

ECSS Secretariat

ESA-ESTEC

Requirements & Standards Section

Noordwijk, The Netherlands

This document is distributed to the ECSS Community for Public Review.

(Duration 8 weeks)

Start of Public Review: 23 August 2022

**End of Public Review: 18 October 2022**

*NOTE: This document is a complete re-write of ECSS-Q-ST-60-02C and therefore no revision tracking was done. This document has been drafted together with the new engineering document ECSS-E-ST-20-40C “ASIC, FPGA and IP Core engineering”.*

**DISCLAIMER** (for drafts)

This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

**Foreword**

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the /ECSS-E-ST-20-40 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

**Disclaimer**

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Section

ESTEC, P.O. Box 299,

2200 AG Noordwijk

The Netherlands

Copyright: 2022 © by the European Space Agency for the members of ECSS

Change log

|  |  |
| --- | --- |
| Previous steps |  |
| ECSS-Q-60-02A  17 July 2008 | First issue |
| ECSS-Q-60-02B | Never issued |
| ECSS-Q-ST-60-02C Rev. 1  30 March 2022 | Second issue  Changes to ECSS-Q-60-02A are:   1. All documents requirements have been moved in normative annexes. The following DRDs have been created: ACP, ADP, DVRMPRS, FRA, VP, DVP, ES, Data Sheet and Detail Specification 2. Some editorial conversions have been done for compliance to ECSS-Drafting rules for Standard. |
| ECSS-Q-ST-60-02C Rev.1 DFR1  8 July 2022 | Draft submitted to TAAR for Parallel Assessment  ================ =======================  Complete re-work:   1. Issue C Rev.1 includes product assurance activities only 2. General engineering is moved to ECSS-E-ST-20-40 3. Annex E provides traceability between issue C and issue Rev.1 |
| Current step |  |
| **ECSS-Q-ST-60-02C Rev.1 DIR1**  **8 July 2022** | **Draft released for Public Review.**  **23 August – 18 October 2022**  Complete re-work of previous version:   1. Issue C Rev.1 includes product assurance activities only 2. General engineering is moved to ECSS-E-ST-20-40 3. Annex E provides traceability between issue C and issue Rev.1 |
| **Next steps** |  |
| DIR + impl. DRRs | Draft with implemented DRRs |
| DIR + impl. DRRs | DRR Feedback |
| DIA | TA Vote for publication |
| DIA | Preparation of document for publication (including DOORS transfer for Standards) |
|  | Publication |

Table of contents

[Change log 3](#_Toc112081985)

[1 Scope 7](#_Toc112081986)

[2 Normative references 8](#_Toc112081987)

[3 Terms, definitions and abbreviated terms 9](#_Toc112081988)

[3.1 Terms from other standards 9](#_Toc112081989)

[3.2 Terms specific to the present standard 10](#_Toc112081990)

[3.3 Abbreviated terms 10](#_Toc112081991)

[3.4 Conventions 12](#_Toc112081992)

[3.4.1 Names of DEVICE development phases and reviews 12](#_Toc112081993)

[3.5 Nomenclature 12](#_Toc112081994)

[4 ASIC, FPGA and IP Core product assurance principles 13](#_Toc112081995)

[4.1 Overview 13](#_Toc112081996)

[4.2 Organization of this Standard 13](#_Toc112081997)

[4.3 Tailoring 14](#_Toc112081998)

[5 Product Assurance programme implementation 15](#_Toc112081999)

[5.1 Organization and responsibility 15](#_Toc112082000)

[5.1.1 Organization 15](#_Toc112082001)

[5.1.2 Responsibility and authority 15](#_Toc112082002)

[5.1.3 DEVICE product assurance responsible 15](#_Toc112082003)

[5.2 DEVICE product assurance programme management 16](#_Toc112082004)

[5.2.1 DEVICE product assurance planning and control 16](#_Toc112082005)

[5.2.2 DEVICE product assurance reporting 16](#_Toc112082006)

[5.2.3 Audits 17](#_Toc112082007)

[5.2.4 Alerts 17](#_Toc112082008)

[5.2.5 DEVICE problems reporting 17](#_Toc112082009)

[5.2.6 Non-conformances 17](#_Toc112082010)

[5.3 Risk management and critical item control 18](#_Toc112082011)

[5.3.1 Risk management 18](#_Toc112082012)

[5.3.2 Critical item control 18](#_Toc112082013)

[5.4 Supplier selection and control 18](#_Toc112082014)

[5.4.1 Supplier selection 18](#_Toc112082015)

[5.4.2 Supplier requirements 18](#_Toc112082016)

[5.4.3 Supplier monitoring 19](#_Toc112082017)

[5.4.4 Criticality classification 19](#_Toc112082018)

[5.5 Tools and supporting environment 19](#_Toc112082019)

[5.5.1 Methods and tools 19](#_Toc112082020)

[5.5.2 Development environment selection 20](#_Toc112082021)

[6 DEVICE Process Assurance 21](#_Toc112082022)

[6.1 DEVICE development lifecycle 21](#_Toc112082023)

[6.1.1 DEVICE life cycle 21](#_Toc112082024)

[6.2 Requirements applicable to all DEVICE engineering processes and phases 21](#_Toc112082025)

[6.2.1 DEVICE dependability and safety 21](#_Toc112082026)

[6.2.2 Handling of critical DEVICES 23](#_Toc112082027)

[6.2.3 Reuse of existing DEVICES 24](#_Toc112082028)

[6.2.4 Automatic code generation 26](#_Toc112082029)

[6.2.5 Project Security Assurance 26](#_Toc112082030)

[6.2.6 Configuration management 27](#_Toc112082031)

[6.2.7 Verification Control Document 27](#_Toc112082032)

[6.3 Requirements applicable to individual DEVICE engineering processes and activities 27](#_Toc112082033)

[6.3.1 DEVICE Definition Phase 27](#_Toc112082034)

[6.3.2 DEVICE Design and Verification Phase 28](#_Toc112082035)

[6.3.3 DEVICE Design Validation, Acceptance and Maintenance phase 28](#_Toc112082036)

[6.4 Process Assessment and improvement 32](#_Toc112082037)

[6.4.1 Process assessment control 32](#_Toc112082038)

[6.4.2 Process assessment reporting 32](#_Toc112082039)

[6.4.3 Process improvement 32](#_Toc112082040)

[7 DEVICE product quality assurance 33](#_Toc112082041)

[7.1 Product quality objectives and metrication 33](#_Toc112082042)

[7.1.1 Assurance activities for product quality requirements 33](#_Toc112082043)

[7.1.2 Product Metrics definition and reporting 33](#_Toc112082044)

[7.1.3 Basic metrics 33](#_Toc112082045)

[7.1.4 Reporting of metrics 34](#_Toc112082046)

[7.2 IP Core or DEVICES intended for Reuse 34](#_Toc112082047)

[7.2.1 Overview 34](#_Toc112082048)

[7.2.2 Self-contained information 34](#_Toc112082049)

[7.2.3 Requirements for intended reuse 34](#_Toc112082050)

[7.2.4 Configuration management for intended reuse 34](#_Toc112082051)

[7.2.5 Testing on different EEE component 34](#_Toc112082052)

[7.2.6 Certificate of conformance 35](#_Toc112082053)

[8 DEVICE Configuration Management 36](#_Toc112082054)

[8.1 DEVICE Configuration Management planning and control 36](#_Toc112082055)

[8.1.1 Configuration Management Plan 36](#_Toc112082056)

[8.1.2 Software tools 36](#_Toc112082057)

[8.2 Configuration Management implementation 36](#_Toc112082058)

[8.2.1 DEVICE Configuration management implementation 36](#_Toc112082059)

[8.2.2 CIDL and ABCL 36](#_Toc112082060)

[8.2.3 Software configuration management implementation 38](#_Toc112082061)

[8.3 Configuration Control 38](#_Toc112082062)

[9 Tailoring by DEVICE criticality 39](#_Toc112082063)

[9.1 Device criticality categories 39](#_Toc112082064)

[9.2 Applicability Matrix 41](#_Toc112082065)

[Annex A (normative) DEVICE Product Assurance Plan (DPAP) - DRD 66](#_Toc112082066)

[Annex B (normative) DEVICE Product Assurance Report (DPAR) - DRD 71](#_Toc112082067)

[Annex C (normative) DEVICE Reuse File (DRF) - DRD 74](#_Toc112082068)

[Annex D (informative) DEVICE Development Expected Outputs 76](#_Toc112082069)

[Annex E (informative) Traceability from ECSS-Q-ST-60-02C to ECSS-Q-ST-60-02C Rev1 82](#_Toc112082070)

[Bibliography 134](#_Toc112082071)

**Figures**

**No table of figures entries found.**

**Tables**

[Table D-1 : ECSS-Q-ST-60-02 list of Expected Outputs 76](#_Toc112082072)

[Table E-1 : ECSS-Q-ST-60-02C to ECSS-Q-ST-60-02C Rev.1 82](#_Toc112082073)

[Table E-2 : Matrix from ECSS-Q-ST-60-02C Rev.1 to ECSS-Q-ST-02C 112](#_Toc112082074)

# Scope

This Standard defines a set of product assurance requirements for the development and maintenance of integrated circuits such as ASICs, and FPGAs, and for IP Cores as reusable building blocks of complex integrated circuits, in space systems. In the context of this standard, the special word DEVICE is used to refer to either an ASIC, and FPGA or an IP Core. Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities.

This Standard also applies to the development or reuse of DEVICES which affects the quality of the deliverable product or service provided by a space system, if the service is implemented by these DEVICES.

ECSS-Q-ST-60-02 interfaces with space product assurance, engineering and management standardisation documents, which are addressed in the Product Assurance (Q), Engineering (E) and Management (M) branches of the ECSS System, and explains how they relate to the DEVICE product assurance processes and phases.

ECSS-Q-ST-60-02 was written in a co-engineering manner with ECSS-E-ST-20-40, and it follows the phases defined in ECSS-E-ST-20-40. As the phases defined in ECSS-E-ST-20-40 do not follow the naming convention of processes defined in ECSS-M-ST-10, ECSS-Q-ST-60-02 provides a bridge between the ECSS-E-ST-20-40 phases and ECSS-M-ST-10 phases and processes, especially between ECSS-E-ST-20-40 DEVICE Validation, Acceptance and Maintenance Phase Review (VAMPR) and ECSS-M-ST-10 Qualification Review and Acceptance Review. Therefore assessment and approval of the qualification status of a DEVICE is defined in ECSS-Q-ST-60-02, while ECSS-E-ST-20-40 focuses on the engineering steps to be followed for a successful IC or IP Core development under customer approval for both engineering and PA.

This standard may be tailored for the specific characteristic and constraints of a space project in conformance with ECSS-S-ST-00.

Tailoring of this Standard to a specific business agreement or project, when ASIC/FPGA/IP Core product assurance requirements are prepared, is also addressed in clause 4.3.

# Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references the latest edition of the publication referred to applies.

|  |  |
| --- | --- |
| ECSS-S-ST-00-01 | ECSS system – Glossary of terms |
| ECSS-E-ST-10-02 | Space engineering – Verification |
| ECSS-E-ST-20-40 | Space engineering – ASIC, FPGA and IP Core engineering |
| ECSS-Q-ST-10 | Space product assurance – Product assurance management |
| ECSS-Q-ST-20 | Space product assurance – Quality assurance |
| ECSS-Q-ST-30 | Space product assurance – Dependability |
| ECSS-Q-ST-40 | Space product assurance – Safety |
| ECSS-E-ST-10 | Space engineering – System engineering general requirements |
| ECSS-M-ST-10 | Space project management – Project planning and implementation |
| ECSS-M-ST-10-01 | Space project management – Organization and conduct of reviews |
| ECSS-M-ST-40 | Space project management – Configuration and information management |
| ECSS-M-ST-80 | Space project management – Risk Management |

# Terms, definitions and abbreviated terms

## Terms from other standards

1. For the purpose of this Standard, the terms and definitions from ECSS‑ST‑00‑01 apply.
   1. acceptance
   2. critical
   3. critical item
   4. dependability
   5. lot
   6. maintainability
   7. maintenance
   8. non-conformance
   9. process
   10. product
   11. product assurance
   12. project
   13. quality
   14. quality assurance
   15. flight operations
   16. qualification
2. The old term “firmware” is defined in ECSS-S-ST-00-01C, and it is not used in the context of this standard because it is ambiguous and unnecessary. It is important not to confuse terms like "FPGA", "FPGA programming file" or “FPGA programming bit stream" with "firmware".
3. For the purpose of this Standard, the terms and definitions from ECSS‑E-ST-20-40 apply.
   1. Application specific integrated circuit (ASIC)
   2. Building Block
   3. code
   4. DEVICE
   5. Field Programmable Gate Array (FPGA)
   6. IP Core
   7. phase
   8. software
   9. system requirement
   10. validation
   11. verification

## Terms specific to the present standard

1. DEVICE Deactivated function

although incorporated through correct design and coding, is intended to execute in certain DEVICE product configurations only, or in none of them

1. unreachable function

function that cannot be executed due to design error or coding error

## Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

|  |  |
| --- | --- |
| Abbreviation | Meaning |
| ADPR | Architecture Definition Phase Review |
| ADPR | DEVICE Architecture Definition Phase Review |
| AR | Acceptance Review |
| CAD | Computer Aided Design |
| DDP | DEVICE development plan |
| CDR | Critical Design Review |
| DADP | DEVICE Architecture Definition Phase |
| DDDP | DEVICE Detailed Design Phase |
| DDP | DEVICE Definition Phase Review |
| DDPR | DEVICE Detailed Design Phase Review |
| DDVP | DEVICE Design and Verification Phase |
| DIP | DEVICE Implementation Phase |
| DLP | DEVICE Layout Phase |
| DPR | DEVICE Definition Phase Review |
| DRB | |  | | --- | | delivery review board  NOTE: DRB is synonymous to “Acceptance Review Board” (ARB) in ECSS-M-ST-10 | |
| DRS | DEVICE Requirements Specification |
| DSMP | DEVICE Support and Maintenance Plan |
| DVAMP | DEVICE Validation, Acceptance and Maintenance Phase |
| DVaP | DEVICE Validation Plan |
| DVeP | DEVICE Verification Plan |
| DVPR | DEVICE Design and Verification Phase Review |
| ASCII | American standard code for information interchange |
| ASIC | application specific integrated circuit |
| DPAP | DEVICE Product Assurance Plan |
| DPAR | DEVICE Product Assurance Report |
| DRF | DEVICE Reuse File |
| DVP | design validation plan |
|  | electronic design automation |
| EIDP | end item data package |
| ESCC | European Space Components Coordination |
| FM | flight model |
| FPGA | field-programmable gate array |
| FRA | feasibility and risk analysis report |
| HDL | hardware description language  NOTE: This term used in general for the various hardware description language which are applied for coding during design phase such as VHDL and verilog. |
| IEEE | Institute of Electrical and Electronics Engineers |
| IC | Integrated Circuit |
| IP | intellectual property |
| IPR | Intellectual Property Rights |
| LPR | DEVICE Layout Phase Review |
| MoM | minutes of meeting |
| NRB | Non-conformance Review Board |
| NCR | Non Conformance Record |
| OTS | Off The Shelf |
| PDR | Preliminary Design Review |
| QSL | Qualification Status List |
| QR | Qualification Review |
| SRR | System Requirements Review |
| VAMPR | Validation, Acceptance and Maintenance Phase Review |
| VHDL | Very High Speed Integrated Circuit hardware description language |

## Conventions

### Names of DEVICE development phases and reviews

ECSS-Q-ST-60-02 follows the names of DEVICE development phases and reviews defined in ECSS-E-ST-20-40. These do not follow the naming conventions defined in ECSS-M-ST-10 in an effort to use widely established ASIC, FPGA and IP Core engineering terminology which is self-explanatory and commonly used by IC engineers. In order to facilitate collaboration between IC and PA engineers ECSS-E-ST-20-40 Annex L provides a comparison between the ECSS-E-ST-20-40 phases and ECSS-M-ST-10 phases and key names.

## Nomenclature

The following nomenclature applies throughout this document:

1. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.
2. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.
3. It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.
4. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.
5. The word “can” is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.
6. In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.
7. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

# ASIC, FPGA and IP Core product assurance principles

## Overview

The objectives of ASIC, FPGA or IP Core DEVICE product assurance are to provide adequate confidence to the customer and to the supplier that the DEVICE satisfies its requirements throughout the system lifetime. In particular, that the DEVICE is developed to perform properly and safely in its operational environment, meeting the quality objectives agreed for the project.

This Standard contributes to these objectives by defining the DEVICE product assurance requirements to be met in a particular space project. These requirements deal with quality management and ECSS framework, life cycle activities and process/phase definition and quality characteristics of products.

One of the fundamental principles of this Standard is the customer/supplier relationship, assumed for all DEVICE developments. The organizational aspects of this are defined in ECSS-M-ST-10. The concept of the customer/supplier relationship is applied recursively, i.e. the customer can himself be a supplier to a higher level in the space system hierarchy.

The requirements of this Standard are applicable to the supplier, unless otherwise explicitly stated.

The supplier demonstrates compliance with the DEVICE product assurance requirements and provides the specified evidence of compliance.

To this end, the supplier specifies the DEVICE product assurance requirements for its suppliers, taking into account their responsibilities and the specific nature of their deliverables.

This Standard complements ECSS-E-ST-20-40 “Space engineering — ASIC, FPGA and IP Core engineering”, with product assurance aspects, integrated in the space system DEVICE engineering processes as defined in ECSS-E-ST-20-40. Together the two standards specify all processes for space ASIC, FPGA and IP Core DEVICE development.

## Organization of this Standard

This Standard is organized into six main parts:

* DEVICE product assurance programme implementation
* DEVICE process assurance
* DEVICE product quality assurance
* DEVICE configuration management
* Tailoring of ECSS-Q-ST-60-02 by criticality.
* Tailoring of ECSS-Q-ST-60-02 by DEVICE type

Annex A and Annex B specify the DRDs (document requirements definitions) of the DEVICE product assurance documents (DPAP and DPAR). Annex C specifies the DEVICE Reuse File (DRF). The DRDs of other engineering and management documents are included in ECSS-Q-ST-20, ECSS-E-ST-10-02 and ECSS-M-ST-40.

The DEVICE expected outputs of the ECSS-Q-ST-60-02 requirements and ECSS-E-ST-20-40 requirements is summarized in Annex D.

Annex E defines the mapping between ECSS-Q-ST-60-02C and the new ECSS-Q-ST-60-02C Revision 1.

This standards details for the DEVICE Product Assurance aspects some of the general requirements already addressed by the ECSS Management, Product Assurance and Quality Assurance standards.

## Tailoring

The general information and requirements for the selection and tailoring of applicable standards are defined in ECSS-S-ST-00.

There are several drivers for tailoring, such as dependability and safety aspects, development constraints, product quality objectives and business objectives.

Tailoring for dependability and safety aspects is based on the selection of requirements related to the verification, validation and levels of proofs demanded by the criticality of the DEVICE. Clause 9 contains a tailoring of this Standard based on DEVICE criticality.

Tailoring for DEVICE type aspects is based on the selection of requirements related to the verification, validation and levels of proofs demanded by the type of the DEVICE. Tailoring of the requirements of ECSS-Q-ST-60-02 by DEVICE type is based on the DEVICE types defined in ECSS-E-ST-20-40 Clause 6. It is noted that PA activities are consistently applied to all DEVICE types so no tailoring table is provided in this document as the tailoring is explicitly stated in the requirements text.

# Product Assurance programme implementation

## Organization and responsibility

### Organization

The supplier shall ensure that a PA organizational structure is defined for DEVICE development, and that individuals have defined tasks and responsibilities in compliance with clause 5.1.1 of ECSS-Q-ST-10 and with DRD from Annex A.

### Responsibility and authority

The responsibility, the authority and the interrelation of personnel who manage, perform and verify work affecting DEVICE quality shall be defined and documented.

The responsibilities and the interfaces of each organisation on the project, either external or internal, involved in a project shall be defined and documented.

The delegation of DEVICE product assurance tasks by a supplier to a lower level supplier shall be done in a documented and controlled way, with the supplier retaining the responsibility towards the customer.

### DEVICE product assurance responsible

#### General

The DEVICE product assurance responsible shall:

report to the project manager through the project product assurance manager;

have organisational authority and independence to propose and maintain an DEVICE product assurance programme in accordance with the project DEVICE product assurance requirements;

have access to higher management as necessary to fulfil his/her duties.

be invited to all project reviews.

#### Training

The supplier shall review the project requirements to establish and make provision for acquiring or developing the resources and skills for the management and technical staff.

The supplier shall maintain training records and ensure that trained personnel are available for the planned activities and tasks.

The supplier shall ensure that personnel conducting activities in compliance with ECSS-Q-ST-60-02 and ECSS-E-ST-20-40 are trained.

The supplier shall specify the training subjects based on the specific tools, techniques, methodologies and computer resources for use in the development and management of the DEVICE product.

1. Personnel can undergo training to acquire skills and knowledge relevant to the specific field with which the DEVICE is to deal.

## DEVICE product assurance programme management

### DEVICE product assurance planning and control

The supplier shall develop a DEVICE product assurance plan in response to the DEVICE product assurance requirements in compliance with DRD in Annex A for customer approval.

1. The DEVICE product assurance plan can be either a standalone document or a section of the supplier overall product assurance plan.

The DEVICE Product assurance programme shall include all internal manuals, standards or procedures listed in the DEVICE product assurance plan.

The DEVICE product assurance plan shall be revisited and updated to ensure that the activities to be undertaken in the following phase are defined.

The supplier shall include in the DEVICE product assurance plan a compliance matrix documenting conformance with the individual DEVICE product assurance requirements applicable for the project or business agreement.

