Defence
Safety Authority

DSA 03.OME Part 1: Defence Code of Practice (DCOP) 109

Software and Programmable Hardware

Version Record

Version 1.0

Version Date: May 2024.

Version changes: document created.

Copyright

Uncontrolled Copies

All hard copies of this document are to be regarded as uncontrolled copies. To check the latest amendment status, reference should be made to current documents which may be viewed on Gov.uk or on the Defence Intranet.

Preface

Requests for Change

1. Proposed changes, recommendations, or amendments to DOSR Regulations and Guidance can be submitted to the DOSR Regulations and Publications Team:

Email Address: dsa-dosr-prg@mod.gov.uk

Postal Address: Juniper #5004, Level 1, Wing 4, Abbey Wood North, Bristol, BS34 8QW

2. Any post and grammar change proposals can be approved or rejected by the DOSR without involvement of the associated Working Group.

3. Technical change proposals should be submitted to the associated Working Group for review and approval or rejection.

4. When incorporating changes, care is to be taken to maintain coherence across regulations.

5. Changes effecting Risk to Life will be published immediately. Other changes will be incorporated as part of routine reviews.

Review Process

6. The DOSR team will ensure OME Regulations remain fit for purpose by conducting regular reviews through the DOSR Governance Committees, consulting with MOD Stakeholders and other Defence Regulators as necessary on interfaces and where there may be overlaps of responsibility.

Further Advice and Feedback

7. For further information about any aspect of this document, or questions not answered within the subsequent sections, or to provide feedback on the content, contact the DOSR Regulations and Publications Team.

Contents

DSA 02.OME Regulation 109

Software and Programmable Hardware

1. The Accountable Person shall ensure that OME software and programmable hardware is developed to a level of rigour which is commensurate to its contribution to the hazard and is managed to be ALARP and Tolerable.

DSA 03.OME DCOP 109

Introduction

2. Software and programmable hardware are captured under the collective term “Programmable Elements” (PE). PE is defined within Defence Standard (Def Stan) 00-055 - Requirements for Safety of Programmable Elements (PE) in Defence Systems, as *“A product, service or system that is implemented in software or programmable hardware, which includes any device that can be customised (e.g., Application Specific Integrated Circuits (ASICs), Programmable Logic Devices (PLDs) and Field Programmable Gate Arrays (FPGAs).”* PE relates to the program or code which is implemented on the programmable hardware device. It should be noted that the term currently is only used within the UK MOD and that other nations, companies, and external personnel will be unaware of it. PE can also be known as or be contained in the following:

a. Software – For ease of writing, JSP 935 - Software Acquisition Management for Defence Equipment, uses the term “software” instead of PE.

b. Firmware – The program code embedded within programmable hardware.

c. Complex Electronic Elements – Previously used by Def Stan 00-056 - Safety Management Requirements for Defence Systems - Requirements and Guidance.

d. Complex Electronic Hardware – This is used in aviation guidance information (similar to Programmable Hardware).

e. Programmable Electronics – This is used in IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), as part of the term E/E/PE meaning Electrical and/or Electronic and/or Programmable Electronic.

f. Simple Electronic Hardware – This is used by DO254 - Design Assurance Guidance for Airborne Electronic Hardware, to refer to a PE which can be tested to a level so that design assurance activities are not required.

3. Over the past four-decades, PE has become increasingly prevalent within all types of systems. Previous functions that would have been implemented in hardware devices have been replaced with PE functions. OME systems are becoming increasingly reliant on PE, as it provides the ability for a system to reduce mass, size, and power consumption, whilst allowing the incorporation of complex functionality, including safety functions.

Safety Concerns of OME PE

4. PE is susceptible to failure, because the program code may contain coding errors (also known as “bugs”). Unlike hardware, bugs are activated systemically, as opposed to randomly (e.g., PE does not “wear out” in the manner a mechanical switch may wear out). Failures of PE are caused by a particular set of conditions being met, which may not have been accounted for. Therefore, PE will always fail in the same way if these conditions are met. This leads to the activation of bugs and can result in unforeseen consequences.

5. Bugs tend to be introduced early in the development process, this can be from a variety of causes including but not limited to poor requirements capture, and the implementation of design into code. No matter how well requirements are captured and implemented, there could be bugs introduced, which won’t be revealed unless the required specific input parameters or system configurations are met.

