process, PSS hazardous behaviour can originate from PE unintended behaviour and interaction arising from PE design decisions and systematic errors. This can also occur if OTS PE is chosen to implement or partially implement PE requirements. The safety implications of PE design decisions include coding errors, compilation errors, code-generation errors and modelling errors.

ii. In order to address these risks of PE unintended behaviour due to implementation errors, the Contractor will need to remove, reduce or mitigate the risks by considering suitable techniques to control the introduction of errors and mitigate known errors. These might include trusted or qualified tools, validating the output of untrustworthy or unqualified tools, modelling and coding rules and the use of particular tools, models, libraries and languages that reduce the possibility of making errors.

iii. If OTS PE forms all or part of the solution, then care will be needed to show that the pedigree and Design Integrity of the OTS PE is sufficient, or any shortfalls in integrity can be mitigated.

9.3.3 The Contractor shall ensure that the mitigation implemented or proposed in the event of the unintended behaviour of PE is appropriate to the Design Integrity (Objectives 4 & 5).

Notes:

i. This requirement fulfils the mitigation of hazardous behaviour of PE aspects of Objective 4, in order that the contribution to the overall PSS Risk to Life can be properly assessed and alternative designs or mitigation considered, where necessary. This can be achieved by the Contractor obtaining formal agreement from the MOD that the chosen mitigation is appropriate to the risk. This may be considered within the scope of contract with the MOD. However, as a minimum, the Contractor can discharge this requirement through the organisation responsible for the Design Integrity of the PSS.

ii. The Contractor also needs to ensure that hazardous behaviour of PE arising from PE design decisions are addressed, and techniques for systematic error risk reduction applied. The Contractor may consider the use of requirement reviews, design review walkthroughs, architectural evaluation, and PE HAZOPs. The Contractor will need to consider whether the techniques applied are sufficient (Objective 5).

iii. It is likely that the options for alternative designs may be limited and that evidence assuring the absence of hazardous behaviour of PE may be difficult to obtain. This may be a consideration regarding the choice of OTS PE depending upon what alternative mitigation is provided.

9.3.4 The Contractor shall implement appropriate protection measures that either prevent or provide mitigation for vulnerabilities due to inappropriate intentional and unintentional change to PE.

Note. Whilst appropriate Configuration Management will provide some mitigation for inappropriate or unintentional changes to PE, there are a number of potential vulnerabilities that need to be considered especially with increased use of open systems.

9.3.5 The Contractor shall justify, demonstrate, document and communicate the chosen risk mitigation to those responsible for the overall PSS integrity.

Note. The Contractor will need to provide justification where it is considered that risk mitigation is sufficient, as the design evolves or the use of the PSS changes, which can be documented in the PESS. However, if there is doubt, the MOD can be consulted to agree that the proposed mitigation is sufficient or if additional mitigation measures are required.

9.3.6 The Contractor shall provide justification supported by evidence to demonstrate, within the PESS report, that identified Design Integrity shortfalls have been mitigated.

Note. This Clause ensures that any shortfall in meeting these requirements is sufficiently mitigated, particularly where there may be a shortfall in achieving Design Integrity within the military environment.

10 Assurance

10.1 PE Safety Evidence

The Contractor shall provide PE Safety Evidence to demonstrate the satisfaction of all PE Safety Requirements. (Objective 3).

Notes:

i. This Clause addresses verification and there are a variety of techniques for achieving this. In meeting Objective 3 it is necessary to first demonstrate that Objective 1 and 2 have been met.

ii. PE Safety Evidence is likely to be derived from testing, analysis, review and field experience that supports the PE Safety claims made in the PESS report. It is not the intent of this Standard to describe or outline specific types of analysis or evidence. However, it is likely that the chosen PE Open Standard will have further guidance and detail of these types.

iii. Where the PE includes the use of OTS PE, additional appropriate evidence may be required to justify the suitability of the OTS PE.

10.1.1 The Contractor shall ensure that the evidence is trustworthy.

Notes:

i. Trustworthiness is established through independent assessment of the evidence source such as competency of staff, qualification of tools and accreditation of agencies.

ii. Issues such as evidence related to Intellectual Property Rights (IPR), may be resolved by the use of independent assessment as agreed within the scope of contract.

10.1.2 The Contractor shall ensure that the evidence is appropriate according to the hierarchy of requirements.

Note. Requirements are often arranged in a hierarchy with low level requirements usually containing more detail than high level requirements which may be more generic and less specific in nature. Accordingly, the amount of evidence demonstrating the satisfaction of each requirement can be commensurate to its level within the hierarchy.

10.2 PE Safety Assurance Reporting

The Contractor shall produce a PESS report that summarises;

a) The justification of how the requirements of this Standard have been met and;

b) The supporting evidence that shows compliance with this Standard.

Note. This requirement applies to all Objectives but, recognises that complete assurance is impractical. Therefore, the Contractor is required to agree with the MOD that the scope and extent of the evidence, such as testing, analysis, review, and field experience are sufficient.

10.2.1 The Contractor shall document and report progress against the PESMP, SMP or acceptable alternative plan within the agreed scope of supply.

10.3 Contractor PE Safety Audits

The Contractor shall propose and conduct internal PE Safety Auditing that is consistent with the chosen PE Open Standards.

Note. The proposed means of auditing is to be defined as soon as possible after deciding the choice of standards to be applied.

10.3.1 The Contractor shall obtain formal MOD agreement that the proposed means of internal PE Safety Auditing is appropriate for supporting demonstration of compliance with the PE Safety Requirements.

Note. This agreement would ideally be undertaken early when deciding the choice of standards to be applied. If this Standard has been invoked through Def Stan 00-056, it is possible that this Clause has already been covered by the SMP.

10.3.2 The Contractor shall ensure that PE Safety Audits are carried out and that the Contractor PE Auditors are independent from those areas within the Contractor's organisation, or any Sub-Contractors, that are subject to Safety Audit.

10.4 Independent PE Safety Auditing

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

Notes:

i. If this Standard has been invoked through Def Stan 00-056, it is possible that this Clause has already been covered by the SMP.

ii. The ISA may be required by the MOD to act as its representative in order to ensure that the governance of the SMS and the application of the PE Open Standard are met either through Def Stan 00-056 or an agreed alternative proposed by the Contractor.

iii. This Standard requires the Contractor to undertake Contractor PE safety audit, and to facilitate audit by a MOD-appointed ISA, if one is appointed. In this way, there is assurance of the safety process.

This page intentionally blank

Annex A

Definitions

For the purpose of this Standard, the definitions from Def Stan 00-056 apply together with the following:

Term	Definition
Complex Electronic Hardware	Complex Electronic Hardware includes but not be limited to custom micro-coded components including **Application Specific Integrated Circuits** (ASIC), **Programmable Logic Devices** (PLD), **Field Programmable Gate Arrays** (FPGA), or similar electronic components used in Systems.
Data Safety Requirements	A subset of PE Safety Requirements that addresses inherent safety properties of data.
Open Standards	The definition of Open Standards adopted by this Standard can be found in Open Standards Principles: For software interoperability, data and document formats in government IT specifications. 1 November 2012.
Military Delta	The evidence shortfall or gap between civil and military needs arising from the use of civil standards or OTS solutions.
PE Safety Summary (PESS)	Justification, supported by a body of evidence that when combined with the PSS ISSS or equivalent safety assessment, provides a compelling, comprehensible and valid case in relation to Assurance for a given PE application in a given military operating environment.
Programmable Elements (PE)	PSS that is implemented in software or programmable hardware, which includes any device that can be customised, eg ASICs, PLDs and FPGAs.
PE Safety Management Plan	A document that defines the strategy for addressing PE safety and the safety management of PE integration into PSS.
PE Safety Requirement	A Safety Requirement that is: a) usually allocated from PSS systems engineering and safety assessment activities; b) derived from the choice of standards to meet the PE Design Integrity, or; c) derived as the PE design evolves.
Recognised Good Practice	Recognised good practice is the generic term for those standards or documented processes for controlling risk which have been judged and recognised as satisfying relevant legislation when applied to a particular relevant case in an appropriate manner. **Note.** This definition of Recognised Good Practice is adapted from the UK Health and Safety Executive's (HSE's) website. It has been extended to include documented processes and it is expected that any judgement will be independent and undertaken by suitably qualified personnel.