For each DEVICE product assurance requirement, the compliance matrix shall provide a reference to the document where the expected output of that requirement is located.

### DEVICE product assurance reporting

The supplier shall provide a Product assurance report for each review and for each DEVICE delivery in compliance with DRD from Annex B covering the DEVICE product assurance activities performed during the past project phases.

### Audits

For DEVICE audits, ECSS-Q-ST-10 clause 5.2.3 shall apply.

Reviews and audits of processes and of products shall be carried out by personnel not directly involved in the DEVICE work being performed.

The supplier shall report on DEVICE Audits in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Alerts

For DEVICE alerts, ECSS-Q-ST-10 clause 5.2.9 shall apply.

The supplier shall report on DEVICE Alerts in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### DEVICE problems reporting

The supplier shall define and implement procedures for the logging, analysis and correction of all DEVICE problems encountered during DEVICE development in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

The DEVICE problem report shall contain the following information:

Identification of the DEVICE item,

Description of the problem,

Recommended solution,

Final disposition,

Modifications implemented, documents, code and tools, and

Tests re-executed.

The procedures for DEVICE problems reporting shall define the interface with the non-conformance system, the circumstances under which a problem qualifies as a non-conformance.

The supplier shall verify the application of problem reporting procedures and report the results in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Non-conformances

For DEVICE non-conformance handling, ECSS-Q-ST-10-09 shall apply.

When dealing with DEVICE non-conformance, the NRB shall include, a representative from the DEVICE product assurance and the DEVICE engineering organizations in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.1.

The NRB shall dispose DEVICE non-conformances according to the following criteria in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.4a:

Use “as‐is”, when the DEVICE is found to be usable without eliminating the non-conformance,

Rework or repair, when the DEVICE product can be made fully in conformance with all specified requirements, by:

correction of the DEVICE,

addition of DEVICE patches, or

re‐design.

Scrap,

Return to supplier.

The DEVICE product assurance plan shall specify the point in the DEVICE life cycle from which the non-conformance procedures apply.

## Risk management and critical item control

### Risk management

The DEVICE Product Assurance responsible shall provide input to Risk management for DEVICE in compliance with ECSS-M-ST-80.

### Critical item control

For critical item control, ECSS-Q-ST-10-04 shall apply.

The supplier shall identify the characteristics of the DEVICEs that qualify for inclusion in the Critical Item List.

## Supplier selection and control

### Supplier selection

For supplier selection ECSS-Q-ST-20 clause 5.4.1 shall apply.

For suppliers of existing DEVICE, including DEVICE contained in OTS equipment and units, the selection shall be performed in compliance with requirements from clause 6.2.3.

### Supplier requirements

The supplier shall establish DEVICE product assurance requirements for the next level suppliers, tailored to their role in the project.

The supplier shall provide the DEVICE product assurance requirements applicable to the next level suppliers for customer approval in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

### Supplier monitoring

The supplier shall monitor the next lower level suppliers’ conformance to the product assurance requirements.

The monitoring process shall include the review and approval of the next lower level suppliers’ product assurance plans, the continuous verification of processes and products, and the monitoring of the final validation of the product.

The supplier shall ensure that DEVICE development processes are defined and applied by the next lower level suppliers in conformance with the DEVICE product assurance requirements for suppliers.

The supplier shall provide the next lower level suppliers’ DEVICE product assurance plan for customer’s acceptance.

### Criticality classification

The supplier shall provide the lower level suppliers with the results of the safety and dependability analyses performed at higher and his level in compliance with requirements from clause 6.2.1, including:

The criticality classification of the DEVICE products to be developed,

Information about the failures that can be caused at higher level by the DEVICE products under development.

## Tools and supporting environment

### Methods and tools

Methods and tools to be used for all the activities of the development cycle, including requirements analysis, specification, modelling, design, coding, validation, testing, configuration management, verification and product assurance shall be identified by the supplier and agreed with the customer.

The choice of development methods and tools shall be justified by demonstrating through testing or documented assessment as follows:

The development team has the experience or training to apply them,

The tools and methods are applicable for the functional and operational characteristics of the product,

The tools are available throughout the development and maintenance lifetime of the product.

The correct use of methods and tools shall be verified and reported in the DEVICE product assurance report in compliance with DRD in Annex B.

### Development environment selection

The DEVICE development environment shall be selected according to the following criteria:

Availability,

Compatibility,

Performance,

Maintenance,

Durability and technical consistency with the operational equipment,

The assessment of the product with respect to requirements, including the criticality category,

The available support documentation,

The acceptance and warranty conditions,

The conditions of installation, preparation, training and use,

The maintenance conditions, including the possibilities of evolutions,

Copyright and intellectual property rights constraints, and

Dependence on one specific supplier.

The selection criteria for the DEVICE development environment shall be justified in the Development plan in compliance with DRD from ECSS-E-ST-20-40 Annex B.

The availability of the DEVICE development environment to developers and other users shall be verified before the start of each development phase.

# DEVICE Process Assurance

## DEVICE development lifecycle

### DEVICE life cycle

The DEVICE development life cycle specified in ECSS-E-ST-20-40 shall be integrated in the DEVICE product assurance plan in compliance with DRD in Annex A.

The following characteristics of the DEVICE life cycle shall be specified:

Phases,

Input and output of each phase,

Status of completion of phase output,

Reviews,

Dependencies,

Responsibilities, and

Role of the customer at each review, in conformance with ECSS-M-ST-10 and ECSS-M-ST-10-01.

In the definition of the DEVICE life cycle specified in requirement 6.1.1a and associated reviews and documents, the quality objectives as defined by the project shall be used.

The Customer shall review the DEVICE life cycle against the contractual DEVICE engineering and product assurance requirements.

The Customer shall review the DEVICE life cycle for the availability of resources.

1. Resources can include tools and human resources.

## Requirements applicable to all DEVICE engineering processes and phases

### DEVICE dependability and safety

#### Criticality classification

The PA responsible shall report the criticality classification at system-level in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

1. For the system-level analyses leading to the criticality classification of DEVICE products based on the severity of failures consequences, see ECSS-Q-ST-40 clause 6.4.1, and ECSS-Q-ST-30 clause 5.4 .

#### DEVICE dependability and safety analysis

The supplier shall perform a dependability and safety analysis at the DEVICE level, using the results of system-level safety and dependability analyses, in order to determine the criticality of each DEVICE function in compliance with ECSS-Q-ST-30 clause 5.4.

If the DEVICE is developed with the single criticality specified in the system-level dependability and safety recommendations, the supplier shall justify not performing a dependability and safety analysis at the DEVICE level.

The supplier shall report the results of the DEVICE dependability and safety analysis in the in the DEVICE Product Assurance Report in compliance with DRD in Annex B .

1. The DPAR can refer to dependability and safety documents.

The supplier shall identify the methods and techniques for the dependability and safety analysis at DEVICE level throughout the DEVICE lifecycle.

1. Dependability and safety methods and techniques are documented in ECSS-Q-ST-30 and ECSS-Q-ST-40.

Methods and techniques for DEVICE dependability and safety analysis shall be agreed between the supplier and customer.

The supplier shall report the methods and techniques used for DEVICE dependability and safety analysis in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

The supplier shall report on the status of the implementation and verification of the DEVICE dependability and safety analysis recommendations in the DEVICE product assurance report in compliance with DRD in Annex B.

1. Dependability and safety recommendations are documented in artefacts from ECSS-Q-ST-30 and ECSS-Q-ST-40.

The supplier shall provide the results of the DEVICE dependability and safety analysis for integration into the system-level dependability and safety analyses, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, addressing the following:

Additional failure modes identified at DEVICE level which had not been identified at system level,

Recommendations for system-level activities.

1. For example: introduction of hardware inhibits, and modifications of the system architecture.

### Handling of critical DEVICES

#### General

The supplier shall define, justify and apply measures to assure the dependability and safety of critical DEVICEs.

* 1. 1 For definition of DEVICEs criticality A, B or C (Catastrophic, Critical or Major) see ECSS-Q-ST-30 clause 6.5
  2. 2 These measures can include:
     + use of DEVICE development methods that have performed successfully in a similar application;
     + insertion of features for failure isolation and handling
     + defensive development techniques, such as input verification and consistency checks;
     + test or simulation coverage % ;
     + witnessed or independent testing;
     + gathering and analysis of failure statistics;
     + removing deactivated DEVICE functions or showing through a combination of analysis and testing that the means by which such DEVICE function can be inadvertently executed are prevented, isolated, or eliminated.

The application of the chosen measures to handle the critical DEVICE shall be verified in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

The need for updating the DRS, and any of DEVICE Development, verification or validation Plans and its impact in the development flow for critical DEVICE shall be analysed, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, after:

Any change of the underlying platform hardware,

Any change in the environment in which the DEVICE operates,

Any change of the tools, including configuration of the tools, that affect directly or indirectly the development of the DEVICE.

* 1. 1 For 2 example is memory used with reprogrammable FPGA.
  2. 2 Additional verification and validation, or regression testing which can be done at DEVICE or system-level

#### Unreachable functions

Identified unreachable DEVICE functions shall be removed and the need for re-verification and re-validation be analysed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Reuse of existing DEVICES

#### Reuse Category

The supplier shall identify the reused DEVICE and classify the DEVICE in one of reuse categories, in compliance with ECSS-E-ST-10-02 Table 5-1, and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

#### DEVICE Reuse File

The supplier shall provide the DEVICE Reuse File in compliance with DRD in Annex C.

The DEVICE Reuse File shall be provided for reuse categories B and C specified in ECSS-E-ST-10-02 Table 5-1.

The supplier shall provide the DEVICE Reuse File with its qualification status at the Equipment Qualification Status Review, in compliance with ECSS-E-ST-10-02 requirement 5.2.4.2.d.

For Reuse Category D, the full life cycle defined in ECSS-E-ST-20-40 shall apply.

Device Reuse File for Reuse Category D specified in requirement 6.2.3.2d is not needed to be produced.

* 1. 1 For Reuse Category A, qualification evidence is included in equipment qualification documentation.
  2. 2 For IP Core, as there is no Equipment Qualification Status Review, the DEVICE Reuse File is expected for each reviews as listed in Annex D.

The Delta qualification activities shall be completed prior to the qualification review at upper level.

Corrective actions shall be identified, documented in the DEVICE Reuse File and applied to the reused DEVICE.

#### DEVICE Licensing scheme

The supplier shall characterise, in the DRF, the deliverable DEVICE, which comprises both developed DEVICE and existing reused DEVICE, in terms of constituent elements and the associated licensing schemes, at all reviews, including:

The IPR regime and licensing scheme of the developed DEVICE, as defined by the contract,

The licence under which the reused DEVICE is accessible by the end user,

The analysis of compatibility between the reused DEVICE licence and the developed DEVICE IPR regime and licensing scheme as defined by the contract. This shall include as a minimum:

analysis of the reused DEVICE licence terms,

whether any modification has been made to the reused DEVICE and whether this modification is in line with the reused licence terms and the developed DEVICE IPR regime and licensing scheme, as defined by the contract,

the development and licensing strategy for both developed DEVICE and reused DEVICE, in order to ensure the compatibility.

1. For IP Core related development activities, item c is essential.

#### Reuse Missing documentation

Reverse engineering techniques shall be applied to generate missing documentation and to achieve the needed verification and validation coverage.

For existing DEVICE whose life cycle data from previous development is not available and reverse engineering techniques are not applicable, the following methods shall be applied:

Generation of validation and verification documents based on the available user documentation, and execution of tests to achieve the needed level of test coverage,

Use of the existing DEVICE heritage to provide evidence of the product’s suitability for the current application, including following information:

relevance of the existing DEVICE heritage for the new operational environment,

configuration management and change control of the DEVICE,

effectiveness of problem reporting,

actual error rates and maintenance records, and

impact of modifications.

#### Reuse Configuration Control

The DEVICE reuse file shall be updated at project reviews to reflect the results of the identified corrective actions for the existing DEVICE(s) not meeting the project requirements.

#### Reuse Configuration Management

All the reused DEVICEs and Building Blocks shall be kept under configuration control in compliance with ECSS-Q-ST-60-02 clause 8.

### Automatic code generation

For the selection of tools for automatic code generation, the supplier shall evaluate the following:

Evolution of the tools in relation to the tools that use the generated code as an input,

Customization of the tools to comply with project requirements,

Collection of the design and code metrics,

Verification of generated code,

Configuration control of the tools including the parameters for customization, and

Compliance with standards.

The requirements on verification and validation applicable to the automatically generated code shall ensure the achievement of the same objectives as those for manually generated code.

In case the tool is used to skip verification or testing activities on the generated code, the level of verification and validation of the automatic generation tool shall be at least the same as the one for the generated code.

Coding rules for automatic code generation tools shall be defined in the DEVICE Product Assurance Plan in compliance with DRD in Annex A and applied.

Compliance to coding rules shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

RequirementECSS-E-ST-20-40 Annex C.2.1.k shall apply to automatically generated code, unless the supplier demonstrates that the automatically generated code is not manually modified to comply with the coding and design rules applied to the manually generated code.

The verification and validation documentation shall address separately the activities to be performed for manually and automatically generated code.

### Project Security Assurance

The supplier shall define PA requirements, based on the security requirements of the project for which the DEVICE is being developed, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A for customer approval.

The supplier shall define methods and tools used to fulfil compliance to the security requirements.

The supplier shall report on conformance to the methods and tools used to fulfil the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

The supplier shall report on conformance to the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Configuration management

For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that the outputs defined in ECSS-E-ST-20-40 and in ECSS-Q-ST-60-02 are under configuration management in compliance with of ECSS-Q-ST-60-02 clause 8.

For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that changes and baseline departure for each outputs and deliverables are under configuration control.

Problems found during verification activities defined in each of ECSS-E-ST-20-40 phase shall be managed in compliance with ECSS-Q-ST-60-02 clause 5.2.5.

The supplier shall report on configuration management compliance in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Verification Control Document

The supplier shall provide for customer approval the initial VCD at the DEVICE Definition Phase review for the DEVICE requirements with the combination of the selected verification methods for the different verification levels at the applicable verification stages, in compliance with ECSS-E-ST-10-02 clause 5.2.

* 1. 1 The verification method is as defined in ECSS-E-ST-20-40 clause 4.2.
  2. 2 Some verification information can be found in ECSS-E-ST-20-40 reports and used to populate parts of the VCD. These reports are Design Verification Report, Netlist Verification Report, Layout Verification Report, ASIC Production Test Report, DEVICE Validation Report and Radiation Test Report.

The supplier shall provide an updated VCD with the Verification close out status for the DEVICE at each phase in compliance with ECSS-E-ST-10-02 clause 5.2 for customer approval.

## Requirements applicable to individual DEVICE engineering processes and activities

### DEVICE Definition Phase

The supplier shall provide traceability between System Requirements and DEVICE requirements in the VCD to confirm coverage of system requirements.

### DEVICE Design and Verification Phase

Design rules and coding rules shall be defined in the DEVICE Product Assurance Plan in compliance with DRD in Annex A and applied.

Compliance to design rules and coding rules specified in requirement 6.3.2a shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### DEVICE Design Validation, Acceptance and Maintenance phase

DEVICE testing shall be performed in accordance with a strategy for each testing level , which includes the following:

The types of tests to perform,

The tests to perform in accordance with the plans and procedures, and

The means and organizations to perform assurance function for testing and validation.

1. Examples for requirement 6.3.3a.1 are: validation against the DEVICE requirements specification, validation against the system requirements, acceptance tests, production tests or FPGA programming test.

Based on the criticality of the DEVICE, test coverage goals defined in ECSS-E-ST-20-40 requirements C2.1.g and C.2.1.l for each testing level shall be agreed between the customer and the supplier and their achievement monitored by metrics:

For validation against the DEVICE Requirements Specification, and

For validation against the system requirements.

The supplier shall ensure through internal review that the test procedures and data are feasible and traceable to the DRS and that they satisfy the DEVICE requirements.

Test coverage shall be checked with respect to the stated goals defined in ECSS-E-ST-20-40 requirement C.2.1.l and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

The supplier shall ensure that non-conformances and problem reports detected during testing are documented and reported.

1. For example: test coverage evaluation, test failure

The completion of actions related to problem reports generated during testing and validation shall be verified and recorded in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

Provisions shall be made to allow witnessing of tests by the customer as agreed by the project, in compliance with ECSS-Q-ST-20 clause 5.6.4.

Provisions shall be made to allow witnessing of tests by supplier personnel independent of the development.

1. For example: specialist product assurance personnel.

The supplier shall verify that:

Tests are conducted in accordance with approved test procedures and data,

Configuration of DEVICE under test is correct,

The tests are documented, and

The test reports are in compliance with DRD from E-ST-10-02 Annex C.

The supplier shall ensure that tests are repeatable by verifying the recording of DEVICE under test, support software and hardware, test environment, supporting documents and problems found.

The supplier shall confirm in writing that the tests are successfully completed, or that non-conformance and problem reports are raised for unsuccessful tests, in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

DEVICE Test Review Board looking to engineering and product assurance aspects shall be convened after the completion of test phases in compliance with ECSS-E-ST-10-03 clause 4.3.2.4.

Functional areas affected by any modification shall be identified and retested.

* 1. 1 This can be triggered by a non-conformance or problem report fix.
  2. 2 This can be triggered by a new FPGA bit stream and can result in full testing of the DEVICE

The need for regression testing and additional verification of the DEVICE shall be analysed after a change or update of any tool used to generate it, and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

Qualification status of the DEVICE shall be assessed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

Any qualification status maintenance activities shall be identified and performed.

In case of retesting, all test related documentation shall be updated.

1. Test related documentation includes test procedures, test specifications, data and reports.

Validation shall be carried out by staff who have not taken part in the design of the DEVICE being validated.

The necessary resources for testing shall be identified early in the DEVICE life cycle, by including the operating and maintenance requirements.

Test tool development or acquisition, hardware and software, shall be planned for in the overall project plan defined in ECSS-E-ST-20-40 Annex B.

The supplier shall establish and review the test procedures and data before starting testing activities and document the constraints of the tests concerning physical, performance, functional, controllability and observability limitations.

If the risks associated with the project justify the costs involved, Independent Verification and Validation shall be performed by a third party.

1. Where the DEVICE validation process and the DEVICE verification process are executed by an organization independent of the supplier, it is called Independent Verification and Validation (IVV).
2. The following outputs are expected:
   * + IVV plan
     + IVV report
3. The customer can consider a less rigorous level of independence, for example, an independent team in the same organization.

The validation shall include testing in the different configurations possible or in a representative set of them when it is evident that the number of possible configurations is too high to allow validation in all of them.

DEVICE containing deactivated functions shall be verified and validated to ensure that the deactivated functions cannot be activated or that their accidental activation cannot harm the operation of the system.

#### Qualification Status

The supplier shall report the assessment of the Qualification Status for the DEVICE in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

The supplier shall assess the DEVICE qualification status as follows:

Evidence of compliance to the verification process defined in ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 is provided,

The VCD, as defined in requirement 6.2.7, is confirmed complete,

All known unresolved issues impact assessment is provided with a correction plan, and

Statement that the qualification status is achieved.

* 1. 1 Examples of unresolved issue in requirement 6.3.3.2b.3 includes: Problem Reports, NCRs, RFD, RFW.
  2. 2 ECSS-M-ST-10 clause 4.4.3.6.3 objectives are used for project phasing.

The qualification status shall be approved by the Customer.

* 1. 1 The qualification status declaration is an input to the System level Qualification Review defined in ECSS-M-ST-10 Clause 4.4.3.6.3.
  2. 2 The DEVICE Qualification Status can be included in the upper-level Qualification Status List (QSL), for example, equipment QSL. QSL is defined in ECSS-Q-ST-10 Annex B.
  3. 3 The DEVICE VCD can be included in the upper level VCD, for example, equipment VCD.

#### Recurrent Products

For recurrent products, the supplier shall produce release documentation as agreed with the customer.

1. The release documentation can be the EIDP.

The Customer shall authorise production of each recurrent product.

#### Acceptance

The customer shall establish an acceptance test plan specifying the intended acceptance tests and inspection.

* 1. 1 The acceptance tests can be partly made up of tests used during previous test activities.
  2. 2 The acceptance test plan takes into account the requirement for operational demonstration, either as part of acceptance or after acceptance.

The acceptance test shall take place on the flight hardware.

The representativeness of the acceptance model against the flight model shall be justified in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

The customer shall ensure that the acceptance tests are performed in accordance with the approved acceptance test plan.

Test witnessing by PA personnel shall be defined in the acceptance Test Plan.

Test performance shall be monitored by the PA personnel in compliance with ECSS-Q-ST-20 clause 5.6.4.

The supplier shall provide an End Item Data Pack for each deliverable end item in conformance with ECSS-Q-ST-20 Annex B.

* 1. 1 The DEVICE EIDP can be part of the system or equipment EIDP
  2. 2 For recurrent products, delivery can be organised by a lot.

The Supplier shall ensure that a Delivery Review Board is convened in compliance with ECSS-Q-ST-20 clause 5.7.3

#### Maintenance

Maintenance activities shall be performed and documented in compliance to DRD in ECSS-E-ST-20-40 Annex E.

## Process Assessment and improvement

### Process assessment control

The supplier shall monitor and control the effectiveness of the processes used during the development of the DEVICE including the relevant processes corresponding to the services called from other organizational entities outside the project team and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

* 1. 1 The process assessment and improvement performed at organization level can be used to provide evidence of compliance for the project.
  2. 2 This encompasses processes defined in ECSS-Q-ST-60-02 and phases defined in ECSS-E-ST-20-40

The process assessment model and method used when performing any DEVICE process assessment shall be documented in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

### Process assessment reporting

The process assessment results shall be reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

### Process improvement

The suppliers shall ensure that the results of the process assessments are used in its project activities and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B.