6. It is often falsely assumed that testing alone is the solution for identifying and resolving bugs. Testing is only able to demonstrate that bugs are present in relation to a set of specific inputs or system configurations (test configuration), not that they do or do not exist. Unanticipated combinations of inputs, parameters, or system configurations could still lead to a failure condition as most programs are too complex to be 100% tested.

7. This is problematic in the OME safety context, as the MoD has a legal obligation to capture system hazards and mitigate against them.

PE Hazard Mitigation

8. PE has the potential to exhibit unpredictable behaviour. Where this may impact safety, action is needed to reduce the unpredictable behaviour. The only viable method of mitigating hazards within OME produced by bugs in the PE is to implement a rigorous development process which covers both managerial and technical aspects. This will minimise the likelihood of bugs being implemented within the program code. Mitigations should result in increased safety and can improve the reliability of the PE.

9. The level of rigour required in the PE development process is proportional to the hazard severity should the PE device fail (the greater the consequence of the hazard, the more process activities are required, i.e., a higher level of rigour is required). Most PE standards sub-divide the process activities into different levels of rigour / design integrities. These establish the amount of trust which can be placed on PE, depending on the level of rigour that is followed. This enforces correct and unambiguous requirements development and ensures that the code implementation accurately reflects against the requirements.

10. An integrity process is not preassigned to PE functions. The integrity process required for a PE function is determined through a hazard analysis. A system level hazard analysis should be an essential starting point for all projects. This should identify the PE functions that are related to safety. The integrity process can then be identified, based on the consequence of the PE failure.

Def Stan 00-055 Part 1 Issue 5 Objectives and Requirements

Objectives

11. To demonstrate that the PE Integrity principles defined in the Def Stan 00-056 Part 2 Annex D: Integrity and Open Standards, have been fulfilled, the Contractor shall ensure that the following PE Safety Objectives from Def Stan 00-055 Part 1 Issue 5 are achieved:

a. Objective 1: PE Safety Requirements shall be defined to manage the PE contribution to Products, Services, and Systems (PSS) hazards.

b. Objective 2: The intent of PE Safety Requirements shall be preserved throughout requirements decomposition.

c. Objective 3: PE Safety Requirement satisfaction shall be demonstrated.

d. Objective 4: Hazardous behaviour of the PE, including generation and use of data, shall be identified, and mitigated.

e. Objective 5: The confidence established in addressing the (other) PE Safety Objectives shall be commensurate to the contribution of the PE to PSS risk.

f. Objective 6: The safety-related consequences of adaptive PE behaviour shall be addressed.

Requirements

12. There are requirements listed in Def Stan 00-055 Part 1 Issue 5 that fall both prior to contract let and post contract let. These requirements feed from the safety objectives listed above and should be complied with. The Design Organisation (DO) should propose their intended compliance with the requirements which should be agreed with the Accountable Person (AP). Evidence is required to demonstrate compliance against the requirements. For information, the two most overlooked requirements prior to contract let for PE are as follows:

a. Agreement of a PE Open Standard,

b. Agreement of the extent and depth of the PE safety evidence.

Agreement of a PE Open Standard

13. The DO should propose and agree with the AP the use of an appropriate PE open standard. This open standard is required to define the PE development process and activities, so that the PE can be developed to a level of trustworthiness. Currently this method is used as there is no military specific development standard for PE and allows the DO to use a PE open standard which they are familiar with, on the provision the DO can maintain the objectives and requirements of Def Stan 00-055 Part 1 Issue 5 .

14. The DO should propose how their chosen open standard will fulfil the objectives and requirements of Def Stan 00-055 Part 1 Issue 5, ensuring resolution of any deltas. This should be agreed with the AP. This proposal should be assessed through an ITE against the adoption practices of Annex A from Def Stan 00-055 Part 1 Issue

5 , guidance should be provided to the AP, and used as part of the safety argument for accepting the proposal from the DO via the AP's safety governance system.