This page intentionally blank

Annex B

Adoption of a PE Open Standard as an Acceptable Means of Compliance

1 Introduction

1.1 This Annex defines the adoption practices for the selection and use of a PE 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 MOD acceptance of the proposal.

Notes:

i. Where the term PE Open Standard is used this does not preclude the use of a standard whose scope is broader than PE, however this Annex is only applicable to the adoption of the PE aspects of such a standard.

ii. Appendices to this Annex provide guidance on the adoption of a selection of PE Open Standards in common use. Inclusion should not be taken to imply a preference for use of that PE Open Standard, nor should exclusion be taken to imply that any standard is unsuitable or unacceptable for adoption.

1.2 A proposed PE Open Standard has to be compared against this Standard's objectives and derived Clauses. This Annex augments the requirements detailed in Clause 8 of this Standard.

2 Adoption Context

2.1 When adopting a PE Open Standard, the context of its application must be considered. This Annex addresses context where the PE is Developmental or un-modified Off-the-Shelf (OTS). Developmental context includes 'green field' and adaptive modification of an OTS PE. Un-modified OTS PE includes use in the context for which the PE was designed, and use in an alternative context without modification.

2.2 This Annex makes no differentiation between procurement scenarios where the MOD procures the PE directly from the Contractor, or where the MOD procures PSS that includes one or more PE(s). In the former case, the MOD may be the provider of the PE requirements, and PE integrator, whereas in the latter case the Contractor is the owner of both the PSS and PE processes.

2.3 The scope of contract may cover multiple PE. The considerations of this Standard must be applied to each of these, though this may be by considering them collectively if a uniform adoption of standards is applicable. Where context of adoption varies for different PE, justifications must be provided for each class of adoption, with particular attention paid to risks introduced by any proposed use of different PE Open Standards across different PEs. In all cases this must be with reference to the higher level PSS safety integrity needs.

3 PE in context of PSS lifecycle

3.1 The Contractor must consider the relationship to the PSS lifecycle. Issues for consideration include:

a) Compatibility of requirements setting;

b) Compatibility of integrity management scheme;

c) Coverage of technical and management interfaces;

d) Integration of PE into PSS.

3.1.1 In considering the compatibility of requirement setting, the Contractor must address the relationship between the proposed PE Open Standard and the PSS level standard used to set the PE Safety Requirements. Factors to consider include:

a) Responsibilities: Do the proposed PSS and PE Open Standards assume compatible responsibilities for identification and validation of requirements? Might there be gaps or overlap that could lead to conflict? Is it clear who does what? Is it clear which standard governs each lifecycle phase? eg development, integration and assurance.

b) Coverage: Does the PSS standard provide requirements on all aspects that the PE standard needs to be enacted? eg function, behaviour, use of resources, technical interfaces, and, integrity including counterfeit and Cyber security.

c) Terminology: Do the PSS and PE standards: talk the same language? Are definitions consistent? Do they require and use process artefacts in a sympathetic manner? ie What management plans are produced? Do they satisfy the needs of the higher level process?

d) OTS PE: do the requirements to which the PE was developed satisfy the requirements demanded in the intended PSS context? Where there are shortfalls or additional capability? What are the risks that may arise?

4 Objectives

4.1 The Contractor must consider how the application of their proposed PE Open Standard addresses each of the objectives set out in this Standard. This must include consideration of the lower level requirements that expand on the objectives.

4.2 Should the proposed PE Open Standard fail to fully address the objectives set out in this Standard, the Contractor should propose supplements that will address the shortfall and express these as DSRs.

4.3 The Contractor is encouraged to make maximum use of the artefacts produced by the proposed PE Open Standard to address the deliverables requirements set out in this Standard. Where this Standard requires content that the proposed PE Open Standard does not naturally produce, the Contractor is encouraged to incorporate it within an alternative higher level document or a supplement, eg justifications for selection of a PE Open Standard could be included in a PSS SMP, Safety Case Report (SCR) or ISSS.

Notes:

i. It is important to consider this in terms of the product of the PE process.

ii. Where the PE is based on OTS PE there may be limited opportunities to supplement the PE process. Care must be taken to ensure that supplemental measures add value in terms of understanding the performance of the PE and its safety contribution to the PSS risk.

iii. Where the PE is based on OTS PE, particularly where it is used without modification, it is important to understand any differences in requirements and interfaces. OTS PE compliant with an Open Standard may:

a) Still present a significant contribution to a safety risk;

b) Fail to mitigate a risk if demands are placed on it;

c) Be used differently from that for which it was designed;

d) Have emergent behaviour that is not anticipated by other system components.

iv. Where the proposed Open Standard does not explicitly address the Data Safety Requirement, then Annex E must be considered and where justifiable, a supplementary Open Standard adopted.

5 Governance

5.1 It is important to consider whether the governance arrangements for the proposed use of a PE Open Standard match those for which the standard was originally intended.

Note. The assessment philosophy for PE Open Standards can vary and is dependent on how the standard defines and measures compliance. When adopting a PE Open Standard the assessment and compliance philosophy must be considered.

5.2 The Standard requires an agreed approach for governance which may vary between MOD regulatory domains. The approach must be based on the proposed PE Open Standard and the requirements of the MOD regulations. The governance must be agreed and formalised in the scope of contract.

6 Applicability and Status

6.1 It is important to consider the applicability of the proposed PE Open Standard to the domain, and its status within the domain. The Contractor must provide a justification for the relevance of the Standard to its domain of use, and demonstrate that it represents current RGP.

6.1.1 If a superseded or obsolete standard, or a standard that is not native to the domain (eg automotive standard for avionics application) is proposed it is likely to require more significant justification.

6.1.2 It may be necessary to supplement the PE Open Standard with additional process or governance to cover shortfalls recognised through application of the standard, eg where the governing body has issued supplemental guidance, or where the standard is being applied outside of its native domain.

Note. Def Stan 05-138 may require maintenance of the Cyber Security Essential Plus Certification which in turn requires additional external assessment (governance) under the Cyber Security Essentials scheme.

7 Derived Safety Requirements and Strategies for Managing Shortfalls

7.1 Annex C identifies a number of high level strategies to deal with potential shortfalls. These should be considered in the context of the proposed PE Open Standard. Where selected, the supplements to the PE Open Standard that address shortfalls should be expressed as DSRs.

Note. In a systems engineering context, the most effective solution may involve imposing DSRs on other elements of the system, rather than simply relying on changes in the PE process.

This page intentionally blank

Appendix 1 to Annex B

Adoption of RTCA DO-178

1 Introduction

1.1 This Appendix addresses the potential adoption of the DO-178 family of PE Open Standards. DO-178 is recognised as a software development standard used within the civil air domain. Whilst DO-178's title implies it is guidance, it is given more authority through endorsement by FAA and EASA as recognised means of compliance with regulatory requirements applicable to design of civil aircraft and their systems. The MAA recognise DO-178 as an acceptable means of compliance for airborne software in Def Stan 00-970.

1.2 This Appendix primarily considers RTCA DO-178C/EUROCAE ED-12C, referred to as DO-178C in this Appendix. For legacy and OTS PE, the Appendix also identifies additional consideration for the earlier version RTCA DO-178B/EUROCAE ED-12B, referred to as DO-178B in this Appendix. Where considerations of both DO-178B/DO-178C are identified then the DO-178 reference is used in this Appendix.