# DEVICE product quality assurance

## Product quality objectives and metrication

### Assurance activities for product quality requirements

The supplier shall define assurance activities to ensure that the DEVICE meets the quality requirements, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A.

### Product Metrics definition and reporting

In order to verify the implementation of the product quality requirements, the supplier shall define a metrication programme in the DEVICE Product Assurance Plan in compliance with DRD in Annex A, specifying:

The metrics to collect and store,

Measurement method used to collect the metrics,

The target values, with reference to the product quality requirements,

The analyses to perform on the collected metrics, including the ones to derive:

descriptive statistics,

trend analysis.

How the results of the analyses performed on the collected metrics are fed back to the development team and used to identify corrective actions;

The schedule of metrics collection, storing, analysis and reporting, with reference to the whole DEVICE development flow.

### Basic metrics

The following basic products metrics shall be used:

DEVICE Requirements coverage,

Test coverage,

Number of failures,

Trend analysis on problem report and NCs.

### Reporting of metrics

The results of metrics collection and analysis shall be included in the DEVICE product assurance report in compliance with DRD in Annex B, in order to provide the customer with an insight into the level of quality obtained.

## IP Core or DEVICES intended for Reuse

### Overview

DEVICE intended for reuse can be IP Core either as a standalone project or in a frame of a project with other components under development.

### Self-contained information

The information related to components developed for reuse in the DEVICE Requirement Specification, the applicable expected outputs from ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 shall be self-contained.

### Requirements for intended reuse

The DEVICE Requirement Specification, in compliance with DRD in ECSS-E-ST-20-40 Annex A, of components developed for reuse shall include requirements for portability.

### Configuration management for intended reuse

The configuration management system shall include provisions for handling specific aspects of DEVICE developed for reuse, such as:

Longer lifetime of the components developed for reuse compared to the other components of the project,

Evolution or change of the development environment for the next project that intends to use the components;

Transfer of the configuration and documentation management information to the next project reusing the DEVICE.

### Testing on different EEE component

Where the IP core, developed for reuse, are developed for multiple EEE components, the testing of the DEVICE shall be performed on all of them.

Statement that tests have been successfully completed on all EEE components specified in requirement 7.2.5a shall be provided in release documentation.

### Certificate of conformance

The supplier shall provide a certificate of conformance in compliance with DRD in ECSS-Q-ST-20 Annex D.

# DEVICE Configuration Management

## DEVICE Configuration Management planning and control

### Configuration Management Plan

The supplier shall develop a DEVICE configuration management plan in conformance with DRD in ECSS-M-ST-40C Annex A.

The DEVICE configuration management plan shall be either a standalone document or a section of the supplier overall configuration management plan.

1. The CMP includes as a minimum:
   * + configuration identification; including identification of configuration baseline;
     + configuration control;
     + configuration status accounting;
     + configuration audits and reviews;
     + interface control;
     + supplier control.

### Software tools

The DCMP shall cover the DEVICE and its associated software tools.

## Configuration Management implementation

### DEVICE Configuration management implementation

The DEVICE configuration management system shall allow regeneration of any reference version from backups.

### CIDL and ABCL

The DEVICE Configuration Item Data List and the As-Built Configuration List shall be provided with each DEVICE delivery.

The CIDL shall be in compliance with DRD from ECSS-M-ST-40 Annex C.

1. The CIDL can be combined with the System CIDL.

The ABCL shall be in compliance with DRD from ECSS-M-ST-40 Annex D.

1. The ABCL can be combined with the System ABCL.

The CIDL and ABCL shall be provided and up to date for each project review.

Any components of the code generation tool that are customizable by the user shall be put under configuration control in the Software Configuration File in compliance with ECSS-M-ST-40 Annex E.

For components specified in the requirement 8.2.2e the change control procedures defined for the project shall address their specific aspects.

The supplier shall ensure that all authorized changes are implemented in accordance with the configuration management plan.

The mask generation and verification for ASICs shall be performed under the foundry's configuration control system.

All inputs to the design that are not automatically generated and are needed to reproduce the design shall be put under a revision control mechanism agreed with the customer.

1. Examples are simulation pattern, schematics, VHDL source codes, synthesis scripts

Each DEVICE development step using design inputs shall reflect the revision numbers of the inputs in a log file to prove consistency.

The following documents shall be controlled in compliance with ECSS-Q-ST-10 clause 5.2.5:

Procedural documents describing the quality system applied during the DEVICE life cycle,

Planning documents describing the planning and progress of the activities,

Documents describing a particular DEVICE, including:

development phase inputs,

development phase outputs,

verification and validation plans and results,

test case specifications, test procedures and test reports,

traceability matrices,

documentation for the DEVICE and system operators and users, and

maintenance documentation.

### Software configuration management implementation

Software configuration for the DEVICE software tools shall be documented in a SCF in compliance with DRD in ECSS-M-ST-40 Annex E.

1. The SCF can be combined with the ABCL.

The SCF shall be available and up to date for each DEVICE project review.

## Configuration Control

Configuration control shall be defined in conformance with ECSS-M-ST-40 clause 5.3.2.

Configuration control shall include problem reports produced during development, in compliance with clause 5.2.5

Configuration control boards shall be defined in compliance with ECSS-M-ST-40C clause 5.3.2.

Each change and departure from baseline shall be classified in accordance with ECSS-M-ST-40 clause 5.3.2.

1. A change is initiated by the customer, a departure is initiated by the supplier as defined in ECSS-M-ST-40C clause 5.3.2

At each review, the supplier shall report on any change and departure which took place during the DEVICE development phase and assess impact on previous review conclusions.

1. Example, a need to update previous review baseline document(s); or a need to perform regression test; or need to assess qualification status and define qualification maintenance.

# Tailoring by DEVICE criticality

## Device criticality categories

Criticality categories are assigned to DEVICE products as specified in ECSS-Q-ST-30 clause 5.4.

Table 9‑1 defines the relationship between the criticality category of the DEVICE, the highest criticality of the functions implemented by the DEVICE and the existing system compensating provisions, as described in ECSS-Q-ST-30, clause 5.4.

To any DEVICE defined in the right column, the corresponding criticality category in the left column is assigned. For example both "DEVICE involved in category I functions AND: no compensating provisions exist" and "DEVICE included in compensating provisions for category I functions" are category A DEVICEs.

Table 9‑1: DEVICE criticality category

| DEVICE criticality category | Definition |
| --- | --- |
| A | DEVICE involved in category I functions  AND: no compensating provisions exist |
| DEVICE included in compensating provisions for category I functions |
| B | DEVICE involved in category I functions  AND: at least one of the following compensating provisions is available, meeting the requirements defined in ECSS-Q-ST-30 clause 5.4:  - A hardware implementation; in case of DEVICE implementation it shall be classified as criticality A  - A software implementation; this software implementation shall be classified as criticality A  - An operational procedure |
| DEVICE involved in category II functions  AND: no compensating provisions exist |
| DEVICE included in compensating provisions for category II functions |
| C | DEVICE involved in category II functions  AND: at least one of the following compensating provisions is available, meeting the requirements defined in ECSS-Q-ST-30 clause 5.4:  - A hardware implementation; in case of DEVICE implementation it shall be classified as criticality B  - A software implementation; this software implementation shall be classified as criticality B  - An operational procedure |
| DEVICE involved in category III functions  AND: no compensating provisions exist |
| DEVICE included in compensating provisions for category III functions |
| D | DEVICE involved in category III functions  AND: at least one of the following compensating provisions is available, meeting the requirements defined in ECSS-Q-ST-30 clause 5.4:  - A hardware implementation; in case of DEVICE implementation it shall be classified as criticality C  - A software implementation; this software implementation shall be classified as criticality C  - An operational procedure |
| DEVICE involved in category IV functions  AND: no compensating provisions exist |

## Applicability Matrix

The following applicability matrix represents a tailoring of the requirements ECSS-Q-ST-60-02 based on the DEVICE criticality categories defined as per 9.1.

For each clause of this Standard and for each DEVICE criticality category, an indication is given whether that clause is applicable (Y), not applicable (N), agreed with Customer (C) or applicable under the conditions thereby specified to that DEVICE criticality category.