15. Annexes B to D of Def Stan 00-055 Part 1 Issue 5 contain three previously adopted standards and the instructions for their adoption. These standards are listed below in order of preference according to JSP 920, MOD Standardization Management Policy:

a. IEC 61508 2010 (Annex C of Def Stan 00-055 Part 1 Issue 5)

b. DO-178B & DO-178C used in conjunction with ARP4754 (Annex B of Def Stan 00-055 Part 1 Issue 5)

c. DO-254 used in conjunction with ARP4754 (Annex D of Def Stan 00-055 Part 1 Issue 5)

16. If the adoption instructions for the previously adopted standards are followed by the DO to enable the use of the open standard, an ITE against Annex A is not required as it has been previously conducted by the Def Stan 00-055 committee and can be accepted by the AP.

Agreement of the extent and depth of the PE safety evidence

17. The DO should propose the extent and depth of the PE safety evidence. This should be agreed with the AP. Failure to do so leads to systems not being able to demonstrate compliance to the regulation, and any evidence delivered to the AP is likely to either be poor or missing.

18. The following types of PE safety evidence are needed to support the successful outcome of an ITE which investigates the compliance of the PE contained within a system against the regulation:

a. Programmable Elements Safety Management Plan (PESMP) – This is a requirement of Def Stan 00-055 Part 1 Issue 5 and should contain the content as described throughout the main body and Annex H of Def Stan 00-055 Part 1 Issue 5 . The PESMP should identify the following:

(1) The agreed scope of contract for the PE and any related PSS, including the scope of analysis and supply.

(2) Both primary and ancillary PE, e.g., the test systems and the main deliverables where they are safety related.

(3) The critical dependencies on externally supplied items, e.g., Government Furnished Equipment or Assets.

(4) The lifecycle of the PE within the scope of analysis.

b. PE Safety Summary (PESS) – This is a requirement of Def Stan 00-055 Part 1 Issue 5 and should contain content as described throughout the main body and Annex G of Def Stan 00-055 Part 1 Issue 5. This is a high-level document which identifies the PE within the system and states what standards were followed to develop the PE, explaining the PE architecture. This document should be a summary for all the Claims, Arguments & Evidence (CAE) and

contain detail or references to supporting documentation. It should include the evidence of how the requirements of Def Stan 00-055 Part 1 Issue 5 and the PE open standard have been followed and achieved. This should feed into the OME Safety and Environmental case(s) (SEC). Documents can be supplied which fulfil the same role and often have one of the following titles:

(1) Software/Firmware Safety Case

(2) Software/Firmware Safety Analysis Report

c. Functional Hazard Analysis Report – This report documents the Functional Hazard Analysis and contains an evaluation of the potential causes and hazardous consequences of a system's functional failures. PE safety uses this analysis to assess the software contribution to the system hazards and identify safety related PE. The analysis should feed into the OME Hazard Log, within the OME SEC.

d. Integrity assignment report – This explains and justifies the choice of the selected design integrity and may be a requirement of some open standards, and should feed into the OME SEC.

e. All additional documentation required by the open standard being followed and access to any of the lower level supporting evidence referenced. i.e., if an artifact is referenced as evidence, then it should be available for inspection.

19. It should be noted that the title given to the artifacts varies between nations, companies, and standards. The evidence should be contracted and scoped based on the description of the items rather than their titles.

20. Post contract let, the DO should be generating and refining the CAE in line with the precontractual agreement. It is recommended that prior to deliverable acceptance, the CAE are reviewed against the precontractual agreement. The evidence can also be reviewed independently throughout the development process to guide the content and quality of the evidence.

Independent Technical Evaluation of Programmable Elements

21. PE within a system should be evaluated for compliance against Def Stan 00-055 Part 1 Issue 5 and the agreed open standard. This evaluation must be conducted by a body independent of the DO with expertise in PE safety. The outcomes of a PE safety ITE should verify the CAE for the PE and its level of achievement in meeting the regulation. ITE should highlight shortfalls found in the CAE and recommend further action where required.

22. The PE safety ITE should consider the following:

a. That the PE within a system that contributes to a hazard and the hazard severity has been identified.

b. That the level of rigour assigned to the PE is commensurate to the PE’s contribution to the hazard.

c. That the CAE is sufficient to demonstrate that the PE is compliant to Def Stan 00-055 Part 1 Issue 5 and the open standard.