2 Adoption Context

2.1 For Developmental 'green field' PE, where DO-178 is proposed, DO-178C should be used, together with relevant supplementary publications. Choice of DO-178B would require further justification identifying clear benefits for the use of DO-178B, and any perceived risks and their mitigation.

Note. Relevant supplementary publications in this context refer to the supplementary guidance to the publication, eg Certification Authorities Software Team position papers and technology supplements such as DO-333.

2.2 For adaptive modification of OTS PE previously developed with DO-178B, consideration must be given to the adoption of DO-178C, weighing benefits and risks against continued use of the version to which the PE was originally developed. Where DO-178B is proposed, consideration must be given to supplementing its use with relevant good practice identified in the current version and relevant supplementary publications.

2.3 For un-modified OTS PE, the DO-178 version used in original development will be applicable by default. It may however still be useful to consider DO-178C if gaps are identified in the consideration against the Objectives of this Standard. This may identify credible supplemental assurance activities, or support a justification that in respect of a particular concern the standard as applied still measures favourably against current RGP.

3 PE in Context of PSS Lifecycle

3.1 DO-178C is designed to be used within a development framework against regulation and Certification Specifications/Technical Standard Orders that are relevant for the class of aircraft/equipment in which they are installed. PSS development is expected to be in accordance with ARP 4754A and with safety assessment performed in accordance with ARP 4761.

3.2 Where the PSS is utilising the above standards, it can be assumed that there is a good match between PE and PSS standards context and Objective 1 of this Standard will be achieved. The use of DO-178 in an alternative PSS standards context would require assessment and justification at the PSS level, prior to the selection of DO-178. In this case the assessment will need to fully consider all the Objectives of this Standard.

4 Objectives

4.1 The appropriate application (see note) of DO-178C is deemed to address the objectives and clauses within the main body of this Standard, with the following limitations:

a) DO-178C does not ensure the validity of requirements, and this needs to be assured in conjunction with the system safety process.

b) Objective 4 is not fully satisfied: DO-178C requires that derived requirements are provided to systems processes including system safety analysis. This may be deemed sufficient for lower Software Levels, however further assessment of the credible PE unintended behaviour is required at higher Software Levels.

c) DO-178C allows tailoring by Software Level. Whilst this is acceptable practice, it is essential that Software Levels are allocated correctly.

Note. Appropriate application implies satisfaction of all relevant objectives with the appropriate control category, in the context of a relevant systems engineering process and governed within a suitable regulatory framework.

4.2 For OTS PE, the shortfalls identified above also apply along with the additional considerations guidance for previously developed software detailed in DO-178.

Note. OTS PE in this Standard includes the term 'previously developed software' used in DO-178.

4.3 The above statements for DO-178C apply equally to DO-178B, however it should be recognised that the later version embodies updates based on experience of applying the earlier version. In line with regulatory advice, consideration should always be given to applying DO-178C where practical.

Notes:

i. DO-178C identifies the allocation of requirements related to performance (Mission), Cyber security and, safety data (Parameter Data Items).

ii. For PE which has critical Mission (performance), Cyber security or Data Safety Requirements, DO-178B proposals are likely to present significant shortfalls (Military Delta) which will need to be managed.

5 Governance

5.1 DO-178 is designed to be applied in a regulated framework. Whilst DO-178 is flexible and entitled as guidance, the regulatory framework ensures that its application is appropriately applied to meet defined objectives. This is achieved through involvement of the Regulator or their agent in key lifecycle stage reviews against the objectives of DO-178, these reviews include planning, development, verification and final. The governance approach enables tailoring of the application of DO-178 to be agreed including the use of alternative methods/approaches that are at least as effective; or supplementary obligations where particular risks or circumstances suggest that the methods recommended in DO-178 may not be sufficient.

5.2 The MOD will appoint, with the agreement of the Contractor, an agent to perform the regulatory oversight/governance to ensure that an equivalent of the civil governance is applied. This will form part of the agreed scope of contract.

5.3 Such regulatory oversight/governance may have been applied during the development of an OTS PE proposed for use in a military context, or may be planned for a developmental PE for use in a civil regulated development of a dual-use PSS. In these cases the MOD appointed governance agent may limit the review of evidence to the Military Delta. The governance agent may also determine that it is necessary to review documentation provided to the Regulator or their agent and the review reports demonstrating satisfaction of the DO-178 objectives.

5.4 In some military projects, civil regulatory involvement may be precluded. In these cases the Contractor may propose governance arrangements to achieve the equivalent governance effects, and ensure appropriate application of DO-178.

6 Applicability and Status

6.1 DO-178 is maintained through current use in a regulated framework, with a wide community of use and supplemental guidance is added to cover novel application and lessons used through practice. DO-178 can be seen as applying RGP within the aerospace domain, when used in an appropriate system development and regulatory framework. Use outside of such a framework may be appropriate/acceptable but requires careful consideration and justification.

7 Derived Safety Requirements and Strategies for Managing Shortfalls

7.1 Annex C identifies a number of high level strategies to deal with potential shortfalls. The following describes potential tactics to address those strategies when applying DO-178:

a) Raising the design integrity: Applying the DO-178C criteria for a higher Software Level, eg Level-A when Level-B may be acceptable in the civil use, may provide sufficient assurance against a shortfall introduced by a Military Delta;

b) Raising the level of design rigour, eg applying the Formal Methods Supplement to DO-178C, DO-333, may help to provide additional assurance where Level-A is not sufficient in a military context. This may apply where Military Delta constraints may preclude fault tolerant architectures, for reasons of space, weight or performance.

Notes:

i. These examples may not be independent; further they should be viewed as illustrative, not an exhaustive list.

ii. In a systems engineering context, the most effective solution for the Military Delta may involve imposing DSRs on other elements of the system.

8 Deliverables

8.1 DO-178 requires a number of artefacts to be produced and in some cases for these to be agreed by the certification authority. These artefacts can be used to address compliance against the deliverable requirements of this Standard with the following limitations:

a) The Plan for Software Aspects of Certification (PSAC) may be used to partially address the requirements for a PE Safety Management Plan, however specific aspects of the interface to the MOD/PSS process may need to be captured elsewhere (eg within a higher level management plan).

b) The Software Accomplishment Summary may be used to partially comply with the requirements for a PESS report, however specific aspects of the safety interfaces to the PSS may need to be included within a supplementary or higher level ISSS.

8.2 DO-178 requires the delivery of a minimum set of life cycle data to the certification authority. It is expected that this minimum set will be delivered as part of the project deliverables, and that reasonable access for MOD and its agreed agents will be provided for all other life cycle data artefacts. The scope of and access to life cycle data artefacts should be addressed by the relevant management plan.

This page intentionally blank

Appendix 2 to Annex B

Adoption of IEC 61508

1 Introduction

1.1 This Appendix addresses the potential adoption of IEC 61508. IEC 61508 is an international standard for Electrical/Electronic/Programmable Electronic Safety-Related Systems, which therefore includes PE within its scope. IEC 61508 is intended to be used pan-domain. It is the basis of many domain specific standards, eg ISO 26262 in automotive. Contractors may propose standards derived from IEC 61508 with the agreement of MOD using the adoption guidance in this Annex.

1.2 IEC 61508 covers a range of issues, but the focus of this Appendix is on IEC 61508 Part 3 that deals with software, a special case of PE. Part 3 cannot be used stand-alone but discussion of the other parts of the standard is limited to those issues that have a direct bearing on Part 3. Part 3 draws on Part 1 (General Requirements) and Part 2 (Requirements for Electrical/ Electronic/Programmable Electronic Safety-Related Systems). Part 2 provides a limited treatment of Application Specific Integrated Circuits (ASICs) including an ASIC lifecycle.