Table 9‑2: Tailoring by criticality

| Clause | Requirement | Cat A | Cat B | Cat C | Cat D |
| --- | --- | --- | --- | --- | --- |
| 5.1.1a | The supplier shall ensure that a PA organizational structure is defined for DEVICE development, and that individuals have defined tasks and responsibilities in compliance with clause 5.1.1 of ECSS-Q-ST-10 and with DRD from Annex A. | Y | Y | Y | Y |
| 5.1.2a | The responsibility, the authority and the interrelation of personnel who manage, perform and verify work affecting DEVICE quality shall be defined and documented. | Y | Y | Y | Y |
| 5.1.2b | The responsibilities and the interfaces of each organisation on the project, either external or internal, involved in a project shall be defined and documented. | Y | Y | Y | Y |
| 5.1.2c | The delegation of DEVICE product assurance tasks by a supplier to a lower level supplier shall be done in a documented and controlled way, with the supplier retaining the responsibility towards the customer. | Y | Y | Y | Y |
| 5.1.3.1a | The DEVICE product assurance responsible shall: 1. Report to the project manager through the project product assurance manager; 2. Have organisational authority and independence to propose and maintain an DEVICE product assurance programme in accordance with the project DEVICE product assurance requirements; 3. Have access to higher management as necessary to fulfil his/her duties. 4. Be invited to all project reviews. | Y | Y | Y | Y |
| 5.1.3.2a | The supplier shall review the project requirements to establish and make provision for acquiring or developing the resources and skills for the management and technical staff. | Y | Y | Y | Expected output not required |
| 5.1.3.2b | The supplier shall maintain training records and ensure that trained personnel are available for the planned activities and tasks. | Y | Y | Y | Expected output not required |
| 5.1.3.2c | The supplier shall ensure that personnel conducting activities in compliance with ECSS-Q-ST-60-02 and ECSS-E-ST-20-40 are trained. | Y | Y | Y | Expected output not required |
| 5.1.3.2d | The supplier shall specify the training subjects based on the specific tools, techniques, methodologies and computer resources for use in the development and management of the DEVICE product. | Y | Y | Y | Expected output not required |
| 5.2.1a | The supplier shall develop a DEVICE product assurance plan in response to the DEVICE product assurance requirements in compliance with DRD in Annex A for customer approval. | Y | Y | Y | Y |
| 5.2.1b | The DEVICE Product assurance programme shall include all internal manuals, standards or procedures listed in the DEVICE product assurance plan. | Y | Y | Y | Expected output not required |
| 5.2.1c | The DEVICE product assurance plan shall be revisited and updated to ensure that the activities to be undertaken in the following phase are defined. | Y | Y | Y | Y |
| 5.2.1d | The supplier shall include into the DEVICE product assurance plan a compliance matrix documenting conformance with the individual DEVICE product assurance requirements applicable for the project or business agreement. | Y | Y | Y | Y |
| 5.2.1e | For each DEVICE product assurance requirement, the compliance matrix shall provide a reference to the document where the expected output of that requirement is located. | Y | Y | Y | Expected output not required |
| 5.2.2a | The supplier shall provide a Product assurance report for each review and for each DEVICE delivery in compliance with DRD from Annex B covering the DEVICE product assurance activities performed during the past project phases. | Y | Y | Y | Y |
| 5.2.3a | For DEVICE audits, ECSS-Q-ST-10 clause 5.2.3 shall apply. | Y | Y | Y | C |
| 5.2.3b | Reviews and audits of processes and of products shall be carried out by personnel not directly involved in the DEVICE work being performed. | Y | Y | Y | Y |
| 5.2.3c | The supplier shall report on DEVICE Audits in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 5.2.4a | For DEVICE alerts, ECSS-Q-ST-10 clause 5.2.9 shall apply. | Y | Y | Y | Y |
| 5.2.4b | The supplier shall report on DEVICE Alerts in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 5.2.5a | The supplier shall define and implement procedures for the logging, analysis and correction of all DEVICE problems encountered during DEVICE development in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | Y | Y |
| 5.2.5b | The DEVICE problem report shall contain the following information: 1. Identification of the DEVICE item, 2. Description of the problem, 3. Recommended solution, 4. Final disposition, 5. Modifications implemented, documents, code and tools, and 6. Tests re-executed. | Y | Y | Y | Y |
| 5.2.5c | The procedures for DEVICE problems reporting shall define the interface with the non-conformance system, the circumstances under which a problem qualifies as a non-conformance. | Y | Y | Y | Y |
| 5.2.5d | The supplier shall verify the application of problem reporting procedures and report the results in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 5.2.6a | For DEVICE non-conformance handling, ECSS-Q-ST-10-09 shall apply. | Y | Y | Y | Y |
| 5.2.6b | When dealing with DEVICE non-conformance, the NRB shall include, a representative from the DEVICE product assurance and the DEVICE engineering organizations in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.1. | Y | Y | Y | Y |
| 5.2.6c | The NRB shall dispose DEVICE non-conformances according to the following criteria in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.4a: 1. Use “as‐is”, when the DEVICE is found to be usable without eliminating the non-conformance, 2. Rework or repair, when the DEVICE product can be made fully in conformance with all specified requirements, by: (a) correction of the DEVICE, (b) addition of DEVICE patches, or (c) re‐design. 3. Scrap,  4. Return to supplier. | Y | Y | Y | Y |
| 5.2.6d | The DEVICE product assurance plan shall specify the point in the DEVICE life cycle from which the non-conformance procedures apply. | Y | Y | Y | Y |
| 5.3.1a | The DEVICE Product Assurance responsible shall provide input to Risk management for DEVICE in compliance with ECSS-M-ST-80. | Y | Y | Y | Y |
| 5.3.2a | For critical item control, ECSS-Q-ST-10-04 shall apply. | Y | Y | Y | N |
| 5.3.2b | The supplier shall identify the characteristics of the DEVICEs that qualify for inclusion in the Critical Item List. | Y | Y | Y | N |
| 5.4.1a | For supplier selection ECSS-Q-ST-20 clause 5.4.1 shall apply. | Y | Y | Y | N |
| 5.4.1b | For suppliers of existing DEVICE, including DEVICE contained in OTS equipment and units, the selection shall be performed in compliance with requirements from clause 6.2.3. | Y | Y | Y | N except for licensing/IPR information |
| 5.4.2a | The supplier shall establish DEVICE product assurance requirements for the next level suppliers, tailored to their role in the project. | Y | Y | Y | Y |
| 5.4.2b | The supplier shall provide the DEVICE product assurance requirements applicable to the next level suppliers for customer approval, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | Y | Y |
| 5.4.3a | The supplier shall monitor the next lower level suppliers’ conformance to the product assurance requirements. | Y | Y | Y | Y |
| 5.4.3b | The monitoring process shall include the review and approval of the next lower level suppliers’ product assurance plans, the continuous verification of processes and products, and the monitoring of the final validation of the product. | Y | Y | Y | Y |
| 5.4.3c | The supplier shall ensure that DEVICE development processes are defined and applied by the next lower level suppliers in conformance with the DEVICE product assurance requirements for suppliers. | Y | Y | Y | Y |
| 5.4.3d | The supplier shall provide the next lower level suppliers’ DEVICE product assurance plan for customer’s acceptance. | Y | Y | Y | Y |
| 5.4.4a | The supplier shall provide the lower level suppliers with the results of the safety and dependability analyses performed at higher and his level in compliance with requirements from clause 6.2.1, including: 1. The criticality classification of the DEVICE products to be developed, 2. Information about the failures that can be caused at higher level by the DEVICE products under development. | Y | Y | Y | N |
| 5.5.1a | Methods and tools to be used for all the activities of the development cycle, including requirements analysis, specification, modelling, design, coding, validation, testing, configuration management, verification and product assurance shall be identified by the supplier and agreed with the customer. | Y | Y | Y | Y |
| 5.5.1b | The choice of development methods and tools shall be justified by demonstrating through testing or documented assessment as follows: 1. The development team has the experience or training to apply them, 2. The tools and methods are applicable for the functional and operational characteristics of the product,  3. The tools are available throughout the development and maintenance lifetime of the product. |  |  |  |  |
| 5.5.1c | The correct use of methods and tools shall be verified and reported in the DEVICE product assurance report in compliance with DRD in Annex B. | Y | Y | Y | Expected output not required |
| 5.5.2a | The DEVICE development environment shall be selected according to the following criteria: 1. Availability, 2. Compatibility, 3. Performance, 4. Maintenance, 5. Durability and technical consistency with the operational equipment, 6. The assessment of the product with respect to requirements, including the criticality category, 7. The available support documentation, 8. The acceptance and warranty conditions, 9. The conditions of installation, preparation, training and use, 10. The maintenance conditions, including the possibilities of evolutions, 11. Copyright and intellectual property rights constraints, and 12. Dependence on one specific supplier. | Y | Y | Y | Expected output not required |
| 5.5.2b | The selection criteria for the DEVICE development environment shall be justified in the Development plan in compliance with DRD from ECSS-E-ST-20-40 Annex B. | Y | Y | Y | Expected output not required |
| 5.5.2c | The availability of the DEVICE development environment to developers and other users shall be verified before the start of each development phase. | Y | Y | Y | Expected output not required |
| 6.1.1a | The DEVICE development life cycle specified in ECSS-E-ST-20-40 shall be integrated in the DEVICE product assurance plan in compliance with DRD in Annex A. | Y | Y | Y | Y |
| 6.1.1b | The following characteristics of the DEVICE life cycle shall be specified:  1. Phases,  2. Input and output of each phase,  3. Status of completion of phase output,  4. Reviews,  5. Dependencies,  6. Responsibilities, and  7. Role of the customer at each review, in conformance with ECSS-M-ST-10 and ECSS-M-ST-10-01. | Y | Y | Y | Y |
| 6.1.1c | In the definition of the DEVICE life cycle specified in requirement 6.1.1a and associated reviews and documents, the quality objectives as defined by the project shall be used. | Y | Y | Y | Y |
| 6.1.1d | The Customer shall review the DEVICE life cycle against the contractual DEVICE engineering and product assurance requirements. | Y | Y | Y | Y |
| 6.1.1e | The Customer shall review the DEVICE life cycle for the availability of resources. | Y | Y | Y | Y |
| 6.2.1.1a | The PA responsible shall report the criticality classification at system-level in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | Y | Y |
| 6.2.1.2a | The supplier shall perform a dependability and safety analysis at the DEVICE level, using the results of system-level safety and dependability analyses, in order to determine the criticality of each DEVICE function in compliance with ECSS-Q-ST-30 clause 5.4. | Y | Y | Y | Y |
| 6.2.1.2b | If the DEVICE is developed with the single criticality specified in the system-level dependability and safety recommendations, the supplier shall justify not performing a dependability and safety analysis at the DEVICE level. | Y | Y | Y | N |
| 6.2.1.2c | The supplier shall report the results of the DEVICE dependability and safety analysis in the in the DEVICE Product Assurance Report in compliance with DRD in Annex B . | Y | Y | Y | N |
| 6.2.1.2d | The supplier shall identify the methods and techniques for the dependability and safety analysis at DEVICE level throughout the DEVICE lifecycle. | Y | Y | Y | N |
| 6.2.1.2e | Methods and techniques for DEVICE dependability and safety analysis shall be agreed between the supplier and customer. | Y | Y | Y | N |
| 6.2.1.2f | The supplier shall report the methods and techniques used for DEVICE dependability and safety analysis in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | Y | N |
| 6.2.1.2g | The supplier shall report on the status of the implementation and verification of the DEVICE dependability and safety analysis recommendations in the DEVICE product assurance report in compliance with DRD in Annex B. | Y | Y | Y | N |
| 6.2.1.2h | The supplier shall provide the results of the DEVICE dependability and safety analysis for integration into the system-level dependability and safety analyses, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, addressing the following: 1. Additional failure modes identified at DEVICE level which had not been identified at system level, 2. Recommendations for system-level activities. | Y | Y | Y | N |
| 6.2.2.1a | The supplier shall define, justify and apply measures to assure the dependability and safety of critical DEVICEs. | Y | Y | Y | N |
| 6.2.2.1b | The application of the chosen measures to handle the critical DEVICE shall be verified in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | N |
| 6.2.2.1c | The need for updating the DRS, and any of DEVICE Development, verification or validation Plans and its impact in the development flow for critical DEVICE shall be analysed, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, after:  1. Any change of the underlying platform hardware,  2. Any change in the environment in which the DEVICE operates, 3. Any change of the tools, including configuration of the tools, that affect directly or indirectly the development of the DEVICE. | Y | Y | Y | Y |
| 6.2.2.2a | Identified unreachable DEVICE functions shall be removed and the need for re-verification and re-validation be analysed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | N |
| 6.2.3.1a | The supplier shall identify the reused DEVICE and classify the DEVICE in one of reuse categories, in compliance with ECSS-E-ST-10-02 Table 5-1, and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.2.3.2a | The supplier shall provide DEVICE Reuse File in compliance with DRD in Annex C. | Y | Y | Y | Y |
| 6.2.3.2b | The DEVICE Reuse File shall be provided for reuse categories B and C specified in ECSS-E-ST-10-02 Table 5-1. | Y | Y | Y | Y |
| 6.2.3.2c | The supplier shall provide the DEVICE Reuse File with its qualification status at the Equipment Qualification Status Review, in compliance with ECSS-E-ST-10-02 requirement 5.2.4.2.d. | Y | Y | Y | Y |
| 6.2.3.2d | For Reuse Category D, the full life cycle defined in ECSS-E-ST-20-40 shall apply. | Y | Y | Y | Y |
| 6.2.3.2e | Device Reuse File for Reuse Category D specified in requirement 6.2.3.2c is not needed to be produced. | Y | Y | Y | Y |
| 6.2.3.2f | The Delta qualification activities shall be completed prior to the qualification review at upper level. | Y | Y | Y | Y |
| 6.2.3.2g | Corrective actions shall be identified, documented in the DEVICE Reuse File and applied to the reused DEVICE. | Y | Y | Y | Y |
| 6.2.3.3a | The supplier shall characterise, in the DRF, the deliverable DEVICE, which comprises both developed DEVICE and existing reused DEVICE, in terms of constituent elements and the associated licensing schemes, at all reviews, including: 1. The IPR regime and licensing scheme of the developed DEVICE, as defined by the contract, 2. The licence under which the reused DEVICE is accessible by the end user, 3. The analysis of compatibility between the reused DEVICE licence and the developed DEVICE IPR regime and licensing scheme as defined by the contract. This shall include as a minimum: (a) analysis of the reused DEVICE licence terms,  (b) whether any modification has been made to the reused DEVICE and whether this modification is in line with the reused licence terms and the developed DEVICE IPR regime and licensing scheme, as defined by the contract,  (c) the development and licensing strategy for both developed DEVICE and reused DEVICE, in order to ensure the compatibility. | Y | Y | Y | Y |
| 6.2.3.4a | Reverse engineering techniques shall be applied to generate missing documentation and to achieve the needed verification and validation coverage. | Y | Y | Y | Y |
| 6.2.3.4b | For existing DEVICE whose life cycle data from previous development is not available and reverse engineering techniques are not applicable, the following methods shall be applied: 1. Generation of validation and verification documents based on the available user documentation, and execution of tests to achieve the needed level of test coverage,  2. Use of the existing DEVICE heritage to provide evidence of the product’s suitability for the current application, including following information: (a) relevance of the existing DEVICE heritage for the new operational environment,  (b) configuration management and change control of the DEVICE,  (c) effectiveness of problem reporting,  (d) actual error rates and maintenance records, and  (e) impact of modifications. | Y | Y | Y | Y |
| 6.2.3.5a | The DEVICE reuse file shall be updated at project reviews to reflect the results of the identified corrective actions for the existing DEVICE(s) not meeting the project requirements. | Y | Y | Y | Y |
| 6.2.3.6a | All the reused DEVICEs and Building Blocks shall be kept under configuration control in compliance with ECSS-Q-ST-60-02 clause 8. | Y | Y | Y | Y |
| 6.2.4a | For the selection of tools for automatic code generation, the supplier shall evaluate the following:  1. Evolution of the tools in relation to the tools that use the generated code as an input,  2. Customization of the tools to comply with project requirements,  3. Collection of the design and code metrics,  4. Verification of generated code,  5. Configuration control of the tools including the parameters for customization, and  6. Compliance with standards. | Y | Y | Y | Y |
| 6.2.4b | The requirements on verification and validation applicable to the automatically generated code shall ensure the achievement of the same objectives as those for manually generated code. | Y | Y | Y | Y |
| 6.2.4c | In case the tool is used to skip verification or testing activities on the generated code, the level of verification and validation of the automatic generation tool shall be at least the same as the one for the generated code. | Y | Y | Y | Y |
| 6.2.4d | Coding rules for automatic code generation tools shall be defined in the DEVICE Product Assurance Plan in compliance with DRD in Annex A and applied. | Y | Y | Y | Y |
| 6.2.4e | Compliance to coding rules shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.2.4f | Requirement ECSS-E-ST-20-40 Annex C.2.1.k shall apply to automatically generated code, unless the supplier demonstrates that the automatically generated code is not manually modified to comply with the coding and design rules applied to the manually generated code. | Y | Y | Y | Y |
| 6.2.4g | The verification and validation documentation shall address separately the activities to be performed for manually and automatically generated code. | Y | Y | Y | Y |
| 6.2.5a | The supplier shall define PA requirements, based on the security requirements of the project for which the DEVICE is being developed in the DEVICE Product Assurance Plan in compliance with DRD in Annex A for customer approval. | Y | Y | Y | Y |
| 6.2.5b | The supplier shall define methods and tools used to fulfil compliance to the security requirements. | Y | Y | Y | Y |
| 6.2.5c | The supplier shall report on conformance to the methods and tools used to fulfil the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.2.5d | The supplier shall report on conformance to the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.2.6a | For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that the outputs defined in ECSS-E-ST-20-40 and in ECSS-Q-ST-60-02 are under configuration management in compliance with of ECSS-Q-ST-60-02 clause 8. | Y | Y | Y | Y |
| 6.2.6b | For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that changes and baseline departure for each outputs and deliverables are under configuration control. | Y | Y | Y | Y |
| 6.2.6c | Problems found during verification activities defined in each of ECSS-E-ST-20-40 phase shall be managed in compliance with ECSS-Q-ST-60-02 clause 5.2.5. | Y | Y | Y | Y |
| 6.2.6d | The supplier shall report on configuration management compliance in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.2.7a | The supplier shall provide for customer approval the initial VCD at the DEVICE Definition Phase review for the DEVICE requirements with the combination of the selected verification methods for the different verification levels at the applicable verification stages, in compliance with ECSS-E-ST-10-02 clause 5.2. | Y | Y | Y | Y |
| 6.2.7b | The supplier shall provide an updated VCD with the Verification close out status for the DEVICE at each phase in compliance with ECSS-E-ST-10-02 clause 5.2. | Y | Y | Y | Y |
| 6.3.1a | The supplier shall provide traceability between System Requirements and DEVICE requirements in the VCD to confirm coverage of system requirements. | Y | Y | Y | Y |
| 6.3.2a | Design rules and coding rules shall be defined in the DEVICE Product Assurance in compliance with DRD in Annex A and applied. | Y | Y | Y | C |
| 6.3.2b | Compliance to design rules and coding Rules specified in requirement 6.3.2a shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | C |
| 6.3.3a | DEVICE testing shall be performed in accordance with a strategy for each testing level , which includes the following:  1. The types of tests to perform, 2. The tests to perform in accordance with the plans and procedures, and 3. The means and organizations to perform assurance function for testing and validation. | Y | Y | Y | Y |
| 6.3.3b | Based on the criticality of the DEVICE, test coverage goals defined in ECSS-E-ST-20-40 requirements C2.1.g and C.2.1.l for each testing level shall be agreed between the customer and the supplier and their achievement monitored by metrics:  1. For validation against the DEVICE Requirements Specification, and 2. For validation against the system requirements. | C | C | C | C |
| 6.3.3c | The supplier shall ensure through internal review that the test procedures and data are feasible and traceable to the DRS and that they satisfy the DEVICE requirements. | Y | Y | Y | Expected output not required |
| 6.3.3d | Test coverage shall be checked with respect to the stated goals defined in ECSS-E-ST-20-40 requirement C.2.1.l and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | C | C | C | C |
| 6.3.3e | The supplier shall ensure that non-conformances and problem reports detected during testing are documented and reported. | Y | Y | Y | Y |
| 6.3.3f | The completion of actions related to problem reports generated during testing and validation shall be verified and recorded in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3g | Provisions shall be made to allow witnessing of tests by the customer as agreed by the project, in compliance with ECSS-Q-ST-20 clause 5.6.4. | Y | Y | Y | Y |
| 6.3.3h | Provisions shall be made to allow witnessing of tests by supplier personnel independent of the development. | Y | Y | Y | Y |
| 6.3.3i | The supplier shall verify that:  1. Tests are conducted in accordance with approved test procedures and data,  2. Configuration of DEVICE under test is correct,  3. The tests are documented, and  4. The test reports are in compliance with DRD from E-ST-10-02 Annex C. | Y | Y | Y | Expected output not required |
| 6.3.3j | The supplier shall ensure that tests are repeatable by verifying the recording of DEVICE under test, support software and hardware, test environment, supporting documents and problems found. | Y | Y | Y | Expected output not required |
| 6.3.3k | The supplier shall confirm in writing that the tests are successfully completed, or that non-conformance and problem reports are raised for unsuccessful tests, in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3l | DEVICE Test Review Board looking to engineering and product assurance aspects shall be convened after the completion of test phases in compliance with ECSS-E-ST-10-03 clause 4.3.2.4. | Y | Y | Y | Y |
| 6.3.3m | Functional areas affected by any modification shall be identified and retested. | Y | Y | Y | Y |
| 6.3.3n | The need for regression testing and additional verification of the DEVICE shall be analysed after a change or update of any tool used to generate it, and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3o | Qualification status of the DEVICE shall be assessed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3p | Any qualification status maintenance activities shall be identified and performed. | Y | Y | Y | Y |
| 6.3.3q | In case of retesting, all test related documentation shall be updated. | Y | Y | Y | Y |
| 6.3.3r | Validation shall be carried out by staff who have not taken part in the design of the DEVICE being validated. | Y | Y | Y | Y |
| 6.3.3s | The necessary resources for testing shall be identified early in the DEVICE life cycle, by including the operating and maintenance requirements. | Y | Y | Y | Expected output not required |
| 6.3.3t | Test tool development or acquisition, hardware and software, shall be planned for in the overall project plan defined in ECSS-E-ST-20-40 Annex B. | Y | Y | Y | Y |
| 6.3.3u | The supplier shall establish and review the test procedures and data before starting testing activities and document the constraints of the tests concerning physical, performance, functional, controllability and observability limitations. | Y | Y | Y | Y |
| 6.3.3v | If the risks associated with the project justify the costs involved, Independent Verification and Validation shall be performed by a third party. | Y | N | N | N |
| 6.3.3w | The validation shall include testing in the different configurations possible or in a representative set of them when it is evident that the number of possible configurations is too high to allow validation in all of them. | Y | N | Y | Y |
| 6.3.3x | DEVICE containing deactivated functions shall be verified and validated to ensure that the deactivated functions cannot be activated or that their accidental activation cannot harm the operation of the system. | Y | Y | Y | Y |
| 6.3.3.2a | The supplier shall report the assessment of the Qualification Status for the DEVICE in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3.2b | The supplier shall assess the DEVICE qualification status as follows: 1. Evidence of compliance to the verification process defined in ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 is provided, 2. The VCD, as defined in requirement 6.2.7, is confirmed complete, 3. All known unresolved issues impact assessment is provided with a correction plan, and 4. Statement that the qualification status is achieved. | Y | Y | Y | Y |
| 6.3.3.2c | The qualification status shall be approved by the Customer. | Y | Y | Y | Y |
| 6.3.3.3a | For recurrent products, the supplier shall produce release documentation as agreed with the customer. | Y | Y | Y | Y |
| 6.3.3.3b | The Customer shall authorise production of each recurrent product. | Y | Y | Y | Y |
| 6.3.3.4a | The customer shall establish an acceptance test plan specifying the intended acceptance tests and inspection. | Y | Y | Y | Y |
| 6.3.3.4b | The acceptance test shall take place on the flight hardware. | Y | Y | Y | Y |
| 6.3.3.4c | The representativeness of the acceptance model against the flight model shall be justified in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | Y | Y |
| 6.3.3.4d | The customer shall ensure that the acceptance tests are performed in accordance with the approved acceptance test plan. | Y | Y | Y | Y |
| 6.3.3.4e | Test witnessing by PA personnel shall be defined in the acceptance Test Plan. | Y | Y | Y | Y |
| 6.3.3.4f | Test performance shall be monitored by the PA personnel in compliance with ECSS-Q-ST-20 clause 5.6.4. | Y | Y | Y | Y |
| 6.3.3.4g | The supplier shall provide an End Item Data Pack for each deliverable end item in conformance with ECSS-Q-ST-20 Annex B. | Y | Y | Y | Y |
| 6.3.3.4h | The Supplier shall ensure that a Delivery Review Board is convened in compliance with ECSS-Q-ST-20 clause 5.7.3 | Y | Y | Y | Y |
| 6.3.3.5a | Maintenance activities shall be performed and documented in compliance to DRD in ECSS-E-ST-20-40 Annex E. | Y | Y | Y | Y |
| 6.4.1a | The supplier shall monitor and control the effectiveness of the processes used during the development of the DEVICE including the relevant processes corresponding to the services called from other organizational entities outside the project team and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | C | N |
| 6.4.1b | The process assessment model and method used when performing any DEVICE process assessment shall be documented in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | C | N |
| 6.4.2a | The process assessment results shall be reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | C | N |
| 6.4.3a | The suppliers shall ensure that the results of the process assessments are used in its project activities and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Y | Y | C | N |
| 7.1.1a | The supplier shall define assurance activities to ensure that the DEVICE meets the quality requirements, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Y | Y | Y | Y |
| 7.1.2a | In order to verify the implementation of the product quality requirements, the supplier shall define a metrication programme , and reported in the DEVICE Product Assurance Plan in compliance with DRD in Annex A, specifying: 1. The metrics to collect and store, 2. Measurement method used to collect the metrics, 3. The target values, with reference to the product quality requirements, 4. The analyses to perform on the collected metrics, including the ones to derive: (a) descriptive statistics, (b) trend analysis. 5. How the results of the analyses performed on the collected metrics are fed back to the development team and used to identify corrective actions; 6. The schedule of metrics collection, storing, analysis and reporting, with reference to the whole DEVICE development flow. | Y | Y | Y | Y |
| 7.1.3a | The following basic products metrics shall be used: 1. DEVICE Requirements coverage, 2. Test coverage, 3. Number of failures, 4. Trend analysis on problem report and NCs. | Y | Y | Y | Y |
| 7.1.4a | The results of metrics collection and analysis shall be included in the DEVICE product assurance report in compliance with DRD in Annex B, in order to provide the customer with an insight into the level of quality obtained. | Y | Y | Y | Y |
| 7.2.2a | The information related to components developed for reuse in the DEVICE Requirement Specification, the applicable expected outputs from ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 shall be self-contained. | Y | Y | Y | Y |
| 7.2.3a | The DEVICE Requirement Specification, in compliance with DRD in ECSS-E-ST-20-40 Annex A, of components developed for reuse shall include requirements for portability. | Y | Y | Y | Y |
| 7.2.4a | The configuration management system shall include provisions for handling specific aspects of DEVICE developed for reuse, such as: 1. Longer lifetime of the components developed for reuse compared to the other components of the project, 2. Evolution or change of the development environment for the next project that intends to use the components;  3. Transfer of the configuration and documentation management information to the next project reusing the DEVICE. | Y | Y | Y | Y |
| 7.2.5a | Where the IP core, developed for reuse, are developed for multiple EEE components, the testing of the DEVICE shall be performed on all of them. | Y | Y | Y | Y |
| 7.2.5b | Statement that tests have been successfully completed on all EEE components specified in requirement 7.2.5a shall be provided in release documentation. | Y | Y | Y | Y |
| 7.2.6a | The supplier shall provide a certificate of conformance in compliance with DRD in ECSS-Q-ST-20 Annex D. | Y | Y | Y | Y |
| 8.1.1a | The supplier shall develop a DEVICE configuration management plan in conformance with DRD in ECSS-M-ST-40C Annex A. | Y | Y | Y | Y |
| 8.1.1b | The DEVICE configuration management plan shall be either a standalone document or a section of the supplier overall configuration management plan. | Y | Y | Y | Y |
| 8.1.2a | The DCMP shall cover the DEVICE and its associated software tools. | Y | Y | Y | Y |
| 8.2.1a | The DEVICE configuration management system shall allow regeneration of any reference version from backups. | Y | Y | Y | Y |
| 8.2.2a | The DEVICE Configuration Item Data List and the As-Built Configuration List shall be provided with each DEVICE delivery. | Y | Y | Y | Y |
| 8.2.2b | The CIDL shall be in compliance with DRD from ECSS-M-ST-40 Annex C. | Y | Y | Y | Y |
| 8.2.2c | The ABCL shall be in compliance with DRD from ECSS-M-ST-40 Annex D. | Y | Y | Y | Y |
| 8.2.2d | The CIDL and ABCL shall be provided and up to date for each project review. | Y | Y | Y | Y |
| 8.2.2e | Any components of the code generation tool that are customizable by the user shall be put under configuration control in the Software Configuration File in compliance with ECSS-M-ST-40 Annex E. | Y | Y | Y | Y |
| 8.2.2f | For components specified in the requirement 8.2.2e the change control procedures defined for the project shall address their specific aspects. | Y | Y | Y | Y |
| 8.2.2g | The supplier shall ensure that all authorized changes are implemented in accordance with the configuration management plan. | Y | Y | Y | Y |
| 8.2.2h | The mask generation and verification for ASICs shall be performed under the foundry's configuration control system. | Y | Y | Y | Y |
| 8.2.2i | All inputs to the design that are not automatically generated and are needed to reproduce the design shall be put under a revision control mechanism agreed with the customer. | Y | Y | Y | Y |
| 8.2.2j | Each DEVICE development step using design inputs shall reflect the revision numbers of the inputs in a log file to prove consistency. | Y | Y | Y | Y |
| 8.2.2k | The following documents shall be controlled in compliance with ECSS-Q-ST-10 clause 5.2.5:  1. Procedural documents describing the quality system applied during the DEVICE life cycle,  2. Planning documents describing the planning and progress of the activities,  3. Documents describing a particular DEVICE, including:  (a) development phase inputs,  (b) development phase outputs,  (c) verification and validation plans and results,  (d) test case specifications, test procedures and test reports,  (e) traceability matrices,  (f) documentation for the DEVICE and system operators and users, and (g) maintenance documentation. | Y | Y | Y | Y |
| 8.2.3a | Software configuration for the DEVICE software tools shall be documented in a SCF in compliance with DRD in ECSS-M-ST-40 Annex E. | Y | Y | Y | Y |
| 8.2.3b | The SCF shall be available and up to date for each DEVICE project review. | Y | Y | Y | Y |
| 8.3a | Configuration control shall be defined in conformance with ECSS-M-ST-40 clause 5.3.2. | Y | Y | Y | Y |
| 8.3b | Configuration control shall include problem reports produced during development, in compliance with clause 5.2.5 | Y | Y | Y | Y |
| 8.3c | Configuration control boards shall be defined in compliance with ECSS-M-ST-40C clause 5.3.2. | Y | Y | Y | Y |
| 8.3d | Each change and departure from baseline shall be classified in accordance with ECSS-M-ST-40 clause 5.3.2. | Y | Y | Y | Y |
| 8.3e | At each review, the supplier shall report on any change and departure which took place during the DEVICE development phase and assess impact on previous review conclusions. | Y | Y | Y | Y |

1. (normative)  
   DEVICE Product Assurance Plan (DPAP) - DRD
   1. DRD identification
      1. Requirement identification and source document

This DRD is called from ECSS-Q-ST-60-02C Rev.1requirement 5.1.1a.

* + 1. Purpose and objective

The purpose of the DEVICE product assurance plan is to provide information on the organizational aspects and the technical approach to the execution of the DEVICE product assurance programme.

* 1. Expected response
     1. Scope and content

Introduction

The DPAP shall contain the definition of the purpose, objective, content and the reason of its preparation.

Applicable and reference documents

The DPAP shall list the applicable and reference documents to support the generation of the document.

Terms, definitions and abbreviated terms

The DPAP shall include any additional terms, definition or abbreviated terms used.

System Overview

The DPAP shall include a description of the system and DEVICE being developed.

DEVICE product assurance programme implementation

Organization

The DPAP shall define the organization of DEVICE product assurance activities, including responsibility, authority and the interrelation of personnel who manage, perform and verify work affecting DEVICE quality.

The DPAP shall include the following topics:

Organizational structure,

Interfaces of each organisation, either external or internal, involved in the project,

Relationship to the system level product assurance and safety,

Independence of the DEVICE product assurance function,

Delegation of DEVICE product assurance tasks to a lower level supplier.

Responsibilities

The DPAP shall define the responsibilities of the DEVICE product assurance function.

Resources

The DPAP shall define the resources used to perform the DEVICE product assurance function.

The resources defined in A.2.1<5.3>a shall include human resources and skills, and software tools.

Reporting

The DPAP shall define the reporting performed by DEVICE product assurance.

Risk management

The DPAP shall define the contribution of the DEVICE product assurance function to the project risk management.

Supplier selection and control

The DPAP shall define the contribution of the DEVICE product assurance function to the next level suppliers selection and control.

Criticality analysis

The DPAP shall define the result of the criticality analysis performed at System level.

The DPAP shall define the method and tools used for the DEVICE criticality analysis.

Methods and tools

The DPAP shall define the methods and tools used for all the activities of the development cycle, and their level of maturity.

Maintenance (optional)

The DPAP shall specify the quality measures related to the operations and maintenance processes

1. Alternatively, a separate DPAP is produced.

DEVICE process assurance

DEVICE development cycle

The DPAP shall refer to the DEVICE development cycle definition in the DEVICE development plan.

If not covered in the DEVICE development plan, the life cycle shall be defined.

The life cycle shall include a milestone immediately before the starting of the DEVICE validation.

Projects plans

The DPAP shall define all plans be produced and used in the project.

The relationship between the project plans and a timely planning for their preparation and update shall be specified.

DEVICE dependability and safety

The DPAP shall contain a definition and justification of the measures applied for the handling of critical DEVICEs, including the analyses performed and the standards applicable for critical DEVICE.

DEVICE security assurance

The DPAP shall contain a description of the Security standards, practices and procedures applied

The DPAP shall contain a description of the tools and methods applied

Process assessment and improvement

The DPAP shall state the scope and objectives of process assessment.

The DPAP shall define the methods and tools used for process assessment and improvement.

DEVICE documentation and configuration management

The DPAP shall define the contribution of the DEVICE product assurance function to the proper implementation of documentation and configuration management.

The non-conformance control system shall be defined or referenced.

The point in the DEVICE life cycle from which the non-conformance procedures apply shall be specified.

The DPAP shall identify method and tool to protect the supplied DEVICE.

Reuse of DEVICE

The DPAP shall define the approach for the reuse of existing DEVICE, including delta qualification.

Product assurance planning for individual processes and activities

The following processes and activities shall be covered, taking into account the project scope and life cycle:

DEVICE definition analysis,

DEVICE design,

DEVICE verification,

testing and validation, including regression testing,

Independent Verification and Validation,

DEVICE delivery and acceptance,

Maintenance.

The DPAP shall define the approach to assess the qualification status of the DEVICE

The DPAP shall specify the approach to allow recurrent(s) production

The DPAP shall define the approach to assess Deactivated functions, Configurable functions and Unreachable functions.

The DPAP shall define the approach to automatic code generation.

Procedures and standards

The DPAP shall define or list by reference all procedures and standards applicable to the development of the DEVICE in the project

The DEVICE product assurance measures to ensure compliance to the project procedures and standards shall be specified.

The standards and procedures defined or listed in accordance with <6.9>a shall be as a minimum those covering the following aspects:

Project management,

Risk management,

Configuration and documentation management,

Verification and validation,

Requirements engineering,

Design,

Coding,

Metrication,

Non-conformance control,

Audits,

Alerts,

Reuse of existing DEVICE,

Use of methods and tools,

Qualification including status assessment

Delivery and acceptance;

Maintenance.

DEVICE product quality assurance

The DPAP shall define the approach to ensure the quality of the DEVICE product.

The description of the approach specified in A.2.1<7>a shall include the:

Specification of the product metrics, their target values and the means to collect them,

Definition of a metrication programme,

Analyses performed on the collected metrics,

Way the results are fed back to the development team,

Documentation quality requirements,

Assurance activities meant to ensure that the product meets the quality requirements.

Compliance matrix to DEVICE product assurance requirements

The DPAP shall include the compliance matrix to the applicable DEVICE product assurance requirements, or a reference to it.

1. For example ECSS-Q-ST-60-02 clauses, as tailored by a product assurance requirements document.

The compliance matrix shall include reference to the associated document where the requirement compliance evidence can be found.

* + 1. Special remarks

The response to this DRD may be combined with the response to the project product assurance report, as defined in ECSS-Q-ST-10.

1. (normative)  
   DEVICE Product Assurance Report (DPAR) - DRD
   1. DRD identification
      1. Requirement identification and source document

This DRD is called from ECSS-Q-ST-60-02requirement 5.2.2a

* + 1. Purpose and objective

The main purpose of the DEVICE product assurance report is to collect and present at project milestones the reporting on the DEVICE product assurance activities performed during the past project phases.

* 1. Expected response
     1. Scope and content

Introduction

The DPAR shall contain a definition of the purpose, objective, content and the reason prompting its preparation.

Applicable and reference documents

The DPAR shall list the applicable and reference documents to support the generation of the document.

Terms, definitions and abbreviated terms

The DPAR shall include any additional terms, definition or abbreviated terms used.

Verification activities performed

The DPAR shall contain reporting on verification activities performed by the product assurance function, including:

Reviews,

Inspections,

Walk-throughs,

Review of traceability matrices,

Documents reviewed.

The DPAR shall contain reporting on the verification of the measures applied for the handling of critical DEVICE.

Criticality Analysis Report

The DPAR shall report the result of the System level dependability and safety analysis, including the criticality(ies) assigned to the DEVICE

The DPAR shall report the result of the DEVICE dependability and safety analysis and identify recommendations for DEVICE and System.

Methods and tools

The DPAR shall include or reference a justification of the suitability of the methods and tools applied in all the activities of the development cycle, including requirements analysis, specification, design, coding, validation, testing, configuration management, verification and product assurance.

The DPAR shall include reporting on the correct use of methods and tools.

Compliance to design and coding standards

The DPAR shall include reporting on the compliance of DEVICE products to the applicable modelling, design and coding standards, including:

Reporting on the application of measures meant to ensure that the design complexity and modularity meet the quality requirements;

Reporting on design documentation . versus suitability for maintenance.

Compliance to security standards

The DPAR shall include reporting on the compliance of DEVICE security requirements, methods and tools.

Product and process metrics

The DPAR shall include reporting on the collected product and process metrics, the relevant analyses performed, the corrective actions undertaken and the status of these actions.

Testing and validation

The DPAR shall include reporting on adequacy of the testing and validation documentation, including feasibility, traceability repeatability, and on the achieved test coverage versus stated goals.

Deactivated, Configurable and Unreachable functions

The DPAR shall report on verification/validation activities performed on :

Deactivated functions,

Configurable functions,

Unreachable functions.

Automatic code generation

The DPAR shall include reporting on verification activities on automatically generated code.

Qualification

The DPAR shall include reporting on the assessment of qualification status and report its status.

The DPAR shall include reporting on assessment of maintenance of qualification status in case of change after achieving qualified state, including delta-qualification definition and results.

Independent Verification and Validation

The DPAR shall include reporting on the results of IVV activities.

The DPAR shall include references to IVV plans and reports as well status of open points with associated correction plan.

Process Assessment and Improvement

The DPAR shall include reporting on the results of process improvement.

The DPAR shall include reporting on Improvement planning and results.

Open points status

The DPAR shall include reporting on the status of problem reports , non-conformances, actions, RFDs and RFWs relevant to DEVICE.

The DPAR shall include the correction plan for all open points.

References to progress reports

Whenever relevant and up-to-date information has been already delivered as part of the regular PA progress reporting, a representative summary shall be provided, together with a detailed reference to the progress report(s) containing that information.

* + 1. Special remarks

The response to this DRD may be combined with the response to the project product assurance report, as defined in ECSS-Q-ST-10.

1. (normative)  
   DEVICE Reuse File (DRF) - DRD
   1. DRD identification
      1. Requirement identification and source document

This DRD is called from ECSS-Q-ST-60-02 requirement 6.2.3.1a.

* + 1. Purpose and objective

The main purpose of the DEVICE product assurance report is to collect and present at project milestones all information relevant to reuse of existing devices and devices intended for reuse..

* 1. Expected response
     1. Scope and content

Configuration management

The DRF shall include the detailed configuration status of the reused DEVICE baseline.

Reuse assessment

The DRF shall include the assessment of the existing DEVICE, including:

The assessment of the existing DEVICE applicable functional, performance and quality requirements,

The results of analysis of the existing DEVICE requirements and design,

Justification for any non-compliance between the applicable functional, performance and quality requirements and the actual characteristics/performances of the existing DEVICE,

Delta qualification activities defining all tasks to be performed to verify the fulfilment of the project requirements.

The DRF shall include the analysis of the suitability of existing DEVICE for reuse to be complemented by an assessment of the following:

DEVICE Suitability Report presenting the results of the Delta qualification activities,

The acceptance and warranty conditions,

The available support documentation,

The identification and registration by configuration management,

Maintenance responsibility and conditions, including the possibilities of changes,

The durability and validity of methods and tools used in the initial development, that are envisaged for use again,

The copyright and Intellectual Property Rights constraints, modification rights, distribution rights,

The licensing conditions,

Exportability constraints,

Identification of technology of the existing DEVICE, qualification heritage, flight heritage, company utilization of the technology.

Licensing scheme

The DRF shall include the assessment of deliverable DEVICE, including both developed DEVICE and existing reused DEVICE) in terms of constituent elements and the associated licensing.

* + 1. Special Remarks

None

1. (informative)  
   DEVICE Development Expected Outputs

Various types of outputs are expected to be produced during the course of the development of a DEVICE and its different phases. Table D-1 is a summary of all the document outputs expected at each review milestone for both, the engineering and the product assurance flows, as explained in ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 respectively. Table D-1 can also be found in ECSS-E-ST-20-40 Annex K.

: ECSS-Q-ST-60-02 list of Expected Outputs

| Document name | Document having a DRD annex | DEVICE Definition Phase Review  (DPR) | DEVICE Architecture Definition Phase Review  (ADPR) | DEVICE Design and Verification Phase Review  (DVPR) | DEVICE Detailed Design Phase Review  (DDPR) | DEVICE Layout Phase Review  (LPR) | DEVICE Validation, Acceptance and Maintenance Phase Review  (VAMP) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DEVICE Requirements Specification (DRS) | ECSS-E-ST-20-40  Annex A | R |  |  |  |  |  |
| DEVICE Development Plan (DDP) | ECSS-E-ST-20-40  Annex B | R |  |  |  |  |  |
| DEVICE Verification Plan (DVeP) | ECSS-E-ST-20-40  Annex C | R | R | R | R |  |  |
| DEVICE Validation Plan (DVaP) | ECSS-E-ST-20-40  Annex D | R | R |  |  | R |  |
| DEVICE Support and Maintenance Plan (DSMP) (conditional) | ECSS-E-ST-20-40  Annex E | R |  |  |  |  | R |
| Feasibility and Risk Assessment Report (FRAR) | ECSS-E-ST-20-40  Annex F | R | R | R | R | R | R |
| DEVICE Product Assurance Plan (DPAP) | ECSS-Q-ST-60-02 Annex A | B |  |  |  |  |  |
| DEVICE Product Assurance Report (DPAR) | ECSS-Q-ST-60-02 Annex B | R | R | R | R | R | R |
| DEVICE Reuse File (DRF) | ECSS-Q-ST-60-02 Annex C | R | R | R | R | R | R |
| Verification Control Document (VCD) | ECSS-E-ST-10-02 Annex B | R | R | R | R | R | B |
| Independent Verification Validation Plan (IVV Plan) |  | B |  |  |  |  |  |
| Configuration Management Plan (CMP) | ECSS-M-ST-40 Annex A | B |  |  |  |  |  |
| Configuration Item Data List (CIDL) | ECSS-M-ST-40 Annex C | B |  |  |  |  |  |
| Architecture Definition Report | ECSS-E-ST-20-40  Annex G |  | R |  |  |  |  |
| DEVICE Design Report |  |  |  | R |  |  |  |
| Design Verification Report |  |  |  | R |  |  |  |
| DEVICE Data Sheet (conditional) | ECSS-E-ST-20-40  Annex H |  |  | R | R | R | R |
| Netlist Generation Report |  |  |  |  | R |  |  |
| Netlist Verification Report |  |  |  |  | R |  |  |
| Layout Generation Report |  |  |  |  |  | R |  |
| Layout Verification Report |  |  |  |  |  | R |  |
| Radiation Test Plan (conditional) |  |  |  |  |  | R |  |
| ESCC Detail Specification (conditional) |  |  |  |  |  | R | R |
| ASIC Production Tests Report  or  FPGA Programming Test Report |  |  |  |  |  |  | R |
| DEVICE Validation report |  |  |  |  |  |  | R |
| Radiation Test Report (conditional) |  |  |  |  |  |  | R |
| DEVICE User Manual (conditional) |  |  |  |  |  |  | R |
| Experience Summary Report (conditional) | ECSS-E-ST-20-40  Annex I |  |  |  |  |  | R |
| As-Built Configuration List (ABCL) | ECSS-M-ST-40 Annex D |  | R | R | B | R | B |
| Software Configuration File (SCF) | ECSS-M-ST-40 Annex E |  | R | R | R | R | B |
| Independent Verification Validation Report (IVV Report) |  |  | R | R | R | R | B |
| End Item Data Pack (EIDP) | ECSS-Q-ST-20 Annex B |  |  |  |  |  | B |
| The following notation is used:  B = Configuration Baseline (as per ECSS-M-ST-40 clause 4.3.2.4)  R = Review | | | | | | | |

1. (informative)  
   Traceability from ECSS-Q-ST-60-02C to ECSS-Q-ST-60-02C Rev1
   1. Traceability from ECSS-Q-ST-60-02C to ECSS-Q-ST-60-02C Rev.1

Table E-1 presents the traceability from Issue C to Issue C Revision 1 of ECSS-Q-ST-60-02. Whereas Table E-2 presents the information from Revision 1 to Issue C.