Notes:

i. IEC 61508 uses the abbreviation PE to mean Programmable Electronics rather than Programmable Elements, and treats software separately. Where PE is used in this Appendix it is used as defined in this Standard.

ii. Whilst IEC 61508 also addresses programmable hardware such as ASICs and FPGAs, these are treated differently to software. Therefore, whilst adoption of IEC 61508 for programmable hardware may be suitable as a means of compliance with this Standard, it is outside of the scope of this Appendix.

2 Adoption Context

2.1 For new development PE, 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.

2.2 For adaptive modification of OTS PE, consideration must be given to adoption of the latest version, weighing benefits and risks against continued use of the version to which the PE was originally developed. Where an earlier version is proposed, consideration must be given to supplementing its use with relevant good practice identified in the current version and relevant supplementary publications.

2.3 For un-modified OTS PE, the version used in original development will be applicable by default. It may however still be useful to consider later versions if gaps are identified in the considerations against the objectives of this Standard. This may identify credible supplemental assurance activities. For example, the concept of a ‘compliant item safety manual’ introduced in the second edition in IEC 61508 is similar to an ISSS (although limited to software) so may assist in meeting the requirements of this Standard.

3 PE in Context of PSS Lifecycle

3.1 IEC 61508 Part 3 is intended to be used within a development and safety assessment framework defined in the other Parts of IEC 61508, especially Parts 1 and 2. It is also invoked from other standards, eg IEC 61511 which is applicable in the process industry. IEC 61511 has requirements for software, but invokes IEC 61508 Part 3 for the more complex software elements; thus the main body of IEC 61511 provides a context for the use of IEC 61508 Part 3, in that sector.

3.2 Where the PSS is utilising IEC 61508 as a whole, or other domain-specific standards that effectively incorporate IEC 61508 (eg IEC 61511), it can be assumed that there is a good match between the PE and PSS standards context. The use of IEC 61508 in an alternative PSS standard context, eg MIL-STD-882, would require assessment and justification as the principles for determining software safety integrity requirements are fundamentally different.

4 Objectives

4.1 The appropriate application (see notes) of IEC 61508 Part 3 is deemed to address the objectives and clauses within the main body of this Standard, with the following limitations:

a) IEC 61508 Part 3 does not address Objective 1 and this needs to be assured in conjunction with the system safety process; however this would be done if working to all parts of IEC 61508.

b) Objective 3 is not fully satisfied. It is not always apparent how meeting the requirements of a particular SIL actually demonstrates satisfaction of the DSRs. Improved traceability between the safety process and the DSRs is required.

c) IEC 61508 Part 3 tailoring by SIL permits less rigorous approaches to meeting the objectives, at lower levels, and this may weaken the confidence in meeting the objectives. Whilst this is acceptable practice, it is essential that SILs are allocated correctly.

Notes:

i. Appropriate application implies satisfaction of all relevant requirements associated with the appropriate Safety Integrity Level (SIL), in the context of a relevant systems engineering process and governed within a suitable regulatory framework.

ii Objective 4 is addressed by the Normative requirements for hazard analysis of software in IEC 61508 Part 3 Table A10. Care is required that the requirements of this aspect of IEC 61508 have been applied correctly. Alternatively, directly addressing PE Failure Assessment Requirements of this Standard may be used to cover any shortfall in compliance.

4.2 The above statements apply equally to all versions of IEC 61508; however it should be recognised that the later version embodies updates based on experience, eg introducing safety manuals and addressing data-driven systems.

Note. PE will have Mission (performance), Cyber security or Data Safety Requirements, IEC 61508 proposals are likely to present shortfalls (Military Delta) which will need to be managed.

4.3 Where OTS PE is used in modified or unmodified form, IEC 61508 identifies a number of different routes to compliance, including the use of safety manuals and a proven in use argument. However, it should be noted that neither of these approaches resolves the shortfall identified against Objective 4.

5 Governance

5.1 IEC 61508 is intended to be applied in a framework involving independent assessment, however, no broader governance structure is assumed. The governance approach defined by IEC 61508 enables tailoring of the application of IEC 61508 to be agreed with the independent assessor, including the use of alternative methods/approaches that are at least as effective as those recommended in the IEC 61508. The tailoring of IEC 61508 allows for highly recommended techniques not to be used (with justification) so there can be considerable flexibility in the use of IEC 61508 assessed as part of PE Failure Assessment.

Note. Both the text in the body of IEC 61508 and the text in its Annexes are designated either as normative or as informative. This is achieved through the sub-clause headings, the use of the mandatory shall and optional should phraseology and, in the case of informative recommendations, by the use of Notes. For compliance mandatory clauses must be satisfied. Similar to other standards, trusted agents may be appointed to assess the extent to which a product is compliant.

5.2 Where there is no civil regulatory framework, the MOD will appoint, with the agreement of the Contractor, an ISA to ensure that an equivalent level of scrutiny is applied, eg to assess tailoring. This will form part of the agreed scope of contract and scope of analysis in a Def Stan 00-056 project.

5.3 Independent assessment may have been employed during the development of an OTS PE proposed for use in a military context. In this case the MOD appointed ISA may limit the review of use of the IEC 61508 and evidence to the Military Delta.

6 Applicability and Status

6.1 IEC 61508 is maintained through periodic update, through the mechanisms provided by the IEC, including review and approval by National standards bodies, such as the BSI in the UK. There is a wide community of use; indeed a very wide community if one considers the use of derivative standards in particular domains. IEC 61508 can be seen as applying generic RGP in a way that is domain independent. However, as a consequence, care should be taken to ensure that the use is appropriate to the defence application and attention should be given to justifying its use if there are domain specific standards, eg ISO 26262, applicable given the domain.

7 Derived Safety Requirements and Strategies for Managing Shortfalls

7.1 Annex C identifies a number of high-level strategies to deal with potential shortfalls. The following describes potential tactics to address those strategies when applying IEC 61508 Part 3:

a) Raising the design integrity: Applying the IEC 61508 Part 3 criteria for a higher SIL, eg SIL 4 when SIL 3 may be acceptable for civil use may provide sufficient assurance against a shortfall introduced by a Military Delta;

b) Raising the level of design rigour, eg changing between the alternative means of complying with a SIL requirement, using more rigorous, eg formal, techniques than had initially been proposed where other protective measures, eg the use of diversity, are not practicable given other constraints.

Notes:

i. These examples may not be independent; further they should be viewed as illustrative, not an exhaustive list.

ii. In a systems engineering context, the most effective solution for the Military Delta may involve imposing DSRs on other elements of the system which is explicitly addressed in IEC 61508 as a whole, particularly Part 1.

8 Deliverables

8.1 IEC 61508 does not specify particular document production or delivery, however in addressing the requirements of the standard it is likely that document artefacts that at least partially address the deliverable requirements of this Standard will be produced. Such documentation should be used where possible to avoid nugatory work; however they may require supplementing with additional documents to address specific aspects of the interface to the MOD/PSS process.

8.2 The scope of and access to life cycle data artefacts should be addressed by the relevant management plan.

This page intentionally blank

Appendix 3 to Annex B

Adoption of RTCA DO-254

1 Introduction

1.1 This Appendix addresses the adoption of RTCA DO-254/EUROCAE ED-80 (DO-254). DO-254 is recognised as a hardware development assurance standard used within the civil air domain. Whilst DO-254's title implies it is guidance, it is given more authority through endorsement by FAA and EASA as recognised means of compliance with regulatory requirements applicable to design of civil aircraft and their systems. The MAA recognise DO-254 as an acceptable means of compliance for airborne hardware in Defence Standard 00-970.

1.2 This Appendix considers the latest version at time of issue of this Standard, DO-254.

1.3 The scope of DO-254 is electronic hardware, with the majority of its requirements focused on Complex Electronic Hardware (CEH). CEH covers both PE and Non-PE hardware. PE includes custom micro-coded components such as Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs). The main body of this Defence Standard addresses design integrity of functional aspects of PE and does not include requirements that address those issues that are specific to design or manufacture of non-programmable hardware.

2 Adoption Context

2.1 For Developmental 'green field' PE, where DO-254 is proposed, the latest version should be used, together with relevant supplementary publications.

Note. Relevant supplementary publications in this context refer to the supplementary guidance to the publication, eg Certification Authorities Software Team position papers and EASA Certification Memorandum.

3 PE in Context of PSS Lifecycle

3.1 DO-254 is designed to be used within a development framework against regulation and Certification Specifications/Technical Standard Orders that are relevant for the class of aircraft/equipment in which they are installed. PSS development is expected to be in accordance with ARP 4754A and with safety assessment performed in accordance with ARP 4761.

3.2 Where the PSS is utilising the above standards, it can be assumed that there is a good match between PE and PSS standards context. The use of DO-254 in an alternative PSS standards context would require assessment and justification.

4 Objectives

4.1 The appropriate application of DO-254 is deemed to address the objectives and clauses within the main body of this Standard, with the following limitations:

a) DO-254 does not ensure the validity of requirements and this needs to be assured in conjunction with the system safety process.

b) Objective 4 is not fully satisfied. DO-254 requires that derived requirements are provided to systems processes including system safety analysis. This may be deemed sufficient for lower design assurance levels, however further assessment of the credible PE unintended behaviour is required at higher design assurance levels.

c) DO-254 tailoring by assurance level. Whilst this is acceptable practice, it is essential that assurance levels are allocated correctly.

d) The broader scope of DO-254 means that some objectives may not be relevant to all PE. Any tailoring to exclude objectives should be carefully assessed to ensure that relevant objectives are not erroneously excluded.

Note. Appropriate application implies satisfaction of all relevant objectives with the appropriate control category, in the context of a relevant systems engineering process and governed within a suitable regulatory framework.

4.2 For OTS PE, the shortfalls identified above also apply along with the additional considerations guidance for previously developed hardware detailed in DO-254.

Notes:

i. OTS PE in this Standard includes the term previously developed hardware terminology used in DO-254.

ii. PE will have critical Mission (performance), Cyber security or Data Safety Requirements, DO-254 proposals are likely to present shortfalls (Military Delta) which will need to be managed.

5 Governance

5.1 DO-254 is designed to be applied in a regulated framework. Whilst DO-254 is flexible and entitled as guidance, the regulatory framework ensures that its application is appropriately applied to meet defined objectives. This is achieved through involvement of the Regulator or their agent in key lifecycle stage reviews against the objectives of DO-254, these reviews include planning, development, verification and final. The governance approach enables tailoring of the application of DO-254 to be agreed including the use of alternative methods/approaches that are at least as effective; or supplementary obligations where particular risks or circumstances suggest that the methods recommended in DO-254 may not be sufficient.

5.2 The MOD will appoint, with the agreement of the Contractor, an agent to perform the regulatory oversight/governance to ensure that an equivalent of the civil governance is applied. This will form part of the agreed scope of contract.

5.3 Such regulatory oversight/governance may have been applied during the development of an OTS PE proposed for use in a military context, or may be planned for a developmental PE for use in a civil regulated development of a dual-use PSS. In these cases the MOD appointed governance agent may limit the review of evidence to the Military Delta. The governance agent may also determine that it is necessary to review documentation provided to the Regulator or their agent and the review reports demonstrating satisfaction of the DO-254 objectives.

5.4 In some military projects, civil regulatory involvement may be precluded. In these cases the Contractor may propose governance arrangements to achieve the equivalent governance effects, and ensure appropriate application of DO-254.

6 Applicability and Status

6.1 DO-254 is maintained through current use in a regulated framework. Supplemental guidance is added to cover novel application and lessons used through practice. There is a wide community of use. DO-254 can be seen as applying RGP within the aerospace domain, when used in an appropriate system development and regulatory framework. Use outside of such a framework may be appropriate/acceptable but requires careful consideration and justification.

7 Derived Safety Requirements and Strategies for Managing Shortfalls

7.1 Annex C identifies a number of high level strategies to deal with potential shortfalls. The following describes potential tactics to address those strategies when applying DO-254:

a) Raising the design integrity: Appling the DO-254 criteria for a higher design assurance level (eg level A when level B may be acceptable in the civil use) may provide sufficient assurance against a shortfall introduce by a Military Delta;

b) Raising the level of design rigour, eg applying the advanced verification methods contained in Appendix B of DO-254 such as Formal Methods, may help to provide additional assurance where level A is not sufficient in a military context. This may apply where Military Delta constraints may preclude fault tolerant architectures, for reasons of space, weight or performance.

Notes:

i. These examples may not be independent; further they should be viewed as illustrative, not an exhaustive list.

ii. In a systems engineering context, the most effective solution for the Military Delta may involve imposing DSRs on other elements of the system.

8 Deliverables

8.1 DO-254 required a number of artefacts to be produced and in some cases for these to be agreed by the certification authority. These artefacts can be used to address compliance against the deliverable requirements of this Standard with the following limitations:

a) The Plan for Hardware Aspects of Certification (PHAC) may be used to partially address the requirements for a PE Safety Management Plan, however specific aspects of the interface to the MOD/PSS process may need to be captured elsewhere (eg within a higher level management plan).

b) The Hardware Accomplishment Summary may be used to partially comply with the requirements for a PESS report, however specific aspects of the safety interfaces to the PSS may need to be included within a supplementary or higher level ISSS.

8.2 DO-254 required the delivery of a minimum set of life cycle data to the certification authority. It is expected that this minimum set will be delivered as part of the project deliverables, and that reasonable access for MOD and its agreed agents will be provided for all other life cycle data artefacts. The scope of and access to life cycle data artefacts should be addressed by the relevant management plan.

This page intentionally blank

Annex C

Addressing the Unique Military Risk Requirement

1. Introduction

1.1 This Annex addresses the impact of differences between civil and military needs arising from the use of civil PE Open Standards or civil OTS solutions. Many of these issues may arise at the system level, but as the resolution may be in terms of PE, the issues need to be dealt with in the context of this Standard.

Note. There will be differences between MOD requirements associated with the unique military risk and civil requirements met by civil PE Open Standards. Civil PE Open Standards are not intended for the development of weapons systems or for the use of PE in military specific contexts.

1.2 The term Military Delta refers to any distinction between civil and military needs or solutions whether they relate to product, process or governance including issues related to the use of civil standards or PE Open Standards. The term includes any difference between UK and overseas military standards.

Note. An OTS solution may have been developed to a foreign military PE Open Standard. In such cases the foreign military PE Open Standard may be treated as if it was a civil PE Open Standard. In such cases, there is likely to still be a delta between MOD military safety needs and those arising from the foreign military PE Open Standard.

1.3 This Annex is intended to address the Military Delta in general terms. The Adoption Annex, Annex B to this Standard, deals with selection and use of standards. Its Appendices address the specifics of the differences between the requirements of this Standard and relevant civil standards, eg DO-178B/C. The aims of this Annex are:

a) To identify governance, product and process considerations which apply when addressing the Military Delta in any domain, and with any standards;

b) To provide the context for the Adoption Annex, and its treatment of specific standards.

Note. MOD has its own regulatory agencies and it will be necessary to bridge between MOD governance needs and the existing mechanisms used by PE Open Standards.

1.4 Applying any Open Standard is not sufficient in itself to ensure or assure that it is effective, eg produce safe PE. A governance framework contributes substantially to the effectiveness of any standard; for military PE applying a relevant governance framework provides the necessary means of assuring that military requirements are met.

Note. Military safety requirements have additional dependencies on the Contractor for the management of the risk of counterfeit material in the supply chain (Def Stan 05-135), and the Cyber security risk (Def Stan 05-138). The governance framework of the proposed PE Open Standard may need to be adapted to help manage these risks.

2 Governance

2.1 When using a civil PE Open Standard in support of a development under Def Stan 00-056 and this Standard, the Contractor must:

a) Identify the roles and responsibilities for safety management and governance defined in the civil standard or standards, or those which are either defined or accepted as good practice, in the normal context of use;

b) Identify the roles and responsibilities for safety management and governance defined by Def Stan 00-056 and this Standard, or in the PESMP, setting out the interpretation of the standards for the project;

c) Assess the differences and propose resolutions, updating the PESMP as appropriate;

d) Record the rationale for the decisions in the PESMP, or in documents referenced from the PESMP;

e) Agree with the MOD an agent to perform regulatory oversight.

Notes:

i. The MOD ISA or appointed agent may provide regulatory oversight. The scope of analysis of the agent will be with the agreement of the Contractor and formalised in the scope of contract.

ii. Wherever possible, the use of the existing civil mechanisms and processes for governance will be adapted for the appropriate MOD regulations.

3 Product and Process Technical Issues

3.1 For OTS PE and modified OTS PE, the Contractor must consider differences in military and civil usage.

Notes:

i. For OTS PE (whether acquired stand alone or as part of a PSS), the change from civil to military use may mean that the PE is not acceptable in the military usage context even though it was in the civil context. If it is new PE, then there should be no product delta, as the PE should be developed to meet the relevant requirements including DSRs.

ii. If the PE is to be used in a known PSS it will be possible to consider the contribution of the PE to hazards and risks; otherwise the focus will be on the unintended behaviour of the PE.

iii. The Contractor may need to define new DSRs to address the differences. These differences may lead to emergent causes or new PE unintended behaviours.

3.2 For OTS PE and modified OTS PE, the Contractor must consider differences in military and civil processes used in managing and developing the OTS PE.

Notes:

i. Process issues relate directly to the satisfaction of the five objectives and clauses, in this Standard. This may lead to shortfalls in process due to the PE Open Standard not meeting the objectives or the specific application of the PE Open Standard on the project has not met the objectives.

ii. A potential shortfall is the process deliverables provided by the PE Open Standard and what is required by this Standard.

3.3 The Contractor should identify necessary DSRs through application of PE Failure Assessment.

Notes:

i. PE Failure Assessment is the main mechanism for identifying the PE specific DSRs and they can be used to address the Military Delta.

ii. There may be cases where use of multiple OTS PE solutions requires the consideration of multiple and different PE Open Standards this in turn may generate additional DSRs related to compatibility.

4 Managing the Military Delta

4.1 To manage PE Military Deltas, particularly for OTS PE, the Contractor must provide sufficient argument supported by evidence to the MOD to inform and enable their ALARP decisions.

Notes:

i. With OTS PE, visibility of the evidence (safety-related information) needed to collate a PESS may be challenging. The Safety Committee will need to make judgments about the risk associated with this uncertainty – usually as an information shortfall. This is likely to be a situation where levering off civil governance evidence and/or employing an ISA is particularly valuable.

ii. Where there are shortfalls or other limitations the construction of arguments may assist the acceptance by the Safety Committee. So far as possible, to aid the decision-making processes, the impact of these limitations should be expressed in terms of operational risk.

4.2 When managing PE related shortfalls and Military Deltas, Contractors should use the principles and requirements defined in the design for safety clauses of the Safety Engineering Section of Def Stan 00-056.

Note. This approach should be applied to all forms of shortfall, eg, a governance shortfall that means that there was no oversight of hazard analysis needs to be addressed. The same applies to product issues, eg a Military Delta related DSR and the civil requirement that the PE satisfies.

4.3 Safety-related trade-off decisions related to shortfalls and DSRs should involve the relevant Safety Committee and the system integrator.

Note. Managing the Military Delta may require dealing with disparate standards, incomplete knowledge and difficult judgments trading-off performance or mission effectiveness against safety. For these reasons it is important that the key decisions regarding the Military Delta be taken in the Safety Committee and involving the system integrator. In particular, the committee should take any decision (or make recommendations) which involves accepting higher risk than would be countenanced under the relevant civil standards.

5 Derived Safety Requirements and Strategies for Managing Shortfalls

5.1 Contractors may propose the following mitigation strategies as a means of meeting shortfalls identified and documented as DSRs:

a) Raising the design integrity, eg increasing integrity or assurance level within the chosen PE Open Standard;

b) Raising the level of design rigour, eg using formal methods to develop key parts of the software or demonstrate a key PE property;

c) Raising the level of assurance, eg by carrying out testing to more demanding coverage criteria, or undertaking static code analysis;

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

e) Reducing dependence on the component, eg by introducing redundancy or diversity (within the PE).

Notes:

i. As indicated above, additional DSRs may be produced to deal with shortfalls in either product or process, which arise due to the Military Delta. Specific DSRs can only be agreed within a system context but mitigation strategies may emerge at the PE level.

ii. Depending on the PE Open Standard chosen these strategies may not be independent; further they should be viewed as illustrative, not an exhaustive list. In a systems engineering context, the most effective solution may involve imposing DSRs on other elements of the system.

This page intentionally blank

Annex D

Data Item Descriptions (DIDs)

1 This Defence Standards Data Item Descriptions (DIDs) are intended to assist Contractors in determining the scope of supply of the project documentation; they have a similar purpose to DIDs in MIL-STD-882 but should not be considered as directly equivalent.

2 The format, content and frequency of deliverable DIDs will be agreed with the MOD and form part of the scope of supply. Domain specific regulations may expand or reduce the intent of the DIDs, eg a PE Safety Management Plan may be replaced by a Safety Management Plan, or authorised alternative. The DIDs contain 'shall' and 'should' statements and these are intended to identify the mandatory and optional scope and content of deliverables. Where possible, Contractors should use civil, open and other standards as a basis of meeting the intent of the DIDs. The PE SMP, SMP or authorised alternative, will define what are the relevant deliverables and agreed DID tailoring.

3 DIDs are at the Appendices as follows:

a) Appendix 1 DID - PE Safety Summary Report

b) Appendix 2 DID - PE Safety Management Plan

This page intentionally blank

Appendix 1 to Annex D

DID - PE Safety Summary Report

1 Introduction

1.1 This DID sets out requirements for a PE Safety Summary report (PESS) in support of this Standard; it is intended to identify the scope and content of the PESS.

1.2 A PESS is similar to an ISSS and either becomes an ISSS for the PSS Safety Case/Safety Assessment Report or supports another PSS ISSS. The PESS draws on the content of the information set to provide a justification of the safety performance of the PE, within bounds that are reasonable, given the scope of contract and other factors set out below.

1.3 The purpose of a PESS is to provide a subset of the information set identifying all the safety properties of the PE. It is a summary report of the information set and it should be succinct, accessible, proportionate and easy to understand. The PESS provides a necessary summary of the technical safety design of the PE and summarises how the objectives have been met.

1.3.1 The PESS supports the conduct of PE Failure Assessment when the PE is intended to be used standalone, as well as when integrated into a (larger) system, or a system or service integrated into a System of Systems, eg for the Air Domain in the Air System Safety Case.

1.3.2 The PESS may also supplement PE Failure Assessment Report which is expected to be focused on a specific in-service use of the PE.

1.3.3 The PESS is constrained by the scope of analysis; a Contractor‘s analysis is constrained to the limits of their visibility of the intended in-service operation of their PE, and features that are inherent in their chosen design approach.

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

2 Scope of Applicability

A PESS is required where the Contract includes the supply of PE that is to be installed, or integrated, into a larger PSS as well as where the PE is intended to be used standalone. The agreed scope of supply should be documented in the PESMP.

3 Application/Interrelationship

This DID contains the content and instructions for preparing an PESS as specified within the PESMP and in conjunction with the relevant PSS Safety Case/Safety Assessment Report, PSS Information Safety Set Summary and Command Summary (or in the Defence Air Environment, the Release to Service document).

4 Preparation Instructions

4.1 The PESS should contain information based on the topics identified in this Section’s sub-headings.

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

4.3 The PESS is a mandatory deliverable, unless its exclusion is explicitly stated within the scope of supply. Preliminary versions of the PESS may be required as the maturity of the PE develops. The timing and scope of preliminary versions should be agreed with the customer and defined within the PESMP.

4.4 Scope

The PESS should include a statement of scope that defines the boundary of the PE covered, taking into account the scope of contract, and the scope of analysis.

4.5 Functional Description

The PESS should include a description of the functionality and/or capability provided by the PE.

4.6 Context of In-Service Use

4.6.1 The PESS should summarise the intended in-service use.

4.6.2 The PESS should also summarise capabilities that are accessible but not intended to be used in-service. This should include capability that is inherent, eg functionality included but not used in COTS PE.

4.7 Unusual Aspects of the PE's Design

The PESS should summarise any aspects of the PE that could be considered unusual, particularly those that are not covered by a PSS Safety Case/Safety Assessment Report.

4.8 Assumptions, Dependencies and Limitations

4.8.1 The PESS should summarise all the assumptions, dependencies and limitations identified in the information set.

4.8.2 This should include assumptions and dependencies related to valid configurations of the PE which are not currently used in-service.

4.9 PE Unintended Behaviour

4.9.1 It is essential that all normal and credible unintended behaviours of the PE are identified, through a formal failure mode identification and analysis process; however it is understood that a Contractor will not be able to determine whether those behaviours are hazardous in all cases.

4.9.2 The Contractor should document all credible unintended behaviours as clearly as possible, enabling the determination of those that are potentially hazardous based on the intended usage of the PE.

4.9.3 The PESS should summarise all the PE normal and unintended behaviours identified in the information set. This should include those where it has been possible for the Contractor to identify them as potentially hazardous but which have sentenced as low risk and are not identified or recorded in the PSS Safety Case/Safety Assessment Report; for example, PE unintended behaviours associated with a capability of the PE that is not currently used in-service.

4.10 Safety Justification

4.10.1 The PESS should summarise safety performance of PE. It should not be as extensive as the safety justification and analysis of the PSS Safety Case/Safety Assessment Report but include elements that may not be in the PSS Safety Case/Safety Assessment Report. This should include all the inherent/intrinsic risks that are part of the PE design but mitigated. These mitigations may be current limitation of use, valid assumptions in the environment and dependencies always available in the current PE in-service use.

4.10.2 The PESS 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 PSS Safety Case/Safety Assessment Report. The PESS should highlight any potential safety issues and how they are controlled.

4.10.3 The PESS should provide evidence of PE Safety Requirements traceability to all the PE safety implementation evidence.

4.10.4 The PESS may provide an essential part of the body of evidence in a PSS Safety Case.

5 Control Requirements

5.1 The PESS should be created, held and managed under an appropriate configuration management system, which should be specified in the PESMP.

5.2 The PESS should be approved by a suitable authorised representative of the Contractor, in accordance with the roles and responsibilities defined in the PESMP and endorsed by the Safety Committee.

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

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

This page intentionally blank

Appendix 2 to Annex D

DID - PE Safety Management Plan

1 Introduction

1.1 This Data Item Description (DID) provides guidance on the Programmable Elements Safety Management Plan (PESMP), and should be viewed as a checklist, rather than as a contents list. This DID is intended to identify the scope and content of the PESMP.

1.2 The PESMP should be updated at a frequency defined in the Contract, but it would be unusual if the PESMP were not updated at least once per annum, and on major project events, eg a Preliminary or Critical Design Review.

1.3 In general, it is likely that the PESMP would be produced by drawing on standard company practices, eg Safety Management Systems, and on the project-specific information defined in the Contract Statement of Work. The PESMP should address the core principles of PE safety engineering and safety management.

2 Scope of Applicability

2.1 The PESMP should identify the agreed scope of contract for the PE and any related PSS(s), including the scope of analysis and supply.

2.2 It should identify both primary and ancillary PE, eg test systems as well as the main deliverables, where they are safety-related. It should identify critical dependencies on externally supplied items, eg Government Furnished Equipment or Assets.

2.3 The PESMP should identify and cover the lifecycle of the PE within the scope of analysis.

3 Application/Interrelationship

3.1 This DID contains the content and instructions for preparing the PESMP; this 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 PESMP should draw on the Contractors Safety Management Systems for PE engineering and management.

4 PESMP Preparation Instructions

4.1 The PESMP shall contain information based on the topics identified in Sections 5 and 6.

4.2 Coverage of these topics is mandatory; however, tailoring may be acceptable subject to robust justification for the changes and agreement with the MOD. The level of detail in the PESMP should be defined at the ITT and agreed prior to Contract award.

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

4.4 The level of detail under each topic will depend on the scale of the project. For simple projects the PESMP may contain detail for all of the topics. For complex projects, the PESMP is likely to contain detail for key elements of these topics, and to refer out to other documents as appropriate. The topics may be viewed as a checklist for the supporting documentation, not just for the PESMP itself.

5 Safety Management

5.1 PE Description

The PESMP should include a clear and concise description of the functionality required from the PE.

5.2 Applicable Legislation and Regulations

The PESMP should identify the legislation, regulations, standards and MOD policies that apply to the PE, taking into account all theatres in which the PE 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 PE.

5.3 Safety Strategy

The PESMP should identify a safety strategy that is appropriate for the scope of supply of the PE, consistent with the Project Management Plan and MOD Policy. The strategy should provide an overarching framework that will enable the PE to meet the Safety Requirements placed on it by the MOD such that it is fit for purpose for its intended usage. The strategy should include information on the derivation of the PE safety criteria.

5.4 Organisation and Responsibilities

The PESMP should identify the key safety roles in the project organisation covering both individuals and committees. It should identify responsibility, authority and accountability for safety 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 PESMP should document the Terms of Reference for the key roles. The PESMP should record how competency of staff in key safety roles is assessed and how it is managed. The PESMP should identify roles outside the Contractor's organisation, eg key suppliers, and MOD stakeholders, eg Regulators. The PESMP should also state the Terms of Reference for the PE Safety Committee as well identifying those stakeholders who will make up the committee.

5.5 Programme Plan and Milestones

The PESMP should identify and provide a schedule for major PE safety activities and milestones. The schedule should be updated periodically reflecting progress and revisions necessary to meet the overall PE Safety Requirements.

5.6 Interfaces

The PESMP 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. Where relevant, the PESMP should also identify technical interfaces to existing or planned PSS within the scope of contract.

5.7 Information Management

The PESMP 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. The PESMP should identify mechanisms for preserving the information set through Contract life.

5.8 Reporting

The PESMP 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, including at the PSS level if relevant. The PESMP should identify the ISSS and any Safety Assessment Reports to be produced, including preliminary reports and/or incremental delivery of the reports. It should identify which of the activities in the safety schedule produce these reports. The PESMP 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 review by the relevant PE Safety Committee). The PESMP 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 PE, PSS(s), regulators, or other official bodies, eg the HSE.

5.9 Safety Auditing

The PESMP should identify Contractor Safety Audit Plans and reporting, including processes, terms of reference for audits, audit frequency, and audit of any Sub-Contractors. This may refer to a dedicated Contractor Safety Audit Plan. However, the PESMP should identify how both Contractor Safety Audit and Independent Safety Audit findings 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.

5.10 Change Management

The PESMP should identify mechanisms and procedures for change, at the engineering level, and dealing with issues such as change in personnel responsibilities, organisation, deployment of PE, etc. These mechanisms and procedures should address updates in the field, and the maintenance of clear records of configuration status, even for PE in geographically dispersed PSS.

5.11 Deliverables

The PESMP 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. The PESMP should identify the review and acceptance process and timeframes for all deliverables.

5.12 Quality Assurance

The PESMP should identify those aspects of Quality Assurance that are specific to safety.

5.13 Supplier/Sub-Contractor Management

Where a Contractor intends to include PE from suppliers or Sub-Contractors, then the mechanisms to be put in place to ensure that safety is assured should be described in the PESMP.

5.14 Incident Reporting and Management

The PESMP should document the procedures and processes to be used for the reporting of incidents and their management thereof.

5.15 Lifecycle

The PESMP should identify and define and (where necessary) justify the methods to be used for the development of PE, particularly in response to integrity requirements, and identify which tasks in the PESMP should use these methods. This should address the PE lifecycle as bounded by the scope of contract. Where appropriate the PESMP should refer to relevant PE Open Standards for definition of good practice.

5.16 Assumptions, Dependencies and Limitations

The PESMP should document any assumptions, dependencies and limitations being made by the Contractor with regard to safety and the usage of the PE to be developed.

5.17 Support Tools and Approval

The PESMP should identify any support tools to be used during the development of the PE, such as development tools, compilers, automatic code/gatemap generators, simulators, etc. This should include the rationale for their use, as well as how such tools are to be approved for use on the safety programme.

5.18 Previously Developed PE

Where the Contractor intends to include previously developed PE, of any kind, in the delivered PSS then this should be clearly stated, together with the means being used by the Contractor to ensure that sufficient evidence of safety and fitness for purpose of such PE items will be included in the Information Set.

5.19 Competence

The PESMP should describe any specific safety and PE-related competencies that are required by Contractor staff during the safety programme.

6 Development

6.1 The PESMP should include some high level description of the all the development processes to be followed. For simple tasks a high level description may be all that is needed. For more complex development tasks, it is expected that detailed descriptions will be included in a separate Development Plan, Plan for Software Aspects of Certification or similar.

6.2 In all cases a rationale should be provided explaining how the approach chosen will contribute to the overall safety of the PE and any associated PSS in which it is intended to be used.

6.3 A clear description of the interfaces to other PE and/or PSS should be included.

6.4 Requirements Analysis

The PESMP should describe how PE Safety Requirements are to be identified, analysed and managed.

6.5 Design

The PESMP should describe how the design elements will be developed and documented, including how any support tools will be approved and used.

6.6 Implementation

The PESMP should describe how the implementation will be developed. This should include reference to relevant and appropriate coding standards, compliers, linkers, automatic code generators, etc.

6.7 Integration

The PESMP should describe how any PE components will be integrated together as a standalone item or as part of a PSS.

6.8 Modification

The PESMP should describe the processes to be used to ensure that any modifications do not undermine safety or any safety arguments that have been made.

6.9 Verification and Validation

6.9.1 The PESMP should describe how verification and validation of the PE will be undertaken throughout the lifecycle.

6.9.2 The PESMP should clearly identify any other PE and/or PSS that will be required to support those verification and validation activities.

7 Abbreviations and Definitions

7.1 The PESMP should list all abbreviations used together with any definitions of terms which are unique to the PESMP or which have differing definitions from those contained within applicable standards, plans, etc.

8 References

8.1 The PESMP should list all documents that are referenced within.

9 Control Requirements

9.1 The PESMP should be created, held and managed under an appropriate configuration management system.

9.2 The PESMP shall be approved by a suitable authorised representative of the Contractor, in accordance with the roles and responsibilities defined in the PESMP and agreed by the MOD and the Safety Committee.

9.3 The PESMP may address information for more than one PE and/or more than one version/modification state of a PE, provided that the association of the information specific to the PE version under Contract is clear.

9.4 Throughout the life of the Contract, the PESMP shall be reviewed and updated to changes in circumstances or plans. The review should be carried out regularly and all changes agreed with the MOD and the Safety Committee.

This page intentionally blank

Annex E

Data Safety

1 The Role and Importance of Data

1.1 PE is PSS that is implemented in software or programmable hardware, which includes data. Therefore Data Safety Requirements are a subset of the PE Safety Requirements.

1.2 Modern PE can make significant use of data. It is often used in ways where the level of safety is an inherent property of the data, rather than being an attribute of a controlling system function. In such situations it is important to consider how the loss of required data properties can affect PE and subsequently Risk to Life.

1.3 The types of activity used to assure the Design Integrity of PE can also be applied to data. What changes is the perspective; the properties that the data is required to exhibit should be identified and the safety argument should demonstrate how these will be achieved and maintained.

1.4 Data often forms an important part of PE that supports human decisions. In these cases PE may behave as intended, but if the associated data does not exhibit the required properties then an inappropriate decision may be made. In such situations the data can be considered as having led to the unintended behaviour of the PE.

1.5 Contractors generating or using data for PSS must address the Data Safety Requirements.

2 Data Safety Requirements

2.1 The demonstration of the data properties related to safety will be through the derivation of Data Safety Requirements that provide assurance that data-related risks in PE have been appropriately considered.

2.2 The Contractor must ensure that the derived Data Safety Requirements demonstrate that the generation and use of data has achieved the PE Safety Objectives. In particular, in achieving Objective 2 the Contractor must maintain the intent of the Data Safety Requirements throughout requirements decomposition.

Note. When considering Data Safety Requirements the Contractor must evaluate the impact of inappropriate intentional and unintentional change of data on Cyber security or Mission performance.

3 Open Standards

The Contractor must ensure that the adopted PE Open Standard achieves the PE Safety Objectives for generation and use of data through the derivation Data Safety Requirements.

Notes:

i. The main body of this Standard advocates the use of PE Open Standards. Contractors need to consider that these standards tend to retain their original focus, eg the processing instructions of the software rather than the data that the instruction act upon.

ii. Some domain Open Standards address Data Safety Requirements when applied within their domain regulatory constraints. The UK Safety Critical System Club Data Safety Initiative Working Group has provided generic Data Safety Guidance, compatible with the Def Stan 00-056 principles, which identifies:

a) Different data types (verification, infrastructure, performance, dynamic and justification) that may have a bearing on system safety;

b) Data properties that may need to be established and maintained;

c) Processes and methods that can be used to identify and analyse risks;

d) Processes and methods and approaches that can be used to evaluate and treat risks and manage data safety requirements.

iii. In the context of this Standard, the Data Safety Requirements would normally be captured as part of either the SMP or where implemented the PESMP, whichever is most applicable.

Inside Rear Cover

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

DStan Helpdesk

Tel: +44 (0) 141 224 2531/2

Fax: +44 (0) 141 224 2503

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

File Reference

The DStan file reference relating to work on this standard is D/DStan/21/55/1.

Contract Requirements

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

Revision of Defence Standards

Defence Standards are revised as necessary by an up-issue or amendment. It is important that users of Defence Standards ensure that they are in possession of the latest issue or amendment. Information on all Defence Standards can be found on the DStan Websites https://www.dstan.mod.uk and http://dstan.uwh.diif.r.mil.uk/, updated weekly. Any person who, when making use of a Defence Standard, encounters an inaccuracy or ambiguity is encouraged to notify UK Defence Standardization (DStan) without delay in order that the matter may be investigated and appropriate action taken. Sponsors and authors shall refer to Def Stan 00-00 before proceeding with any standards work.