: ECSS-Q-ST-60-02C to ECSS-Q-ST-60-02C Rev.1

| ECSS-Q-ST-60-02C | Original requirement | ECSS-Q-ST-60-02C Rev.1 |
| --- | --- | --- |
| 4.1.1a | The supplier shall establish and implement an ASIC and FPGA development, as part of the component programme (in conformance with ECSS-Q-ST-60), that ensures full conformance with the requirements of the project as defined by the customer in line with this standard. |  |
| 4.1.2a | The supplier shall establish and maintain an organization for the management of the ASIC and FPGA programme. |  |
| 4.1.2b | The organization shall comply with the requirements specified in ECSS-Q-ST-10. | 5.1, 5.3, 5.4,5.5 |
| 4.1.2c | In case of major problems, the development team, as allocated in the development plan (see 4.3.1), shall directly report to the component advisory board as defined in ECSS-Q-ST-60. |  |
| 4.1.3a | The supplier shall ensure that:     1. the ASIC and FPGA developments that are necessary for the implementation of the ASIC and FPGA programme are planned, documented and implemented, and      2. preventive or corrective actions are initiated whenever there is evidence of possible schedule or technical problems. |  |
| 4.2a | The supplier shall prepare an ASIC and FPGA control plan (ACP) in conformance with the DRD in Annex A. |  |
| 4.3.1a | The supplier shall prepare a detailed ASIC and FPGA development plan (ADP) in conformance with the DRD in Annex B. |  |
| 4.3.1b | The supplier shall maintain the ADP after the requirements are settled and the feasibility and risk for the ASIC and FPGA development is assessed. |  |
| 4.3.2a | The supplier shall establish a verification plan in conformance with the DRD in Annex E. |  |
| 4.3.2b | The verification plan shall define how the functionality and non-functional requirements stated in the definition phase documentation are demonstrated at all levels of modelling. |  |
| 4.3.3a | The supplier shall establish a design validation plan (DVP) in conformance with the DRD in Annex F. |  |
| 4.3.3b | The DVP shall specify the measurements performed on the prototypes.     NOTE Those measurements allow verifying that the implemented devices contain the functionality and the characteristics they are designed for. |  |
| 4.4a | At the end of the ASIC and FPGA development cycle, the supplier should establish an experience summary report in conformance with the DRD in Annex I.     NOTE The experience summary report can be written in the frame of the supplier’s continued quality improvement activities in order to establish economic and efficient development and test requirements for expected future projects. |  |
| 5.2a | The ASIC and FPGA development flow shall be in conformance with ECSS-M-ST-10.  NOTE Figure 5-1 gives an example of the ASIC and FPGA development flow, adapted from ECSS-M-ST-10. |  |
| 5.2b | All inputs to the design, that are not automatically generated and are necessary to reproduce the design shall be put under a revision control mechanism agreed between the contractors;     NOTE Examples are simulation pattern, schematics, VHDL source codes, synthesis scripts. |  |
| 5.2c | Each development step using design inputs shall reflect the revision numbers of the inputs in a log file to prove consistency; |  |
| 5.2d | Each development step shall be verified by a mechanism, as impartial as possible, to guarantee successful completion of the development step.      NOTE The development step is completed when the steps itself as well as its verification were performed and any error or serious warning being flagged by the tools was approved in the corresponding review meeting. |  |
| 5.3.2a | The supplier shall ensure that all relevant system configurations and characteristics and all issues imposing requirements on the device are used.      NOTE This allows settling out without any ambiguity the definition status of the collected requirements and verifying that all necessary resources for the design activities are available. |  |
| 5.3.2b | The supplier shall specify the complete set of traceable ASIC and FPGA requirements in the ASIC and FPGA requirements specification (ARS) in conformance with the DRD in Annex C. |  |
| 5.3.3.1a | The feasibility of the intended ASIC and FPGA development shall be assessed against the established ASIC and FPGA requirements specification and the available resources. |  |
| 5.3.3.1b | As a minimum, the following tasks shall be performed and documented:     1. Estimate design complexity;     2. Estimate power consumption;     3. Assess feasibility of speed requirements by a preliminary timing analysis;     4. Select a radiation hardening approach that ensures compliance with radiation tolerance requirements. Determine a rough estimate of impact on chip area and circuit speed;     5. Select a production test approach and its feasibility against all requirements;     6. Identify and evaluate the suitability and qualification status of the ASIC technologies or FPGA available to implement the device, fulfilling all functional and non-functional requirements including the specified derating factors. Make a baseline selection;     7. Identify packages, fulfilling all requirements. Make a baseline selection;     8. Ensure that the baseline technology and package or FPGA have a remaining lifetime, so that flight and compatible prototype parts can be manufactured and are available during the expected procurement phase(s);     9. Ensure that technical support for the device can be guaranteed during the expected lifetime;     10. Determine availability and status of the required design and test tools (H/W & S/W) and libraries;     11. Determine availability of the necessary human resources;     12. Determine availability, licensing, support, legal and economical aspects of using IP cores from third parties;     13. Ensure that no patents are infringed or agreements exist or can be made with the patent holder. |  |
| 5.3.3.2a | As a tool of the quality assurance system (see clause 6.3) a risk analysis shall be performed that identifies potential risk items and assigns preventive measures and contingency plans. | 5.3 |
| 5.3.3.2b | The risk analysis shall result in a Feasibility and risk analysis (FRA) report in conformance with the DRD in Annex D. |  |
| 5.3.4a | The ADP shall ensure prospective design portability for devices with long term availability or multiple usage requirements. |  |
| 5.3.5a | The definition phase shall be concluded by a system requirements review (SRR) meeting (see quality assurance clause 6.2). |  |
| 5.3.5b | The documentation generated within this phase shall be reviewed. |  |
| 5.3.5c | The reviewers shall check that the development activity as defined in the ADP is feasible within the limits imposed by the project requirements, resources, schedule and budgetary constraints. |  |
| 5.3.5d | The reviewers shall check that contingency plans exist for all identified open issues and risk items and that the risk analysed can be taken for starting the Architectural Design phase. |  |
| 5.3.5e | The reviewers shall check that ARS and FRA are complete and documented in a level of detail that avoid any ambiguity for the Architectural Design and all subsequent design work. |  |
| 5.3.5f | The reviewers shall check that ARS and FRA include as a minimum:  1. Summary of the system architecture and all expected configurations in which the device can be used;  2. Specify the external devices connected to the chip and their interface protocols;  3. Bit numbering and naming convention ( maintained throughout the design flow);  4. Format of data structures;  5. Functionality in all nominal operational modes;  6. Functionality for error handling;  7. Functionality in all system test modes;  8. Internal communication protocols;  9. Signal processing algorithms;  10. Definitions of programmable memory elements and their state after reset;  11. Functional partitioning, establishing a high-level block diagram;  12. Preliminary architectural and hardware/software partitioning, including external and internal memory mapping;  13. For components providing software programmability, associated software requirements specifications ;  14. State and behaviour of l/Os during and after reset and power-up;  15. State functions explicitly not implemented in the design, in order to avoid potential misunderstandings;  16. Pin list including power supply, test pins, if already known, name, polarity, bus width and interface protocol;  17. Electrical specifications (maximum ratings, AC, DC and timing diagrams);  18. Power dissipation estimates for main functional modes;  19. Operating conditions (supply, temperature, radiation);  20. Baseline package and pin-out, if already known. |  |
| 5.4.1a | During the architectural design phase, the architecture of the chip shall be defined, verified and documented down to the level of basic blocks implementing all intended functions, their interfaces and interactions. |  |
| 5.4.1b | Important selections for the implementation of the chip shall be made or confirmed. |  |
| 5.4.1c | All definitions and selections made shall conform to the definition phase documentation. |  |
| 5.4.1d | Any deviation shall be justified in the preliminary design review. |  |
| 5.4.1e | The architecture definition and the baseline choices made during the definition phase shall be settled, frozen and documented with a level of detail that allows proceeding with the subsequent detailed design. |  |
| 5.4.2a | As a minimum the following tasks shall be performed and documented in an architecture definition report:     1. Subdivide the chip into its fundamental functions or blocks, identifying and thoroughly documenting their interfaces, functionalities and interactions;     2. Define the architecture down to the level required to implement technology specific, transistor- or gate-level mapping;     3. Select suitable algorithms and circuit schemes including their parameters to implement the identified functions;     4. Identify sub-functions, which can be used as an individual block at different locations of the chip or possibly be compiled as a core for other designs;     5. Identify a suitable clocking and reset scheme assuring correct transitions of data between clock domains and identify asynchronous parts of the design;     6. Select (if not yet done), IP-cores used or previously designed units re-used in the design. Procure and verify them.          NOTE This verification can be done by test cases provided by the IP core manufacturer, by test benches from an independent source, or by newly designed test programs.     7. If the verification is accomplished during prior instantiations of the core, assess it for covering the actual system environment, and eventually perform bug-fixes and workarounds or additional verification;     8. Identify and eventually procure custom cells, used in the design, verify the consistency of the different models delivered (e.g. simulation models, layout and timing view);     9. Generate models required as an input to the subsequent detailed design phase (e.g. synthesizable RTL models);         NOTE There is no firm requirement for intermediate behavioural simulations, nor for any model being coded in a particular language or a specific level of abstraction. However, the coding of behavioural models of critical functions and algorithms is strongly encouraged, since they frequently are valuable tools for further verification tasks. | Re-use -6.2.3 |
| 5.4.2b | The architecture definition report shall include the architecture broken down to the selected blocks, their interfaces, functionality or algorithms and interactions. |  |
| 5.4.2c | Even though the chip and its architecture is completely described in a simulation model (executable specification), a detailed text specification shall be edited. |  |
| 5.4.3a | The supplier shall establish a verification plan in conformance with the DRD in Annex E. |  |
| 5.4.4a | As a minimum, the following activities shall be performed and documented in an architecture verification and optimization report:     1. Verify that the defined architecture meets the requirements by appropriate simulation and analysis techniques;     2. Verify that the models referred to in clause 5.4.2a.9 above are compliant to the verification plan;     3. Perform an independent verification in order to avoid masking of design errors;     4. When allocation and connectivity of hard-macro cells can be an issue, a preliminary floorplan, assure that the expected cells are effectively place- and routable within the given constraints;          NOTE This is not applicable for FPGA designs.     5. Re-assess the feasibility and risks;     6. Find an application related trade-off for conflicting requirements;         NOTE For example: power consumption vs. speed and performance, pin count vs. package size and complexity vs. die area.      7. Establish the implementation choices. |  |
| 5.4.5a | A preliminary data sheet shall be established in conformance with the DRD in Annex G.     NOTE The preliminary data sheet is updated and completed at the end of the ASIC and FPGA development. |  |
| 5.4.6a | The architectural design phase shall be concluded by the preliminary design review (PDR) meeting (see quality assurance clause 6.2). |  |
| 5.4.6b | The documentation generated within this phase shall be reviewed. |  |
| 5.4.6c | The reviewers shall check that the selected trade-off meets the requirements fixed during the definition phase. |  |
| 5.4.6d | The reviewers shall check that preventive measures or contingency plans exist for all identified risk items and that the risk analysed can be taken for starting the detailed design. |  |
| 5.4.6e | The reviewers shall check that the architectural design documentation (see clause 7.3.4) together with the documentation of previous development phases is complete, traceable and documented in a level of detail that allow to proceed with the detailed design. |  |
| 5.4.6f | The reviewers shall identify, justify and approve discrepancies between the architectural design documentation and the definition phase documentation. |  |
| 5.4.6g | The reviewers shall check that the planned measures, tools, methods and procedures are applied. | 5.5 |
| 5.5.2a | Influences from layout such as cross talk and matching shall be accounted for during the design work. |  |
| 5.5.2b | For analog designs circuit and layout are developed concurrently, and the reviews for detailed design and layout phases may be held together. |  |
| 5.5.2c | For FPGAs and analog designs, a combined DDR and CDR meeting may be justified.      NOTE In these cases also the corresponding output reports can be merged together. |  |
| 5.5.2d | The scripts used for an automatic and repeatable generation shall be part of the design database.     NOTE 1 The main output of the detailed design is a design database, which contains, or allows an automatic and repeatable generation of the above-mentioned inputs to the layout.     NOTE 2 The scripts defined for this generation are an essential part of the detailed design, |  |
| 5.5.3a | During the design entry the following tasks shall be performed and documented in a design entry report. |  |
| 5.5.3b | Use the agreed design tools as specified in the ADP (see clause 5.3.4). Check their maintenance status. Consider known bugs, existing patches, preventive and workaround measures. | 5.5 |
| 5.5.3c | Implement the specified test concept during design entry and synthesis (e.g. scan paths, DFT logic, measurement points, test busses and boundary scan (JTAG, see IEEE 1149.1). |  |
| 5.5.3d | Implement the specified radiation hardening concept by design and during synthesis. |  |
| 5.5.3e | Continuously verify the results by the appropriate methods, as specified in the verification plan. |  |
| 5.5.3f | Determine a pin-out and bonding scheme with particular attention to the technical constraints.      NOTE For example, power supply pin definition and bondability issues. |  |
| 5.5.3g | Select buffers according to the I/O requirements defined in the ASIC and FPGA requirements specification. |  |
| 5.5.3h | Establish or refine the floorplan.     NOTE This is not applicable for FPGA designs. |  |
| 5.5.4a | Enough iterations between design entry, netlist and layout generation shall be performed in order to accomplish the design requirements. |  |
| 5.5.4b | Iterations back to the architectural design shall be avoided. |  |
| 5.5.4c | If an iteration back to the architectural design is required by means of changes in the model released during the PDR, that model shall be verified again. |  |
| 5.5.4d | As a minimum the following tasks shall be performed and documented in a netlist generation report:     1. Consider the required derating factors;     2. Ensure that the appropriate library cells are used as to fulfil all the requirements collected in the ASIC and FPGA requirements specification;     3. Select or generate appropriate models for parasitism (e.g. wire load models);         NOTE This is not applicable for FPGA designs.     4. Perform a design parameter centring;          NOTE This is only applicable for analog ASIC designs.     5. Ensure that the intended operating (process, voltage, temperature) and environment (radiation) conditions are used during the translation and verification exercise;     6. If synthesis tools are used, generate scripts which allow performing the fully automatic pre-layout netlist generation in a repeatable way;      7. Ensure that these scripts, being part of the inputs to the design, are compliant to the general requirements for e.g. documentation, commenting and version control;     8. Specify timing constraints, and supplier or manufacturer-specific design rules;     9. Consider over-constraining to anticipate parasitic effects. |  |
| 5.5.5a | As a minimum the following tasks shall be performed and documented in a netlist verification report:     1. Verify the netlist according to the verification plan;     2. Verify the estimated data for the layout parasitics and delays;     3. Perform gate level simulations, using the complete test suite from the architectural design, or an equivalent set of methods, such as formal verification and static timing analysis;         NOTE This is not applicable for analog ASIC designs.     4. Verify key parameters, such as bias voltages, operating point, frequencies, bandwidth, matching, s-parameters, noise, dynamic and linear ranges and shaping times;      5. Perform a functional verification, including the interfaces.          NOTE This is only applicable for analog ASIC designs.     6. If a complete simulation of all modes (including test modes) at top level cannot be performed (e.g. due to run-time restrictions), simulate a representative subset;      7. Verify by an extrapolating analysis, the not simulated cases;     8. Verify that the specified test concept is implemented through e.g. scan paths, DFT logic, measurement points and test busses;     9. Verify that the radiation-hardening concept is successfully included in the netlist. Consider e.g. netlist inspection and SEU injection simulations;     10. Verify that the specified power consumption is respected;     11. Update relevant parameters in the preliminary data sheet according to the results obtained during the verification;     12. If production tests or a pre- and post burn-in test are planned, generate the test vectors and verify the requirements for fault coverage;     13. For IP cores and macro cells: include the core's test patterns in the overall ASIC's test programmes;     14. Verify, that the pre-layout supplier or manufacturer design rules are met and assess the relevance of violations;          NOTE This is not applicable for FPGA designs.     15. Perform a parameter sensitivity analysis;          NOTE This is only applicable for analog ASIC designs. |  |
| 5.5.6a | The supplier shall update the data sheet to incorporate the new established information on for instance pinout and estimated timing.      NOTE For further details see Annex G. |  |
| 5.5.7a | The detailed design phase shall be concluded by the detailed design review (DDR) meeting (see clause 6.2). |  |
| 5.5.7b | The documentation generated within this phase shall be reviewed. |  |
| 5.5.7c | The reviewers shall verify that the detailed design documentation (see clause 7.3.5) together with the documentation of previous development phases completely documents all results obtained and decisions made along with the corresponding justifications in a level of detail that allow to proceed with the layout. |  |
| 5.5.7d | This verification shall include as a minimum:     1. Circuit implementation shows details of the implementation, which were not specified during architectural design;     2. Description of implemented testability and production test methods including the achieved fault coverage figures obtained;     3. Description of implemented radiation hardening measures;     4. All verification results;     5. Description of cells specially developed for the design;     6. Configuration and modifications applied to IP cores used in the design;     7. List of items with name and format provided to the foundry (i.e. netlist, stimuli files for production test and constraints files);          NOTE This is not applicable for FPGA designs.     8. Description of the design database, including the file structure, naming conventions, version control labels, netlist generation methods and constraints;     9. All tools and ASIC libraries actually used during the entire design development, including the versions and operating platforms used;     10. Problems encountered with design tools and their workarounds. | paragraph 9 -> 5.5, 8.1 |
| 5.5.7e | The reviewers shall check that the planned measures, tools, methods and procedures were applied; | 5.5; 5.2.1 |
| 5.5.7f | The reviewers shall check that the outputs are in conformance to the requirements fixed during the definition phase; |  |
| 5.5.7g | In particular, when the layout is performed by another company (foundry), the reviewers shall assess the specific foundry requirements (netlist sign-off criteria). |  |
| 5.6.1a | The layout shall generate the placement and routing information to meet the design rules, timing and other constraints. |  |
| 5.6.1b | In addition, netlist optimization by local re-synthesis or physical synthesis shall be applied.     NOTE This provides reliable information about loads and coupling capacitors and the final design rule check that assures a verified netlist which can be forwarded to the foundry. |  |
| 5.6.2a | As a minimum the following tasks shall be performed and documented in a layout generation report:     1. finalize the floorplan of the chip;          NOTE This is not applicable for FPGA designs.     2. perform place and route (P&R) taking into account all layout constraints;     3. perform netlist optimizations (see clause 5.6.1) for timing and design rules if necessary;          NOTE This is only applicable for digital ASIC designs.     4. generate the power distribution;     5. generate the clock distribution (clock tree and buffers);          NOTE This is not applicable for analog ASIC designs.     6. insert core and pad ring power distribution and possibly additional test pads in the circuit;     7. determine the die size;          NOTE This is not applicable for FPGA designs.     8. generate the bonding diagram respecting bonding and package constraints;          NOTE This is not applicable for FPGA designs.     9. generate the input data for mask or programming file generation (IDMP). |  |
| 5.6.3a | As a minimum the following tasks shall be performed and documented in a layout verification report:     1. layout design rule check (DRC);     2. electrical rule check (ERC), check cross-talk sensitivity, if required by customer;     3. extract a netlist from the layout given in terms of IDMP;     4. verify that the gate-level netlist is consistent with the layout by performing a layout versus schematic (LVS) comparison, i.e. a netlist comparison check (NCC) between the post-layout netlist and the layout (IDMP) extracted netlist;     5. verify that the post-layout netlist is consistent in terms of functionality with the pre-layout netlist by simulation and formal methods;     6. extract the parasitic information;         NOTE This delivers capacitance, resistance and inductivity values (only deep sub-micron technology), from which the actual delays are calculated for digital designs.     7. perform comprehensive post-layout verification according to the verification plan;         NOTE This is mostly accomplished by back-annotated simulations and timing analysis     8. check the resulting clock skew and latency;          NOTE This is not applicable for FPGA designs.     9. check relevant timing of I/Os;      10. check the power distribution on the chip;          NOTE This is not applicable for FPGA designs.     11. perform transition check and load check on the nets inside the ASIC;     12. characterize ASIC and FPGA timing performances,          NOTE For example: max clock frequency, clock duty cycle, set-up and hold times for all inputs and propagation delays for all outputs. |  |
| 5.6.4a | The supplier shall establish and maintain a design validation plan (DVP) in conformance with the DRD in Annex F. |  |
| 5.6.5a | The supplier shall update the parameters in the data sheet according to the results obtained during the layout verification.      NOTE For further details see Annex G. |  |
| 5.6.6a | Based on the information collected in the design documentation a draft detail specification shall be established in conformance with the DRD in Annex H. |  |
| 5.6.7a | The layout phase shall be concluded by the critical design review (CDR) meeting (see 6.2). |  |
| 5.6.7b | The documentation generated within this phase shall be reviewed. |  |
| 5.6.7c | The layout documentation (see 7.3.6) together with the documentation of previous development phases completely documents the progress and decisions made during the layout shall be checked. |  |
| 5.6.7d | As a minimum, the review of the documentation at CDR shall address:     1. Post-layout clock distribution tree and clock skew and latency analysis;     2. Post-layout verification results and analysis of timing margins;     3. Results from all layout checks (e.g., DRC, ERC, LVS and NCC) Any violation of or deviations from the design rules and justifications. |  |
| 5.6.7e | The reviewers shall check that the planned measures, tools, methods and procedures have been applied. |  |
| 5.6.7f | The reviewers shall check that the outputs are in conformance to the requirements fixed during the definition phase. |  |
| 5.6.7g | In the case where no DDR was held after the detailed design phase, the reviewers shall check that the CDR encompasses also all review items of the DDR. |  |
| 5.6.7h | The reviewers shall check that preventive measures or contingency plans exist for all identified risk items and that the risk analysed can be taken for starting the Prototype Implementation. |  |
| 5.7.2a | As a minimum, the following tasks as described in 5.7.2b up to 5.7.2j shall be performed and documented in the production test report. |  |
| 5.7.2b | The package shall be the same as for flight devices, if required by the customer. |  |
| 5.7.2c | The mask generation and verification shall be performed under the foundry's configuration control system.     NOTE This is not applicable for FPGA designs. |  |
| 5.7.2d | The committed number of prototypes shall be produced and delivered, so that design validation can be performed. |  |
| 5.7.2e | The production test shall be performed on 100 % of the delivered prototypes, using the test vectors generated during the previous phases. |  |
| 5.7.2f | The production test shall demonstrate that the device was produced correctly.      NOTE This is not applicable for FPGA designs. |  |
| 5.7.2g | The correctness of the FPGA programming shall be verified (checksum test).      NOTE This is only applicable for FPGA designs. |  |
| 5.7.2h | The tested parameters and conditions shall be according to the draft detail specification (see clause 7.4.3). |  |
| 5.7.2i | Test reports shall be generated and delivered, documenting the measured parameters. |  |
| 5.7.2j | Tester log files shall be delivered in electronic format. |  |
| 5.8.1a | The design validation shall be performed to confirm the achievement of all functional, performance, interface and compatibility requirements. |  |
| 5.8.1b | As a minimum, the following tasks shall be performed and documented in a validation report:     1. carry out the validation according the established validation plan;     2. design and build the test set-up or system breadboard in order to represent a realistic system application;     3. use the breadboard to perform validation tests that cover full functionality and all operating modes and conditions of the device;     4. specify, design and execute specific burn-in or other screening tests for the later test of the FM parts; if agreed by the business agreement;     5. document scope, sequences, set-up and results of the validation tests in the validation report;          NOTE The validation report becomes part of the design validation documentation.      6. Compare specified parameters with measured parameters. |  |
| 5.8.1c | The validation report shall be made available to the foundry and the design house. |  |
| 5.8.2a | The device prototypes shall undergo radiation testing according to the requirements of the project, if the required hardening level is not yet demonstrated for the technology involved. |  |
| 5.8.2b | Radiation testing shall be performed according to the established radiation verification plan included in the design validation plan and documented in a radiation test report. |  |
| 5.8.3a | For the design release and FM production preparation, the tasks, as described in 5.8.3b to 5.8.3h, shall be performed and documented in the release report. |  |
| 5.8.3b | License agreements for the intellectual property (the design itself and third party IP cores) contained in the device shall be established to cover the whole lifetime. |  |
| 5.8.3c | The supplier shall ensure technical support of the device during the lifetime of the product. |  |
| 5.8.3d | This can be accomplished through a know-how transfer from the design house to the foundry or a third party, or by the design house itself. |  |
| 5.8.3e | The suppler shall ensure the storage of the complete design database during the lifetime of the product, including associated data, documentation, pattern generation files, test program(s) and mask sets used. |  |
| 5.8.3f | In the case of using non-QML manufacturer or foundry, an evaluation programme (in conformance with ECSS-Q-ST-60) shall be performed that include as agreed by the customer the following activities:     1. manufacturer evaluation;     2. constructional analysis;     3. evaluation testing. |  |
| 5.8.3g | On completion of the evaluation programme additional data such as reliability and radiation data shall be available ensuring that the mission requirements can be met. |  |
| 5.8.3h | The supplier shall assess the risk involved for the FM production. |  |
| 5.8.4a | The executive summary report shall be completed in conformance with the DRD in Annex I. |  |
| 5.8.5a | The detail specification, in conformance with Annex H shall be updated based on the validation test results. |  |
| 5.8.5b | If requested by the customer, the data sheet, in conformance with Annex G shall be updated based on the validation test results. |  |
| 5.8.5c | The data sheet, eventually transformed to the foundry specific format, shall be available during the device lifetime. |  |
| 5.8.5d | An application note (see clause 7.4.2) shall be established. |  |
| 5.8.6a | The design validation phase shall be concluded by the qualification and acceptance review (QR/AR) meeting (see clause 6.2). |  |
| 5.8.6b | The documentation generated within this phase shall be reviewed. |  |
| 5.8.6c | The reviewer shall check that the design validation documentation (see clause 7.3.6) together with the documentation of previous development phases is complete. |  |
| 5.8.6d | The reviewer shall check that the device achieves functional, performance, interface and compatibility characteristics satisfying the ASIC and FPGA requirements specification. |  |
| 5.8.6e | The reviewer shall check that the planned measures, tools, methods and procedures were applied. |  |
| 5.8.6f | The reviewer shall check that preventive measures or contingency plans exist for all identified risk items and that the risk of FM production can be taken. |  |
| 6.1a | ECSS-Q-ST-20 clause “QA status reporting” shall apply. | 5.2.2, Annex B |
| 6.1b | ECSS-Q-ST-30 clause “criticality classification of functions and products” shall apply. | 6.2.1, 9 |
| 6.1c | ECSS-Q-ST-60 clauses 4.5, 5.5 and 6.5 (components quality assurance) shall apply. | 7 |
| 6.1d | The objective of the quality assurance system is to ensure the development of reliable, manufacturable, testable and reproducible, custom designed components for space application. | All |
| 6.1e | The tools used shall be specified and approved by the customer. |  |
| 6.1f | All technology independent CAD tools employed during the development shall be mature and fit for their purpose. |  |
| 6.1g | All technology dependent CAD tools shall be used as approved and supported by the selected manufacturer. |  |
| 6.1h | Preference shall be given to the use of established international standards, such as VHDL as defined in IEEE 61691-1-1 and EDIF. |  |
| 6.2a | The supplier shall schedule and conduct design reviews in conformance with ECSS-M-ST-10-01. |  |
| 6.2b | Design reviews shall be defined along with the criteria for their successful completion in the ASIC and FPGA development plan (see clause 5.3.4). |  |
| 6.2c | Representation, for design and quality assurance, from all relevant organizations (customer, system supplier, design house and foundry) shall be ensured. |  |
| 6.2d | The supplier shall produce and circulate in advance of each design review a design review package containing a checklist based on the established requirements and the data necessary for the particular review. |  |
| 6.2e | The following reviews shall be performed:     1. System requirements review (SRR)         NOTE This review results in the authorization to start the architectural design. The outputs reviewed and the items checked are detailed in clause 5.3.5.     2. Preliminary design review (PDR)         NOTE PDR results in the authorization to start with the detailed design. The outputs reviewed and the items checked are detailed in clause 5.4.6.     3. Detailed design review (DDR) (if applicable)         NOTE 1 DDR results in the authorization to proceed with the layout. The outputs reviewed and the items checked are detailed in clause 5.5.7         NOTE 2 In the case the design and layout is a concurrent or interdigitated activity (for instance analog or FPGA design) this review meeting can be combined with the subsequent CDR meeting.     4. Critical design review (CDR)         NOTE CDR results in the approval of design and layout and the release for prototype implementation. The outputs reviewed and the items checked are detailed in clause 5.6.7.      5. Qualification and acceptance review (QR/AR)         NOTE QR/AR results in the final acceptance of the design and the release for FM production. The outputs reviewed and the items checked are detailed in clause 5.8.6.      6. Additional design reviews as agreed by the supplier. |  |
| 6.2f | Direct or delegated customer participation and under the responsibility of the supplier, manufacturer or foundry participation for CDR and QR/AR shall be mandatory.     NOTE 1 The decision on a successful completion of a review meeting can only be achieved by consent of all parties.      NOTE 2 A review identifying a limited number of only minor discrepancies can be completed after successful implementation of the corrective actions defined during the review. |  |
| 6.2g | A review failing major acceptance criteria and resulting in a design iteration shall be repeated in full. |  |
| 6.2h | The criteria for a successful review meeting shall be defined prior to the relevant meeting.      NOTE These criteria can be defined on the preceding review meeting. |  |
| 6.2i | All review meetings shall be minuted. |  |
| 6.2j | The MoMs of the review meetings shall be added to the management documentation. |  |
| 6.3a | The design risk for the timely and successful completion of the development activity shall be assessed according to the items listed in clause 5.3.3.2. |  |
| 6.3b | Risk assessment shall be performed concurrently to the design activity. |  |
| 6.3c | Extraordinary risks shall be covered by a contingency plan identifying alternative or back-up solutions. |  |
| 6.3d | A check of the risk mitigation activities shall be a major item of the agenda of every review meeting. |  |
| 7.1a | At all stages of the ASIC and FPGA development, the supplier shall produce, maintain, control and archive all related documentation as defined and detailed in the following clauses. |  |
| 7.1b | The documentation shall be well structured and easily readable, so that the design can be understood by other ASIC and FPGA designers of the supplier and manufacturer not permanently involved in the design work.      NOTE For example, names of signals and blocks are chosen to indicate their function. |  |
| 7.1c | One consistent language shall be used throughout the documentation, preferably English. |  |
| 7.1d | The documentation shall be consistent, e.g. the same item have the same name in all documentation. |  |
| 7.1e | Block diagrams, control flow charts, timing diagrams and other figures shall be introduced where beneficial for the understanding of the text. |  |
| 7.1f | Every time an updated document is delivered, it shall include a detailed change list, and all significant changes marked using a change bar in the margin. |  |
| 7.1g | If a document is delivered before being complete, each page with incomplete information shall be clearly marked.      NOTE Some of the information listed is better delivered separately or in appendices, such as layout plots, gate-level schematics and lists of undetected faults. |  |
| 7.1h | All documents shall be archived for a minimum period of five years after completion of the development activity or as agreed by the customer. |  |
| 7.2a | The management documentation shall provide the overall strategy for the development activity including task planning and organization and approaches, methods and applicable procedures.      NOTE The management documentation also includes the status reporting as MoM of the review meetings and an assessment of the experience gained during the development activity. The management documentation is a gathering of separate documents (see clauses 4.2a, 4.4a, 4.3.2a and 4.3.3a). |  |
| 7.3.1.2a | All design information shall be stored in a design database by applying the revision control mechanism agreed in the business agreement (see clause 5.1). |  |
| 7.3.1.2b | All intermediate design data shall be reproducible to assist possible iterations. |  |
| 7.3.1.2c | As the design database consists of electronic data that cannot be reviewed directly, formless reports shall be established that contain a legible extract of the database. |  |
| 7.3.1.2d | Reports that shall be produced during the individual phases of a development activity are detailed in clause 5.     NOTE 1 An example of a suitable filing of this design documentation is given in Figure 7-1     NOTE 2 In the case the design and layout is a concurrent or interdigitated activity (e.g. analog and FPGA design) the corresponding output reports can be merged together. |  |
| 7.3.2a | The definition phase documentation shall consist of the following contributions:     1. The ASIC and FPGA requirements specification (ARS) established during the first development phase.     2. ARS including a complete set of ASIC and FPGA requirements, in conformance with the DRD in Annex C that are settled, unambiguous and frozen.     3. An assessment of the feasibility and risk analysis (FRA) with regards to the following drivers:          (a) consistency and quality of the ASIC and FPGA,          (b) system requirements feasibility of the ASIC and FPGA development,         (c) estimate of the risk involved.              NOTE The feasibility and risk analysis (FRA) report is the second part of the definition phase documentation. |  |
| 7.3.2b | FRA shall cover the items detailed in clause 5.3.3. |  |
| 7.3.3a | The architectural design documentation shall include the following contributions to the definition phase documentation:     1. The architectural definition report that includes the architecture broken down to the selected blocks, their interfaces, functionality, algorithms and interactions as specified in clause 5.4.2.     2. The verification and optimization report that provides the simulations performed, the results received, the trade-offs found and the implementation choices established.          NOTE Further details are given in clause 5.4.4. |  |
| 7.3.4a | The detailed design documentation shall consist of the following contributions to the architectural design documentation:     1. The design entry report providing all inputs available for the detailed design phase as detailed in clause 5.5.3.     2. The netlist generation report describing the work performed and the decisions taken to generate a netlist as detailed in clause 5.5.4.     3. The netlist verification report listing all steps of simulation and verification performed (see clause 5.5.5) together with the corresponding results. |  |
| 7.3.5a | The layout documentation shall consist of the following contributions to the detailed design documentation:     1. The layout generation report describing the work performed and the decisions taken to generate layout as detailed in clause 5.6.2.     2. The layout verification report listing all steps of verification performed (see clause 5.6.3) together with the corresponding results. |  |
| 7.3.6a | The design validation documentation shall consist of the following contributions to the layout documentation:  1. The validation report presenting the scope, sequences, set-up and results of the validation tests performed as detailed in clause 5.8.1.  2. The radiation test report (if applicable) providing the test board circuitry and bias conditions, the test sequence and investigated irradiation levels, the performed measurements and the resulting degradations.  3. The release report summarizing all activities performed to assure that all necessary prerequisites are fulfilled to start a FM production (see clause 5.8.3). |  |
| 7.4.1a | If requested by the customer, a data sheet that describes the functionality of the device so it can be used by a board or system designer shall be established in conformance with the DRD in Annex G. |  |
| 7.4.2a | If requested by the customer, an application note shall be established for components that are regarded as standard parts for a variety of system applications. This note shall provide information to guide the reader through the possible configurations the device or module can be operated with examples for the corresponding bias circuitry, supply voltages and configuration signals shall be provided. |  |
| 7.4.3a | All devices intended for use as FM products shall be procured according to controlled specifications. |  |
| 7.4.3b | All new specifications shall be designed totally in conformance to one of the existing European standardization systems. |  |
| 7.4.3c | New detail specifications shall be established in conformance with the DRD in Annex H. |  |
| 7.4.3d | Specifications shall include configuration control requirements that ensure that any change of the product that refers to the qualification or that can affect performance, quality, reliability and interchangeability is identified by the manufacturers. |  |
| 8.1a | Upon request, the customer shall receive free of charge from the supplier the information coming from the manufacturer or foundry, for the duration of the development, a complete design kit for the selected process, including all libraries and design kit tools and their complete documentation, in order to allow the customer to independently verify the design.     NOTE This only applies if such a design kit actually exists for the design tools available at the customer. |  |
| 8.1b | The quantity delivered of each individual deliverable item shall be agreed between customer and supplier according to the requirements of the actual project. |  |
| 8.1c | Additional items shall be defined as necessary. |  |
| 8.1d | Each delivery of a design document shall be accompanied by a written statement of the status of the deliverable item. |  |
| 8.1e | The IP rights status shall be reported. |  |
| 8.1f | Paper copies shall be easily readable and suitable for subsequent photo-copying. Electronic copies shall be submitted via electronic media in an agreed format with agreed characteristics.     NOTE Search capability, printability, usage of hyperlinks, traceability and changeability. |  |
| 8.1g | Photos and layout plots may be part of the documentation only for promotional information with restricted details, if not specified elsewhere. |  |
| 8.2a | The list of deliverables defined per the SoW agreed in the business agreement. shall be established , based on Table J-1.      NOTE Table J-1 is a guideline for documentation, design database deliverables and hardware deliverables that become available during the ASIC and FPGA development. |  |
| A.2.1a | The ACP shall include a description of the following items:     1. Organizational structure and management approach including the definition of organizational interfaces between different design groups and identification of the supplier organization for the product assurance of the ASIC and FPGA development;      2. Role, tasks and responsibilities of product assurance personnel in conformance with ECSS-Q-ST-10 and ECSS-Q-ST-20;      3. Management tools used for planning (see clause 4.3) and quality assurance system (see clause 6) of the ASIC and FPGA developments;     4. Intended overall schedule;     5. Overall strategy and general approach for the ASIC and FPGA developments;     6. Risk mitigation procedures applied (see clause 6.3);     7. Requirements on, and system for the control of the foundry and other subcontractors or service providers involved according to the experience available for the respective supplier. | Q-10 - 5.1, 5.2 Q-20 - 5.2, 5.3, 5.4, 5.5, 7.1, 7.2 |
| A.2.1b | Compliance matrix to the clauses of this standard taking into account applicable tailoring. | 5.2.1d, 5.2.1.e |
| A.2.1c | Initiation of the definition phase for the ASIC and FPGA developments. |  |
| B.2.1a | The ADP shall include the following items:     1. Name of the ASIC and FPGA and its basic function;     2. References to the design documentation and other applicable and reference documents;         NOTE Internal and external standards, procedures or coding guidelines.     3. Development team and assignment of major responsibilities;     4. The baseline FPGA device or ASIC technology including baseline radiation hardening and testability approach;     5. Companies involved (foundry, subcontractors, suppliers), indicating their assigned tasks, technical and administrative interfaces;     6. Versions and platforms of tools used, including the foundry or specific tools;      7. Statement for the availability of each design tool (at the site as well as the dedication to the particular development);     8. The design flow;          NOTE Design entry, synthesis, simulation and verification, layout generation and verification, production tests and validation.     9. Identification of a configuration management system in conformance with ECSS-M-ST-40;     10. Identification of a verification and validation scheme in conformance with ECSS-E-ST-10;      11. The subdivision of the ASIC and FPGA development into reasonably sized work packages in conformance with ECSS-M-ST-10;     12. The schedule of the ASIC and FPGA development, with estimated effort and duration of each work package and the planned dates of milestones and review meetings;     13. Identification and full description, including formats, of all relevant outputs, deliverable or not, produced along the ASIC and FPGA development (documentation, simulation and test results, test boards, test samples, source or generated codes and programs) and measures intended to achieve best design quality (e.g. HDL coding conformity to an appropriate set of coding rules). | paragraph 9 -> 8 |
| C.2.1a | The ARS shall include the following items:     1. Overall system partitioning, system configurations and operating modes;     2. Interfaces of the ASIC and FPGA to the system and communication protocols to external devices, including memory mapping;     3. Operating frequency range;     4. Electrical constraints (e.g. voltage and current supply, drive capabilities and external load);     5. Functional requirements;     6. Applicable algorithms;     7. Power-up and initialization state;     8. Reset and power cycling requirements;     9. Error handling;     10. Test modes: system and device tests, on ground and in flight;     11. Fault coverage required at production test;         NOTE This is only applicable for digital ASIC designs.     12. Timing of critical signals;     13. Radiation environment constraints;     14. Thermal environment constraints;     15. Power budget and dissipation;     16. Physical and mechanical constraints: pin assignment, size, encapsulation;     17. Reusability or additional functions for future applications;     18. Portability to different or newer technologies;     19. Intellectual property rights of the design developed;     20. Proprietary designs (IP cores) used as building blocks of the design developed, if already identified. |  |
| D.2.1a | The FRA shall include the following items:     1. Assurance that the collected ASIC and FPGA requirements are complete, settled and unambiguous;     2. Maturity of envisaged ASIC or FPGA manufacturers and possible technologies;     3. Experience and familiarity of engineering resources with the design type, tools, technology and the potential foundries;     4. Risk of underestimation of design and verification effort;     5. Risk of underestimation of debug and repair efforts;     6. Risk of overestimation of actual gate capacity and clocking frequency;     7. Risk of undetermined I/O behaviour during power-up. |  |
| E.2.1a | The VP shall include a description of the following items:     1. In the case of complex digital ASIC developments, verification by FPGA prototyping or emulation;      2. Requirements for code coverage in digital designs;      3. Requirements for hardware-software interaction, possibly by performing co-simulation;     4. Application of coding rules. |  |
| F.2.1a | The DVP shall include the following items:     1. description and requirements for the test set-up or system breadboard;     2. operating modes and test conditions of the prototypes under test;     3. characteristics and functions validated and checked against the ASIC and FPGA requirements specification;     4. if a radiation test is required by the customer, the corresponding radiation verification test plan. |  |
| G.2.1a | Each page shall contain the device name and number and the date of issue.      NOTE The first page contain a summary of the device functionality, a block diagram and short list of features, such as operating frequency, technology and the foundry address. |  |
| G.2.1b | All characteristics and limitations introduced during the design shall be described, such as detailed interface descriptions, register definitions and memory maps. |  |
| G.2.1c | The data sheet shall include a system overview of the device and a description of how to use the device in a representative system environment, including an application block diagram. |  |
| G.2.1d | The full functionality and all operating modes shall be specified in detail. |  |
| G.2.1e | All signal interfaces shall be described in detail including for instance a description of all signals, test and power pins, specifying e.g. the usage of the signals and the signal polarity. |  |
| G.2.1f | The signal descriptions shall be grouped according to their function. |  |
| G.2.1g | All electrical and mechanical data shall be specified, together with their relevant applicable conditions (e.g. temperature and capacitive load), including:     1. Absolute maximum ratings, including storage temperature, operating temperature, supply voltage, maximum input current for any pin, total dose, single event upset, latch-up, electrostatic discharge and reliability figures;     2. DC parameters, including voltage levels, leakage currents, pin capacitances and output currents;     3. Static and dynamic (per MHz) power dissipation, allowing the power consumption at lower operating frequencies calculated, if representative;     4. AC parameters, including e.g. set-up and hold times, cycle periods, output delays and tri-state delays, together with waveform diagrams;     5. Evidences that timing parameters relate to the relevant reference signal edges;     6. Package description, including pin assignment, package figure with pin numbers and preferably signal names, and a mechanical drawing for the package dimensions including information on the thermal characteristic of the package such as wall thickness, thermal coefficient of material or package. |  |
| G.2.1h | A preliminary data sheet shall contain all parts of a final data sheet, with the same level of detail. |  |
| G.2.1i | When data does not exist, estimates shall be used and clearly indicated estimates. |  |
| H.2.1a | The final detail specification shall include the following items:      1. relevant electrical and mechanical parameters;     2. screening, burn-in, and acceptance requirements;     3. deviations from the generic specification;     4. documentation and data requirements;     5. delta limits, when applicable;     6. criteria for percent defective allowable;     7. lot acceptance tests or quality conformance inspections;     8. marking;     9. storage requirements;     10. requirements for lot homogeneity;     11. serialization, when applicable;     12. protective packaging and handling requirements;     13. radiation verification testing requirements, when applicable. |  |
| I.2.1a | The experience summary report shall include the following items:     1. A summary of the main design objectives and constraints;     2. An assessment of the actual development programme with respect to the original ADP;     3. Controls, schedule, design iterations and communications;     4. An assessment of EDA tool suitability and performance;     5. An assessment of the manufacturer support;     6. A presentation of non-conformances and problem areas;     7. In the case of usage of existing IP cores, experiences gained in terms of product quality and suitability;     8. synthesis results, modelling, test stimuli, documentation, application support and problems encountered;     9. Recommendations and lessons learned. |  |

* 1. Traceability from ECSS-Q-ST-60-02C Rev.1 to ECSS-Q-ST-60-02C

Table E-2 presents the traceability from Issue C Revision 1 to Issue C of ECSS-Q-ST-60-02. Whereas Table E-1 presents the information from Issue C to Revision 1.

: Matrix from ECSS-Q-ST-60-02C Rev.1 to ECSS-Q-ST-02C

| ECSS-Q-ST-60-02C Rev.1 | Requirement text | ECSS-Q-ST-60-02C |
| --- | --- | --- |
| 5.1.1a | The supplier shall ensure that a PA organizational structure is defined for DEVICE development, and that individuals have defined tasks and responsibilities in compliance with clause 5.1.1 of ECSS-Q-ST-10 and with DRD from Annex A. | Annex A |
| 5.1.2a | The responsibility, the authority and the interrelation of personnel who manage, perform and verify work affecting DEVICE quality shall be defined and documented. | Annex A |
| 5.1.2b | The responsibilities and the interfaces of each organisation on the project, either external or internal, involved in a project shall be defined and documented. | Annex A |
| 5.1.2c | The delegation of DEVICE product assurance tasks by a supplier to a lower level supplier shall be done in a documented and controlled way, with the supplier retaining the responsibility towards the customer. | Annex A |
| 5.1.3.1a | The DEVICE product assurance responsible shall: 1. Report to the project manager through the project product assurance manager; 2. Have organisational authority and independence to propose and maintain an DEVICE product assurance programme in accordance with the project DEVICE product assurance requirements; 3. Have access to higher management as necessary to fulfil his/her duties. 4. Be invited to all project reviews. | Annex A |
| 5.1.3.2a | The supplier shall review the project requirements to establish and make provision for acquiring or developing the resources and skills for the management and technical staff. | Annex A |
| 5.1.3.2b | The supplier shall maintain training records and ensure that trained personnel are available for the planned activities and tasks. | Annex A |
| 5.1.3.2c | The supplier shall ensure that personnel conducting activities in compliance with ECSS-Q-ST-60-02 and ECSS-E-ST-20-40 are trained. | Annex A |
| 5.1.3.2d | The supplier shall specify the training subjects based on the specific tools, techniques, methodologies and computer resources for use in the development and management of the DEVICE product. | Annex A |
| 5.2.1a | The supplier shall develop a DEVICE product assurance plan in response to the DEVICE product assurance requirements in compliance with DRD in Annex A for customer approval. | Annex A, section 6 |
| 5.2.1b | The DEVICE Product assurance programme shall include all internal manuals, standards or procedures listed in the DEVICE product assurance plan. | Annex A, section 6 |
| 5.2.1c | The DEVICE product assurance plan shall be revisited and updated to ensure that the activities to be undertaken in the following phase are defined. | Annex A, section 6 |
| 5.2.1d | The supplier shall include into the DEVICE product assurance plan a compliance matrix documenting conformance with the individual DEVICE product assurance requirements applicable for the project or business agreement. | Annex A, section 6 |
| 5.2.1e | For each DEVICE product assurance requirement, the compliance matrix shall provide a reference to the document where the expected output of that requirement is located. | Annex A, section 6 |
| 5.2.2a | The supplier shall provide a Product assurance report for each review and for each DEVICE delivery in compliance with DRD from Annex B covering the DEVICE product assurance activities performed during the past project phases. | Annex A, section 6 |
| 5.2.3a | For DEVICE audits, ECSS-Q-ST-10 clause 5.2.3 shall apply. | Annex A, section 6 |
| 5.2.3b | Reviews and audits of processes and of products shall be carried out by personnel not directly involved in the DEVICE work being performed. | Annex A, section 6 |
| 5.2.3c | The supplier shall report on DEVICE Audits in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A, section 6 |
| 5.2.4a | For DEVICE alerts, ECSS-Q-ST-10 clause 5.2.9 shall apply. | Annex A, section 6 |
| 5.2.4b | The supplier shall report on DEVICE Alerts in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A, section 6 |
| 5.2.5a | The supplier shall define and implement procedures for the logging, analysis and correction of all DEVICE problems encountered during DEVICE development in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Annex A, section 6 |
| 5.2.5b | The DEVICE problem report shall contain the following information: 1. Identification of the DEVICE item, 2. Description of the problem, 3. Recommended solution, 4. Final disposition, 5. Modifications implemented, documents, code and tools, and 6. Tests re-executed. | Annex A, section 6 |
| 5.2.5c | The procedures for DEVICE problems reporting shall define the interface with the non-conformance system, the circumstances under which a problem qualifies as a non-conformance. | Annex A, section 6 |
| 5.2.5d | The supplier shall verify the application of problem reporting procedures and report the results in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A, section 6 |
| 5.2.6a | For DEVICE non-conformance handling, ECSS-Q-ST-10-09 shall apply. | Annex A, section 6 |
| 5.2.6b | When dealing with DEVICE non-conformance, the NRB shall include, a representative from the DEVICE product assurance and the DEVICE engineering organizations in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.1. | Annex A, section 6 |
| 5.2.6c | The NRB shall dispose DEVICE non-conformances according to the following criteria in compliance with ECSS-Q-ST-10-09 requirement 5.2.2.4a: 1. Use “as‐is”, when the DEVICE is found to be usable without eliminating the non-conformance, 2. Rework or repair, when the DEVICE product can be made fully in conformance with all specified requirements, by: (a) correction of the DEVICE, (b) addition of DEVICE patches, or (c) re‐design. 3. Scrap,  4. Return to supplier. | Annex A, section 6 |
| 5.2.6d | The DEVICE product assurance plan shall specify the point in the DEVICE life cycle from which the non-conformance procedures apply. | Annex A, section 6 |
| 5.3.1a | The DEVICE Product Assurance responsible shall provide input to Risk management for DEVICE in compliance with ECSS-M-ST-80. | Annex A |
| 5.3.2a | For critical item control, ECSS-Q-ST-10-04 shall apply. | Annex A |
| 5.3.2b | The supplier shall identify the characteristics of the DEVICEs that qualify for inclusion in the Critical Item List. | Annex A |
| 5.4.1a | For supplier selection ECSS-Q-ST-20 clause 5.4.1 shall apply. | Annex A |
| 5.4.1b | For suppliers of existing DEVICE, including DEVICE contained in OTS equipment and units, the selection shall be performed in compliance with requirements from clause 6.2.3. | Annex A |
| 5.4.2a | The supplier shall establish DEVICE product assurance requirements for the next level suppliers, tailored to their role in the project. | Annex A |
| 5.4.2b | The supplier shall provide the DEVICE product assurance requirements applicable to the next level suppliers for customer approval, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Annex A |
| 5.4.3a | The supplier shall monitor the next lower level suppliers’ conformance to the product assurance requirements. | Annex A |
| 5.4.3b | The monitoring process shall include the review and approval of the next lower level suppliers’ product assurance plans, the continuous verification of processes and products, and the monitoring of the final validation of the product. | Annex A |
| 5.4.3c | The supplier shall ensure that DEVICE development processes are defined and applied by the next lower level suppliers in conformance with the DEVICE product assurance requirements for suppliers. | Annex A |
| 5.4.3d | The supplier shall provide the next lower level suppliers’ DEVICE product assurance plan for customer’s acceptance. | Annex A |
| 5.4.4a | The supplier shall provide the lower level suppliers with the results of the safety and dependability analyses performed at higher and his level in compliance with requirements from clause 6.2.1, including: 1. The criticality classification of the DEVICE products to be developed, 2. Information about the failures that can be caused at higher level by the DEVICE products under development. | Annex A |
| 5.5.1a | Methods and tools to be used for all the activities of the development cycle, including requirements analysis, specification, modelling, design, coding, validation, testing, configuration management, verification and product assurance shall be identified by the supplier and agreed with the customer. | Annex A |
| 5.5.1b | The choice of development methods and tools shall be justified by demonstrating through testing or documented assessment as follows: 1. The development team has the experience or training to apply them, 2. The tools and methods are applicable for the functional and operational characteristics of the product,  3. The tools are available throughout the development and maintenance lifetime of the product. | Annex A |
| 5.5.1c | The correct use of methods and tools shall be verified and reported in the DEVICE product assurance report in compliance with DRD in Annex B. | Annex A |
| 5.5.2a | The DEVICE development environment shall be selected according to the following criteria: 1. Availability, 2. Compatibility, 3. Performance, 4. Maintenance, 5. Durability and technical consistency with the operational equipment, 6. The assessment of the product with respect to requirements, including the criticality category, 7. The available support documentation, 8. The acceptance and warranty conditions, 9. The conditions of installation, preparation, training and use, 10. The maintenance conditions, including the possibilities of evolutions, 11. Copyright and intellectual property rights constraints, and 12. Dependence on one specific supplier. | Annex A |
| 5.5.2b | The selection criteria for the DEVICE development environment shall be justified in the Development plan in compliance with DRD from ECSS-E-ST-20-40 Annex B. | Annex A |
| 5.5.2c | The availability of the DEVICE development environment to developers and other users shall be verified before the start of each development phase. | Annex A |
| 6.1.1a | The DEVICE development life cycle specified in ECSS-E-ST-20-40 shall be integrated in the DEVICE product assurance plan in compliance with DRD in Annex A. | Annex A |
| 6.1.1b | The following characteristics of the DEVICE life cycle shall be specified:  1. Phases,  2. Input and output of each phase,  3. Status of completion of phase output,  4. Reviews,  5. Dependencies,  6. Responsibilities, and  7. Role of the customer at each review, in conformance with ECSS-M-ST-10 and ECSS-M-ST-10-01. | Annex A |
| 6.1.1c | In the definition of the DEVICE life cycle specified in requirement 6.1.1a and associated reviews and documents, the quality objectives as defined by the project shall be used. | Annex A |
| 6.1.1d | The Customer shall review the DEVICE life cycle against the contractual DEVICE engineering and product assurance requirements. | Annex A |
| 6.1.1e | The Customer shall review the DEVICE life cycle for the availability of resources. | Annex A |
| 6.2.1.1a | The PA responsible shall report the criticality classification at system-level in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Annex A |
| 6.2.1.2a | The supplier shall perform a dependability and safety analysis at the DEVICE level, using the results of system-level safety and dependability analyses, in order to determine the criticality of each DEVICE function in compliance with ECSS-Q-ST-30 clause 5.4. | Annex A |
| 6.2.1.2b | If the DEVICE is developed with the single criticality specified in the system-level dependability and safety recommendations, the supplier shall justify not performing a dependability and safety analysis at the DEVICE level. | Annex A |
| 6.2.1.2c | The supplier shall report the results of the DEVICE dependability and safety analysis in the in the DEVICE Product Assurance Report in compliance with DRD in Annex B . | Annex A |
| 6.2.1.2d | The supplier shall identify the methods and techniques for the dependability and safety analysis at DEVICE level throughout the DEVICE lifecycle. | Annex A |
| 6.2.1.2e | Methods and techniques for DEVICE dependability and safety analysis shall be agreed between the supplier and customer. | Annex A |
| 6.2.1.2f | The supplier shall report the methods and techniques used for DEVICE dependability and safety analysis in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Annex A |
| 6.2.1.2g | The supplier shall report on the status of the implementation and verification of the DEVICE dependability and safety analysis recommendations in the DEVICE product assurance report in compliance with DRD in Annex B. | Annex A |
| 6.2.1.2h | The supplier shall provide the results of the DEVICE dependability and safety analysis for integration into the system-level dependability and safety analyses, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, addressing the following: 1. Additional failure modes identified at DEVICE level which had not been identified at system level, 2. Recommendations for system-level activities. | Annex A |
| 6.2.2.1a | The supplier shall define, justify and apply measures to assure the dependability and safety of critical DEVICEs. | Annex A |
| 6.2.2.1b | The application of the chosen measures to handle the critical DEVICE shall be verified in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.2.2.1c | The need for updating the DRS, and any of DEVICE Development, verification or validation Plans and its impact in the development flow for critical DEVICE shall be analysed, in the DEVICE Product Assurance Report in compliance with DRD in Annex B, after:  1. Any change of the underlying platform hardware,  2. Any change in the environment in which the DEVICE operates, 3. Any change of the tools, including configuration of the tools, that affect directly or indirectly the development of the DEVICE. | Annex A |
| 6.2.2.2a | Identified unreachable DEVICE functions shall be removed and the need for re-verification and re-validation be analysed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.2.3.1a | The supplier shall identify the reused DEVICE and classify the DEVICE in one of reuse categories, in compliance with ECSS-E-ST-10-02 Table 5-1, and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.2.3.2a | The supplier shall provide DEVICE Reuse File in compliance with DRD in Annex C. | New |
| 6.2.3.2b | The DEVICE Reuse File shall be provided for reuse categories B and C specified in ECSS-E-ST-10-02 Table 5-1. | New |
| 6.2.3.2c | The supplier shall provide the DEVICE Reuse File with its qualification status at the Equipment Qualification Status Review, in compliance with ECSS-E-ST-10-02 requirement 5.2.4.2.d. | New |
| 6.2.3.2d | For Reuse Category D, the full life cycle defined in ECSS-E-ST-20-40 shall apply. | New |
| 6.2.3.2e | Device Reuse File for Reuse Category D specified in requirement 6.2.3.2c is not needed to be produced. | New |
| 6.2.3.2f | The Delta qualification activities shall be completed prior to the qualification review at upper level. | New |
| 6.2.3.2g | Corrective actions shall be identified, documented in the DEVICE Reuse File and applied to the reused DEVICE. | New |
| 6.2.3.3a | The supplier shall characterise, in the DRF, the deliverable DEVICE, which comprises both developed DEVICE and existing reused DEVICE, in terms of constituent elements and the associated licensing schemes, at all reviews, including: 1. The IPR regime and licensing scheme of the developed DEVICE, as defined by the contract, 2. The licence under which the reused DEVICE is accessible by the end user, 3. The analysis of compatibility between the reused DEVICE licence and the developed DEVICE IPR regime and licensing scheme as defined by the contract. This shall include as a minimum: (a) analysis of the reused DEVICE licence terms,  (b) whether any modification has been made to the reused DEVICE and whether this modification is in line with the reused licence terms and the developed DEVICE IPR regime and licensing scheme, as defined by the contract,  (c) the development and licensing strategy for both developed DEVICE and reused DEVICE, in order to ensure the compatibility. | New |
| 6.2.3.4a | Reverse engineering techniques shall be applied to generate missing documentation and to achieve the needed verification and validation coverage. | New |
| 6.2.3.4b | For existing DEVICE whose life cycle data from previous development is not available and reverse engineering techniques are not applicable, the following methods shall be applied: 1. Generation of validation and verification documents based on the available user documentation, and execution of tests to achieve the needed level of test coverage,  2. Use of the existing DEVICE heritage to provide evidence of the product’s suitability for the current application, including following information: (a) relevance of the existing DEVICE heritage for the new operational environment,  (b) configuration management and change control of the DEVICE,  (c) effectiveness of problem reporting,  (d) actual error rates and maintenance records, and  (e) impact of modifications. | New |
| 6.2.3.5a | The DEVICE reuse file shall be updated at project reviews to reflect the results of the identified corrective actions for the existing DEVICE(s) not meeting the project requirements. | New |
| 6.2.3.6a | All the reused DEVICEs and Building Blocks shall be kept under configuration control in compliance with ECSS-Q-ST-60-02 clause 8. | New |
| 6.2.4a | For the selection of tools for automatic code generation, the supplier shall evaluate the following:  1. Evolution of the tools in relation to the tools that use the generated code as an input,  2. Customization of the tools to comply with project requirements,  3. Collection of the design and code metrics,  4. Verification of generated code,  5. Configuration control of the tools including the parameters for customization, and  6. Compliance with standards. | New |
| 6.2.4b | The requirements on verification and validation applicable to the automatically generated code shall ensure the achievement of the same objectives as those for manually generated code. | New |
| 6.2.4c | In case the tool is used to skip verification or testing activities on the generated code, the level of verification and validation of the automatic generation tool shall be at least the same as the one for the generated code. | New |
| 6.2.4d | Coding rules for automatic code generation tools shall be defined in the DEVICE Product Assurance Plan in compliance with DRD in Annex A and applied. | New |
| 6.2.4e | Compliance to coding rules shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.2.4f | Requirement ECSS-E-ST-20-40 Annex C.2.1.k shall apply to automatically generated code, unless the supplier demonstrates that the automatically generated code is not manually modified to comply with the coding and design rules applied to the manually generated code. | New |
| 6.2.4g | The verification and validation documentation shall address separately the activities to be performed for manually and automatically generated code. | New |
| 6.2.5a | The supplier shall define PA requirements, based on the security requirements of the project for which the DEVICE is being developed in the DEVICE Product Assurance Plan in compliance with DRD in Annex A for customer approval. | New |
| 6.2.5b | The supplier shall define methods and tools used to fulfil compliance to the security requirements. | New |
| 6.2.5c | The supplier shall report on conformance to the methods and tools used to fulfil the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.2.5d | The supplier shall report on conformance to the project security requirements in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.2.6a | For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that the outputs defined in ECSS-E-ST-20-40 and in ECSS-Q-ST-60-02 are under configuration management in compliance with of ECSS-Q-ST-60-02 clause 8. | Annex B paragraph 9 |
| 6.2.6b | For each DEVICE phase specified in ECSS-E-ST-20-40, the supplier shall ensure that changes and baseline departure for each outputs and deliverables are under configuration control. | Annex B paragraph 9 |
| 6.2.6c | Problems found during verification activities defined in each of ECSS-E-ST-20-40 phase shall be managed in compliance with ECSS-Q-ST-60-02 clause 5.2.5. | Annex B paragraph 9 |
| 6.2.6d | The supplier shall report on configuration management compliance in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex B paragraph 9 |
| 6.2.7a | The supplier shall provide for customer approval the initial VCD at the DEVICE Definition Phase review for the DEVICE requirements with the combination of the selected verification methods for the different verification levels at the applicable verification stages, in compliance with ECSS-E-ST-10-02 clause 5.2. | 5.8.6 |
| 6.2.7b | The supplier shall provide an updated VCD with the Verification close out status for the DEVICE at each phase in compliance with ECSS-E-ST-10-02 clause 5.2. | 5.8.6 |
| 6.3.1a | The supplier shall provide traceability between System Requirements and DEVICE requirements in the VCD to confirm coverage of system requirements. | Annex A |
| 6.3.2a | Design rules and coding rules shall be defined in the DEVICE Product Assurance in compliance with DRD in Annex A and applied. | Annex A |
| 6.3.2b | Compliance to design rules and coding rules specified in requirement 6.3.2a shall be verified and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3a | DEVICE testing shall be performed in accordance with a strategy for each testing level , which includes the following:  1. The types of tests to perform, 2. The tests to perform in accordance with the plans and procedures, and 3. The means and organizations to perform assurance function for testing and validation. | Annex A |
| 6.3.3b | Based on the criticality of the DEVICE, test coverage goals defined in ECSS-E-ST-20-40 requirements C2.1.g and C.2.1.l for each testing level shall be agreed between the customer and the supplier and their achievement monitored by metrics:  1. For validation against the DEVICE Requirements Specification, and 2. For validation against the system requirements. | Annex A |
| 6.3.3c | The supplier shall ensure through internal review that the test procedures and data are feasible and traceable to the DRS and that they satisfy the DEVICE requirements. | Annex A |
| 6.3.3d | Test coverage shall be checked with respect to the stated goals defined in ECSS-E-ST-20-40 requirement C.2.1.l and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3e | The supplier shall ensure that non-conformances and problem reports detected during testing are documented and reported. | Annex A |
| 6.3.3f | The completion of actions related to problem reports generated during testing and validation shall be verified and recorded in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3g | Provisions shall be made to allow witnessing of tests by the customer as agreed by the project, in compliance with ECSS-Q-ST-20 clause 5.6.4. | Annex A |
| 6.3.3h | Provisions shall be made to allow witnessing of tests by supplier personnel independent of the development. | Annex A |
| 6.3.3i | The supplier shall verify that:  1. Tests are conducted in accordance with approved test procedures and data,  2. Configuration of DEVICE under test is correct,  3. The tests are documented, and  4. The test reports are in compliance with DRD from E-ST-10-02 Annex C. | Annex A |
| 6.3.3j | The supplier shall ensure that tests are repeatable by verifying the recording of DEVICE under test, support software and hardware, test environment, supporting documents and problems found. | Annex A |
| 6.3.3k | The supplier shall confirm in writing that the tests are successfully completed, or that non-conformance and problem reports are raised for unsuccessful tests, in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3l | DEVICE Test Review Board looking to engineering and product assurance aspects shall be convened after the completion of test phases in compliance with ECSS-E-ST-10-03 clause 4.3.2.4. | Annex A |
| 6.3.3m | Functional areas affected by any modification shall be identified and retested. | Annex A |
| 6.3.3n | The need for regression testing and additional verification of the DEVICE shall be analysed after a change or update of any tool used to generate it, and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3o | Qualification status of the DEVICE shall be assessed and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | 5.8.6 |
| 6.3.3p | Any qualification status maintenance activities shall be identified and performed. | 5.8.6 |
| 6.3.3q | In case of retesting, all test related documentation shall be updated. | 5.8.6 |
| 6.3.3r | Validation shall be carried out by staff who have not taken part in the design of the DEVICE being validated. | 5.8.6 |
| 6.3.3s | The necessary resources for testing shall be identified early in the DEVICE life cycle, by including the operating and maintenance requirements. | Annex A |
| 6.3.3t | Test tool development or acquisition, hardware and software, shall be planned for in the overall project plan defined in ECSS-E-ST-20-40 Annex B. | Annex A |
| 6.3.3u | The supplier shall establish and review the test procedures and data before starting testing activities and document the constraints of the tests concerning physical, performance, functional, controllability and observability limitations. | Annex A |
| 6.3.3v | If the risks associated with the project justify the costs involved, Independent Verification and Validation shall be performed by a third party. | Annex A |
| 6.3.3w | The validation shall include testing in the different configurations possible or in a representative set of them when it is evident that the number of possible configurations is too high to allow validation in all of them. | Annex A |
| 6.3.3x | DEVICE containing deactivated functions shall be verified and validated to ensure that the deactivated functions cannot be activated or that their accidental activation cannot harm the operation of the system. | New |
| 6.3.3.2a | The supplier shall report the assessment of the Qualification Status for the DEVICE in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3.2b | The supplier shall assess the DEVICE qualification status as follows: 1. Evidence of compliance to the verification process defined in ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 is provided, 2. The VCD, as defined in requirement 6.2.7, is confirmed complete, 3. All known unresolved issues impact assessment is provided with a correction plan, and 4. Statement that the qualification status is achieved. | Annex A |
| 6.3.3.2c | The qualification status shall be approved by the Customer. | Annex A |
| 6.3.3.3a | For recurrent products, the supplier shall produce release documentation as agreed with the customer. | Annex A |
| 6.3.3.3b | The Customer shall authorise production of each recurrent product. | Annex A |
| 6.3.3.4a | The customer shall establish an acceptance test plan specifying the intended acceptance tests and inspection. | Annex A |
| 6.3.3.4b | The acceptance test shall take place on the flight hardware. | Annex A |
| 6.3.3.4c | The representativeness of the acceptance model against the flight model shall be justified in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | Annex A |
| 6.3.3.4d | The customer shall ensure that the acceptance tests are performed in accordance with the approved acceptance test plan. | Annex A |
| 6.3.3.4e | Test witnessing by PA personnel shall be defined in the acceptance Test Plan. | Annex A |
| 6.3.3.4f | Test performance shall be monitored by the PA personnel in compliance with ECSS-Q-ST-20 clause 5.6.4. | Annex A |
| 6.3.3.4g | The supplier shall provide an End Item Data Pack for each deliverable end item in conformance with ECSS-Q-ST-20 Annex B. | Annex A |
| 6.3.3.4h | The Supplier shall ensure that a Delivery Review Board is convened in compliance with ECSS-Q-ST-20 clause 5.7.3 | Annex A |
| 6.3.3.5a | Maintenance activities shall be performed and documented in compliance to DRD in ECSS-E-ST-20-40 Annex E. | 5.2.a |
| 6.4.1a | The supplier shall monitor and control the effectiveness of the processes used during the development of the DEVICE including the relevant processes corresponding to the services called from other organizational entities outside the project team and report it in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.4.1b | The process assessment model and method used when performing any DEVICE process assessment shall be documented in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | New |
| 6.4.2a | The process assessment results shall be reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 6.4.3a | The suppliers shall ensure that the results of the process assessments are used in its project activities and reported in the DEVICE Product Assurance Report in compliance with DRD in Annex B. | New |
| 7.1.1a | The supplier shall define assurance activities to ensure that the DEVICE meets the quality requirements, in the DEVICE Product Assurance Plan in compliance with DRD in Annex A. | Annex A |
| 7.1.2a | In order to verify the implementation of the product quality requirements, the supplier shall define a metrication programme , and reported in the DEVICE Product Assurance Plan in compliance with DRD in Annex A, specifying: 1. The metrics to collect and store, 2. Measurement method used to collect the metrics, 3. The target values, with reference to the product quality requirements, 4. The analyses to perform on the collected metrics, including the ones to derive: (a) descriptive statistics, (b) trend analysis. 5. How the results of the analyses performed on the collected metrics are fed back to the development team and used to identify corrective actions; 6. The schedule of metrics collection, storing, analysis and reporting, with reference to the whole DEVICE development flow. | New |
| 7.1.3a | The following basic products metrics shall be used: 1. DEVICE Requirements coverage, 2. Test coverage, 3. Number of failures, 4. Trend analysis on problem report and NCs. | New |
| 7.1.4a | The results of metrics collection and analysis shall be included in the DEVICE product assurance report in compliance with DRD in Annex B, in order to provide the customer with an insight into the level of quality obtained. | New |
| 7.2.2a | The information related to components developed for reuse in the DEVICE Requirement Specification, the applicable expected outputs from ECSS-E-ST-20-40 and ECSS-Q-ST-60-02 shall be self-contained. | Annex A |
| 7.2.3a | The DEVICE Requirement Specification, in compliance with DRD in ECSS-E-ST-20-40 Annex A, of components developed for reuse shall include requirements for portability. | New |
| 7.2.4a | The configuration management system shall include provisions for handling specific aspects of DEVICE developed for reuse, such as: 1. Longer lifetime of the components developed for reuse compared to the other components of the project, 2. Evolution or change of the development environment for the next project that intends to use the components;  3. Transfer of the configuration and documentation management information to the next project reusing the DEVICE. | Annex B2.1 paragraph 9 |
| 7.2.5a | Where the IP core, developed for reuse, are developed for multiple EEE components, the testing of the DEVICE shall be performed on all of them. | Annex A |
| 7.2.5b | Statement that tests have been successfully completed on all EEE components specified in requirement 7.2.5a shall be provided in release documentation. | Annex A |
| 7.2.6a | The supplier shall provide a certificate of conformance in compliance with DRD in ECSS-Q-ST-20 Annex D. | Annex A |
| 8.1.1a | The supplier shall develop a DEVICE configuration management plan in conformance with DRD in ECSS-M-ST-40C Annex A. | Annex B2.1 paragraph 9 |
| 8.1.1b | The DEVICE configuration management plan shall be either a standalone document or a section of the supplier overall configuration management plan. | Annex B2.1 paragraph 9 |
| 8.1.2a | The DCMP shall cover the DEVICE and its associated software tools. | Annex B2.1 paragraph 9 |
| 8.2.1a | The DEVICE configuration management system shall allow regeneration of any reference version from backups. | Annex B2.1 paragraph 9 |
| 8.2.2a | The DEVICE Configuration Item Data List and the As-Built Configuration List shall be provided with each DEVICE delivery. | Annex B2.1 paragraph 9 |
| 8.2.2b | The CIDL shall be in compliance with DRD from ECSS-M-ST-40 Annex C. | Annex B2.1 paragraph 9 |
| 8.2.2c | The ABCL shall be in compliance with DRD from ECSS-M-ST-40 Annex D. | Annex B2.1 paragraph 9 |
| 8.2.2d | The CIDL and ABCL shall be provided and up to date for each project review. | Annex B2.1 paragraph 9 |
| 8.2.2e | Any components of the code generation tool that are customizable by the user shall be put under configuration control in the Software Configuration File in compliance with ECSS-M-ST-40 Annex E. | Annex B2.1 paragraph 9 |
| 8.2.2f | For components specified in the requirement 8.2.2e the change control procedures defined for the project shall address their specific aspects. | Annex B2.1 paragraph 9 |
| 8.2.2g | The supplier shall ensure that all authorized changes are implemented in accordance with the configuration management plan. | Annex B2.1 paragraph 9 |
| 8.2.2h | The mask generation and verification for ASICs shall be performed under the foundry's configuration control system. | Annex B2.1 paragraph 9 |
| 8.2.2i | All inputs to the design that are not automatically generated and are needed to reproduce the design shall be put under a revision control mechanism agreed with the customer. | Annex B2.1 paragraph 9 |
| 8.2.2j | Each DEVICE development step using design inputs shall reflect the revision numbers of the inputs in a log file to prove consistency. | Annex B2.1 paragraph 9 |
| 8.2.2k | The following documents shall be controlled in compliance with ECSS-Q-ST-10 clause 5.2.5:  1. Procedural documents describing the quality system applied during the DEVICE life cycle,  2. Planning documents describing the planning and progress of the activities,  3. Documents describing a particular DEVICE, including:  (a) development phase inputs,  (b) development phase outputs,  (c) verification and validation plans and results,  (d) test case specifications, test procedures and test reports,  (e) traceability matrices,  (f) documentation for the DEVICE and system operators and users, and (g) maintenance documentation. | Annex B2.1 paragraph 9 |
| 8.2.3a | Software configuration for the DEVICE software tools shall be documented in a SCF in compliance with DRD in ECSS-M-ST-40 Annex E. | Annex B2.1 paragraph 9 |
| 8.2.3b | The SCF shall be available and up to date for each DEVICE project review. | Annex B2.1 paragraph 9 |
| 8.3a | Configuration control shall be defined in conformance with ECSS-M-ST-40 clause 5.3.2. | Annex B2.1 paragraph 9 |
| 8.3b | Configuration control shall include problem reports produced during development, in compliance with clause 5.2.5 | Annex B2.1 paragraph 9 |
| 8.3c | Configuration control boards shall be defined in compliance with ECSS-M-ST-40C clause 5.3.2. | Annex B2.1 paragraph 9 |
| 8.3d | Each change and departure from baseline shall be classified in accordance with ECSS-M-ST-40 clause 5.3.2. | Annex B2.1 paragraph 9 |
| 8.3e | At each review, the supplier shall report on any change and departure which took place during the DEVICE development phase and assess impact on previous review conclusions. | Annex B2.1 paragraph 9 |

Bibliography

|  |  |
| --- | --- |
| ECSS-S-ST-00 | ECSS system – Description, implementation and general requirements |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |