ECSS-Q-ST-80C Rev.2
30 April 2025

Space product assurance

Software product assurance

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Section
Noordwijk, The Netherlands

Foreword

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-Q-ST-80C Rev.2 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

Published by: ESA Requirements and Standards Section
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-Q-80A 19 April 1996	First issue
ECSS-Q-80B 10 October 2003	Second issue
ECSS-Q-ST-80C 6 March 2009	Third issue
ECSS-Q-ST-80C Rev.1 15 February 2017	Third issue, Revision 1
ECSS-Q-ST-80C Rev.2 30 April 2025	Third issue, Revision 2 Changes with respect to ECSS-Q-ST-80C Rev.1 (15 February 2027) are identified with revision tracking. Main changes • Implementation of change requests • Addition of clause 6.2.9 “Software security” • Addition of clause 6.2.10 “Handling of security software” • Split of former clause 6.3.6 “Software delivery and acceptance” to new clauses 6.3.6 “Software delivery and installation” and 6.3.7 “Software acceptance”, including renumbering of existing and addition of new subclauses. **Detailed Change Record:** Deleted requirements: 6.3.7.4a (formerly 6.3.6.6a). Added requirements: 5.1.5.4b; 5.2.6.1d; 5.4.5a; 6.1.4b; 6.2.4.8b and c; 6.2.4.12a; 6.2.6.13c; 6.2.7.3b; 6.2.9.1a; clause 6.2.9 “Software security”; clause 6.2.10 “Handling of security”; 6.3.1.3b; 6.3.2.3b; 6.3.5.14b; 6.3.5.28b; 6.3.5.33a; 6.3.6.1a and b; 6.3.6.3a; 6.3.7.1b; 7.5.2b; B.2.1<6.4>a and b. Modified requirements: 5.1.5.4a; 5.2.7.2a Note; 5.4.1.2a (editorial); 5.5.3a; 5.5.6a (Note added); 5.6.1.2a; 5.7.1a; 5.7.2.2.a; 5.7.2.3a; 5.7.2.4a; 5.7.3.3a Note; 6.1.3a; 6.1.5a; 6.2.1.1a; 6.2.3.2 Note; 6.2.4.7a; 6.2.4.9a; 6.2.4.10a; 6.2.4.11a; 6.2.6.1a (Exp. Output); 6.2.6.13 Note added; 6.2.6.13b; 6.2.7.3 (Exp. Output removed), 6.2.7.4a; 6.2.7.8b; 6.3.4.1a; 6.3.4.4a; 6.3.4.6a; 6.3.5.1 Note; 6.3.5.2a; 6.3.5.28a (Exp. Output removed); 6.3.9.2a; 6.3.9.4a; 6.3.9.7a; 7.1.1a; 7.2.2.3a Note; 7.4.4a; 7.5.1a; 7.5.2a.

	Editorial changes: • Notes placed always after the text of the normative provision or Expected Output. • Addition of new 6.3.6.1 and 6.3.6.3 causes renumbering of previous clause numbers. • Addition of heading 6.3.7 “Software acceptance” causes renumbering of subsequent clause numbers. • Clause 7.5 renamed from “Firmware” to “Programmable devices”. • Annexes updated.

Table of contents

Change log **3**

1 Scope **10**

2 Normative references **11**

3 Terms, definitions and abbreviated terms **12**

3.1 Terms from other standards 12
3.2 Terms specific to the present standard 12
3.3 Abbreviated terms 17
3.4 Nomenclature 19

4 Space system software product assurance principles **20**

4.1 Introduction 20
4.2 Organization of this Standard 21
4.3 Tailoring of this Standard 23
4.4 Security aspects of this Standard 23

5 Software product assurance programme implementation **24**

5.1 Organization and responsibility 24
5.1.1 Organization 24
5.1.2 Responsibility and authority 24
5.1.3 Resources 25
5.1.4 Software product assurance manager/engineer 25
5.1.5 Training 25
5.2 Software product assurance programme management 26
5.2.1 Software product assurance planning and control 26
5.2.2 Software product assurance reporting 28
5.2.3 Audits 28
5.2.4 Alerts 28
5.2.5 Software problems 29
5.2.6 Nonconformances 29
5.2.7 Quality requirements and quality models 30
5.3 Risk management and critical item control 31
5.3.1 Risk management 31
5.3.2 Critical item control 31
5.4 Supplier selection and control 32

5.4.1 Supplier selection....32
5.4.2 Supplier requirements....32
5.4.3 Supplier monitoring....32
5.4.4 Criticality classification....33
5.4.5 Security sensitivity....33
5.5 Procurement....34
5.5.1 Procurement documents....34
5.5.2 Review of procured software component list....34
5.5.3 Procurement details....34
5.5.4 Identification....34
5.5.5 Inspection....34
5.5.6 Exportability....34
5.6 Tools and supporting environment....35
5.6.1 Methods and tools....35
5.6.2 Development environment selection....35
5.7 Assessment and improvement process....36
5.7.1 Process assessment....36
5.7.2 Assessment process....37
5.7.3 Process improvement....38

6 Software process assurance....40
6.1 Software development life cycle....40
6.1.1 Life cycle definition....40
6.1.2 Process quality objectives....40
6.1.3 Life cycle definition review....40
6.1.4 Life cycle resources....40
6.1.5 Software validation process schedule....41
6.2 Requirements applicable to all software engineering processes....41
6.2.1 Documentation of processes....41
6.2.2 Software dependability and safety....42
6.2.3 Handling of critical software....45
6.2.4 Software configuration management....47
6.2.5 Process metrics....50
6.2.6 Verification....51
6.2.7 Reuse of existing software....54
6.2.8 Automatic code generation....57
6.2.9 Software security....58
6.2.10 Handling of security sensitive software....60

6.3 Requirements applicable to individual software engineering processes or activities....61
6.3.1 Software related system requirements process....61
6.3.2 Software requirements analysis....62
6.3.3 Software architectural design and design of software items....63
6.3.4 Coding....64
6.3.5 Testing and validation....66
6.3.6 Software delivery and installation....72
6.3.7 Software acceptance....72
6.3.8 Operations....74
6.3.9 Maintenance....74

7 Software product quality assurance....77
7.1 Product quality objectives and metrication....77
7.1.1 Deriving of requirements....77
7.1.2 Quantitative definition of quality requirements....77
7.1.3 Assurance activities for product quality requirements....77
7.1.4 Product metrics....77
7.1.5 Basic metrics....78
7.1.6 Reporting of metrics....78
7.1.7 Numerical accuracy....78
7.1.8 Analysis of software maturity....79
7.2 Product quality requirements....79
7.2.1 Requirements baseline and technical specification....79
7.2.2 Design and related documentation....80
7.2.3 Test and validation documentation....80
7.3 Software intended for reuse....81
7.3.1 Customer requirements....81
7.3.2 Separate documentation....81
7.3.3 Self-contained information....81
7.3.4 Requirements for intended reuse....81
7.3.5 Configuration management for intended reuse....82
7.3.6 Testing on different platforms....82
7.3.7 Certificate of conformance....82
7.4 Standard ground hardware and services for operational system....82
7.4.1 Hardware procurement....82
7.4.2 Service procurement....83
7.4.3 Constraints....83

7.4.4 Selection 83
7.4.5 Maintenance 84
7.5 Programmable devices 84
7.5.1 Device programming 84
7.5.2 Marking 84
7.5.3 Calibration 84

Annex A (informative) Software documentation 85

Annex B (normative) Software product assurance plan (SPAP) - DRD 91
B.1 DRD identification 91
B.1.1 Requirement identification and source document 91
B.1.2 Purpose and objective 92
B.2 Expected response 93
B.2.1 Scope and content 93
B.2.2 Special remarks 97

Annex C (normative) Software product assurance milestone report (SPAMR) - DRD 98
C.1 DRD identification 98
C.1.1 Requirement identification and source document 98
C.1.2 Purpose and objective 98
C.2 Expected response 99
C.2.1 Scope and content 99
C.2.2 Special remarks 100

Annex D (normative) Tailoring of this Standard based on software criticality 101
D.1 Software criticality categories 101
D.2 Applicability matrix 102

Annex E (informative) List of requirements with built-in tailoring capability 114

Annex F (informative) Document organization and content at each milestone 115
F.1 Introduction 115
F.2 ECSS-Q-ST-80 Expected Output at SRR 115
F.3 ECSS-Q-ST-80 Expected Output at PDR 118
F.4 ECSS-Q-ST-80 Expected Output at CDR 123
F.5 ECSS-Q-ST-80 Expected Output at QR 126
F.6 ECSS-Q-ST-80 Expected Output at AR 128

F.7 ECSS-Q-ST-80 Expected Output not associated with any specific milestone review 129

Bibliography 132

Figures

Figure 4-1: Software related processes in ECSS Standards 21

Figure 4-2: Structure of this Standard 22

Figure A-1 : Overview of software documents 85

Tables

Table A-1 : ECSS-E-ST-40 and ECSS-Q-ST-80 Document requirements list (DRL) ... 86

Table B-1 : SPAP traceability to ECSS-E-ST-40 and ECSS-Q-ST-80 clauses 91

Table C-1 : SPAMR traceability to ECSS-Q-ST-80 clauses 98

Table D-1 : Software criticality categories 101

Table D-2 : Applicability matrix based on software criticality 102

1 Scope

This Standard defines a set of software product assurance requirements to be used for the development and maintenance of software for space systems. 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 non-deliverable software which affects the quality of the deliverable product or service provided by a space system, if the service is implemented by software.

ECSS-Q-ST-80 interfaces with space engineering and management, which are addressed in the Engineering (-E) and Management (-M) branches of the ECSS System, and explains how they relate to the software product assurance processes.

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 software product assurance requirements are prepared, is also addressed in clause 4.3.

2
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 revision 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 more 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-40	Space engineering — Software general requirements
ECSS-E-ST-80	Space engineering – Security in space systems lifecycles
ECSS-Q-ST-10	Space product assurance – Product assurance management
ECSS-Q-ST-10-04	Space product assurance – Critical-item control
ECSS-Q-ST-10-09	Space product assurance – Nonconformance control system
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-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
CSW-ESAISVV-2022-GBK-02897	ESA ISVV Handbook - Independent software verification and validation handbook
ISO/IEC 33002:2015	Information technology – Process assessment – Requirements for performing process assessment Process assessment

3 Terms, definitions and abbreviated terms

3.1 Terms from other standards

a. For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply.

b. For the purpose of this Standard, the following terms and definitions from ECSS-E-ST-80 apply:

1. security sensitivity

3.2 Terms specific to the present standard

3.2.1 acceptance test

test of a system or functional unit usually performed by the customer on his premises after installation, with the participation of the supplier to ensure that the contractual requirements are met

NOTE Adapted from ISO/IEC 2382-20:1990

3.2.2 automatic code generation

generation of source code with a tool from a model

3.2.3 code coverage

percentage of the software that has been executed (covered) by the test suite

3.2.4 competent assessor

person who has demonstrated the necessary skills, competencies and experience to lead a process assessment in conformance with ISO/IEC 15504

NOTE Adapted from ISO/IEC 15504:1998, Part 9.

3.2.5 condition

boolean expression not containing boolean operators

3.2.6 configurable code

code that is only intended to be executed in certain specific configurations of the software product

NOTE This can be achieved either by use of compilation/link directives, parameter configuration (e.g. in a configuration file or database) or by target computer environment (e.g. hardware pin selection).

3.2.7 COTS, MOTS software

for the purpose of this Standard, commercial-off-the-shelf and modified-off-the-shelf software for which evidence of use is available

3.2.8 critical software

software of criticality category A, B or C

NOTE See ECSS-Q-ST-80 Annex D.1 – Software criticality categories.

3.2.9 deactivated code

code that is not intended to be executed in the target software product, or in the operational configuration of the target software product

NOTE Code related to defensive programming is not considered as deactivated code.

3.2.10 existing software

any software developed outside the business agreement to which this Standard is applicable, including software from previous developments provided by the supplier, software from previous developments provided by the customer, COTS and MOTS software, freeware and open source software

3.2.11 integration testing

testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them

[IEEE 610.12:1990]

3.2.12 metric

a quantitative measure of the degree to which a system, component, or process possesses a given attribute

[ISO/IEC/IEEE 24765:2017]

3.2.13 migration

porting of a software product to a new environment

3.2.14 mission products

products and services delivered by the space system

NOTE For example: Communications services, science data.

3.2.15 operational

for the purpose of this Standard, related to the software operation

NOTE It is not related to the spacecraft operation.

3.2.16 portability (a quality characteristic)

capability of software to be transferred from one environment to another

3.2.17 processing unit

function which is defined to execute software.

NOTE The term covers the hardware functions such as processing core, Graphical Processing Unit (GPU), Vision Processing Unit (VPU), Tensor Processing Unit (TPU), Neural Processing Unit (NPU), Physics Processing Unit (PPU), Digital Signal Processor (DSP), Image Signal Processor (ISP). It also covers the software processing units such as interpreters, emulators and virtual machines.

3.2.18 quality characteristics (software)

set of attributes of a software product by which its quality is described and evaluated

NOTE A software quality characteristic can have multiple levels of sub-characteristics.

3.2.19 quality model (software)

defined set of characteristics, and of relationships between them, which provides a framework for specifying quality requirements and evaluating quality

[ISO/IEC 25000:2014]

3.2.20 real-time

pertaining to a system or mode of operation in which computation is performed during the actual time that an external process occurs, in order that the computation results can be used to control, monitor, or respond in a timely manner to the external process

[IEEE 610.12:1990]

3.2.21 regression testing (software)

selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements

[IEEE 610.12:1990]

3.2.22 reusability

degree to which a software unit or other work product can be used in more than one computer program or software system

[IEEE 610.12:1990]

3.2.23 software

set of instructions and data executed on a processing unit

NOTE 1: A processing unit can be hardware, e.g. a processor or software, e.g. a virtual machine or an interpreter.

NOTE 2: Some processing units only require data, e.g. configuration of state machines or configuration data of a neural network.

3.2.24 software component

part of a software system

NOTE 1 Software component is used as a general term.

NOTE 2 Components can be assembled and decomposed to form new components. In the production activities, components are implemented as units, tasks or programs, any of which can be configuration items. This usage of the term is more general than in ANSI/IEEE parlance, which defines a component as a "basic part of a system or program"; in this Standard, components are not always "basic" as they can be decomposed.

3.2.25 software item

see "software product"

3.2.26 software product

set of software, procedures, scripts, documentation and their associated data

NOTE The term "software item" is synonymous.

3.2.27 software problem

condition of a software product that causes difficulty or uncertainty in the use of the software

[CMU/SEI-92-TR-022]

3.2.28 software product assurance

totality of activities, standards, controls and procedures in the lifetime of a software product which establishes confidence that the delivered software product, or software affecting the quality of the delivered product, conforms to customer requirements

3.2.29 software unit

atomic level software component that can be subjected to stand-alone testing

3.2.30 test case

set of test inputs, execution conditions and expected results developed for a particular objective such as to exercise a particular program path or to verify compliance with a specified requirement

3.2.31 test procedure

detailed instructions for the set up, operation and evaluation of the results for a given test

3.2.32 threat

potential cause of an unwanted incident, which can result in harm to a system or organization

[ISO/IEC 27000:2018]

3.2.33 unit test

test of individual software unit

3.2.34 unreachable code

code that cannot be executed due to design or coding error

3.2.35 usability (a quality characteristic)

capability of the software to be understood, learned, used and liked by the user, when used under specified conditions

3.2.36 validation

<CONTEXT: software> process to confirm that the requirements are correctly and completely implemented in the final product

3.2.37 verification

<CONTEXT: software> process to confirm that adequate specifications and inputs exist for any activity, and that the outputs of the activities are correct and consistent with the specifications and input

NOTE The definition of verification at software level differs from the definition of verification at system level.

3.2.38 vulnerability

weakness which can be exploited by a threat source

3.2.39 walk-through

static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and make comments about possible errors, violation of development standards, and other problems

[IEEE 1028-1997]

3.3 Abbreviated terms

For the purpose of this Standard and of ECSS-E-ST-40, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

For the definition of DRD acronyms see Annex A.

NOTE The abbreviated terms are common for the ECSS-E-ST-40 and ECSS-Q-ST-80 Standards.

Abbreviation	Meaning
AR	acceptance review NOTE The term SW-AR can be used for clarity to denote ARs that solely involve software products.
CDR	critical design review NOTE The term SW-CDR can be used for clarity to denote CDRs that solely involve software products.
CMMI	capability maturity model integration
COTS	commercial-off-the-shelf
CPU	central processing unit NOTE The term CPU is commonly used to identify one or a group of processing units (PU).
DDF	design definition file
DDR	detailed design review
DJF	design justification file
DRD	document requirements definition
ECSS	European Cooperation for Space Standardization
eo	expected output
GS	ground segment
HMI	human machine interface
HSIA	hardware-software interaction analysis
HW	hardware
ICD	interface control document
IRD	interface requirements document
ISO	International Organization for Standardization
ISV	independent software validation
ISVV	independent software verification and validation
MGT	management file
MF	maintenance file
MOTS	modified off-the-shelf
OBCP	on-board control procedure
OP	operational plan
ORR	operational readiness review

Abbreviation	Meaning
OTS	off-the-shelf
PAF	product assurance file
PDR	preliminary design review NOTE The term SW-PDR can be used for clarity to denote PDRs that solely involve software products.
PRR	preliminary requirement review
PU	processing unit
QR	qualification review NOTE The term SW-QR can be used for clarity to denote QRs that solely involve software products.
RB	requirements baseline
SCAMPI	standard CMMI appraisal method for process improvement
SCMP	software configuration management plan
SDD	software design document
SDE	software development environment
SECOPS	Security operations
SF	security file
SOS	software operation support
SPA	software product assurance
SPAMR	software product assurance milestone report
SPAP	software product assurance plan
SPR	software problem report
SRB	software review board
SRR	system requirements review NOTE The term SW-SRR can be used for clarity to denote SRRs that solely involve software products.
SSMP	software security management plan
SVSR	software validation specification review
SW	software
SWE	software engineering
TRR	test readiness review
TS	technical specification

3.4 Nomenclature

The following nomenclature applies throughout this document:

a. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.

b. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.

NOTE It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.

c. 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”.

d. 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.

NOTE In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.

e. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

4
Space system software product assurance principles

4.1 Introduction

The objectives of software product assurance are to provide adequate confidence to the customer and to the supplier that the developed or procured/reused software satisfies its requirements throughout the system's lifetime. In particular, that the software is developed to perform properly, securely, and safely in its operational environment, meeting the project's agreed quality objectives.

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

One of the fundamental principles of this Standard is the customer-supplier relationship, assumed for all software developments. The organizational aspects of this are defined in ECSS-M-ST-10. In the general case, the customer is the procurer of two strongly associated products: the hardware and the software components of a system, subsystem, set, equipment, or assembly. The concept of the customer-supplier relationship is applied recursively, i.e. the customer can 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 software product assurance requirements and provides the specified evidence of compliance.

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

This Standard complements ECSS-E-ST-40 "Space engineering — Software general requirements", with product assurance aspects, integrated in the space system software engineering processes as defined in ECSS-E-ST-40. Together the two standards specify all processes for space software development.

Figure 4-1 schematically presents the different Software processes addressed by the set of the ECSS standards.

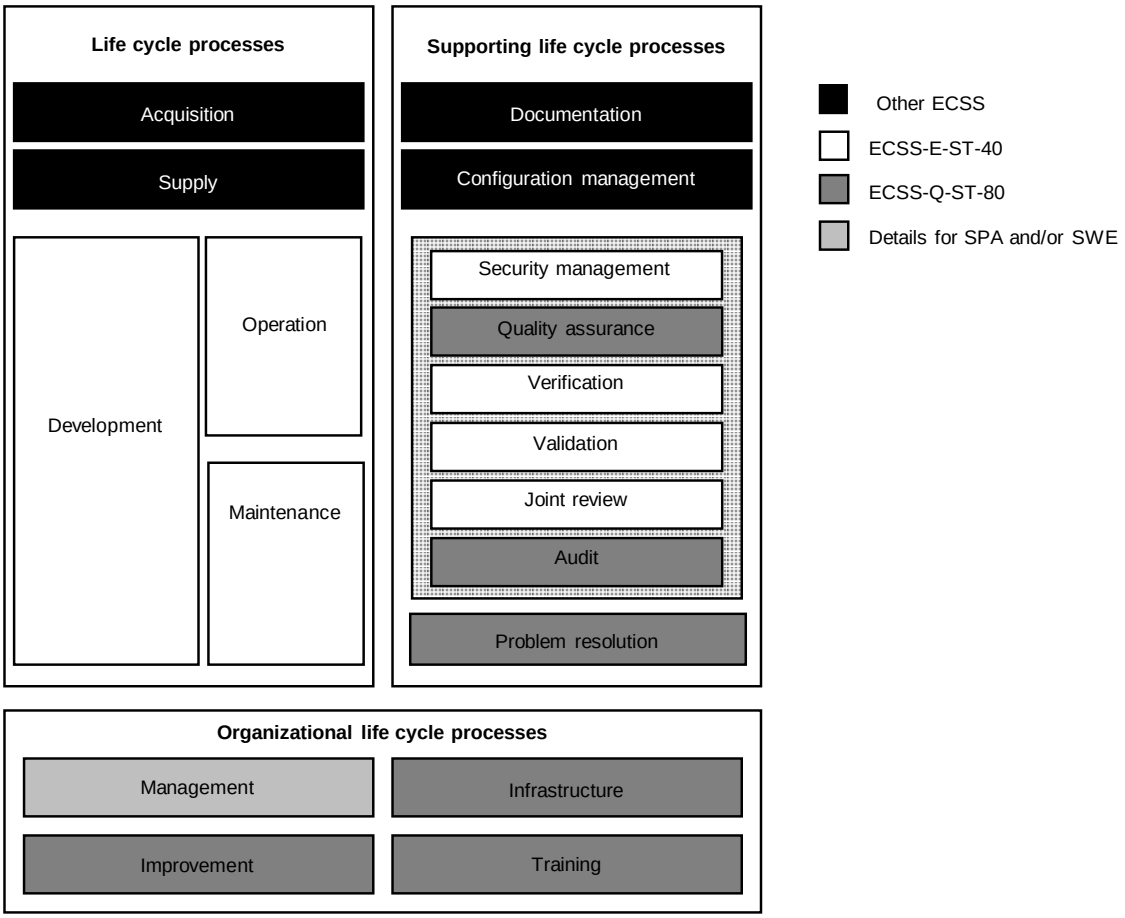

Figure 4-1: Software related processes in ECSS Standards

4.2 Organization of this Standard

This Standard is organized into three main parts:

- Software product assurance programme implementation
- Software process assurance
- Software product quality assurance.

The software documentation collecting the expected output of the ECSS-E-ST-40 and ECSS-Q-ST-80 requirements is summarized in Annex A.

Annex B and Annex C specify the DRDs (document requirements definitions) of the software product assurance documents (SPAP and SPAMR). The DRDs of other software engineering and management documents are included in ECSS-E-ST-40 and ECSS-M-ST-40.

The organization of this Standard is reflected in detail in Figure 4-2.

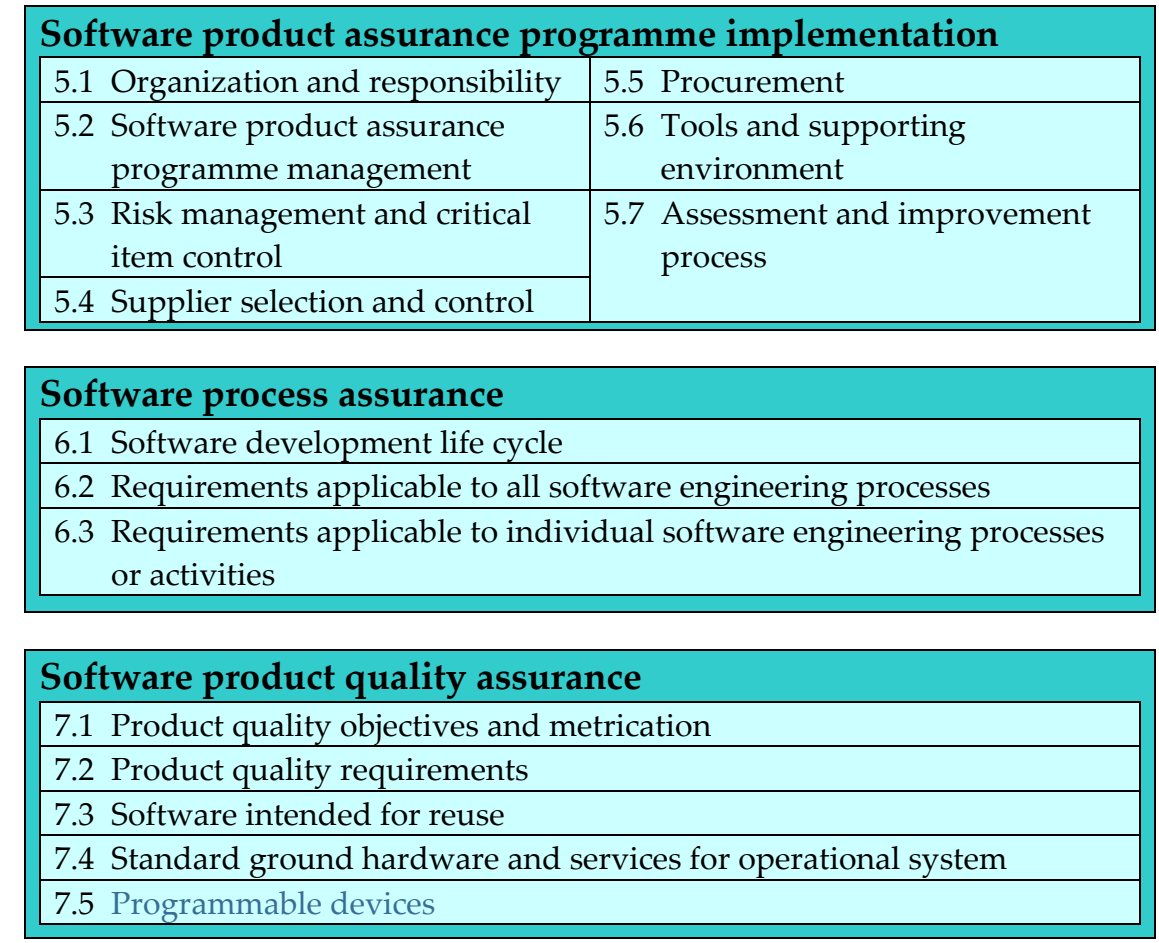

Figure 4-2: Structure of this Standard

Each requirement of this Standard is identified by a hierarchical number, plus a letter if necessary (e.g. 5.3.1.5, bullet a). For each requirement, the associated output is given in the "Expected Output" section. When several outputs are expected, they are identified by a letter (e.g. "a", "b", etc.). With each output, the destination file of the output is indicated in brackets, together with the corresponding document DRD (after a comma) and review(s) (after a semicolon). For example: "*[PAF, SPAP; SRR]*" denotes an output contained in the Software Product Assurance Plan, part of the Product Assurance File, and required at SRR. When no DRD is defined for an Expected Output, and/or the Expected Output is not to be provided at any specific milestone review, then the corresponding sections of that Expected Output are replaced by dashes (e.g. "*[PAF, -; -]*").

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

4.3 Tailoring of this Standard

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

Several drivers for tailoring, include security, dependability and safety aspects, software 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 software. Annex D contains a tailoring of this Standard based on software criticality.

Tailoring for security is based on the selection of requirements related to the verification, validation and levels of proofs demanded by the sensitivity of the software.

Tailoring for software development constraints considers the special characteristics of the software being developed and the development environment. The type of software development (e.g. database or real-time) and the target system (e.g. embedded processor, host system, programmable devices, or application-specific integrated circuits) are also taken into account (see Annex T of ECSS-E-ST-40). Specific requirements for verification, review, and inspection are imposed, for example, when full validation on the target computer is not feasible or performance goals are difficult to achieve.

Tailoring for product quality and business objectives is done by selecting requirements on quality of the product, as explained in clause 7 of this Standard, based on the quality objectives for the product specified by the customer.

4.4 Security aspects of this Standard

Given the particularities related to security requirements, the following consideration is made:

Security assurance requirements significantly influence the security requirements for software product development. Higher levels of security assurance increase confidence in the security features but demand increased security controls on the development and evaluation of the software, to limit the potential for weaknesses and vulnerabilities present in the software.

5
Software product assurance programme implementation

5.1 Organization and responsibility

5.1.1 Organization

ECSS-Q-ST-80_0720001

a. The supplier shall ensure that an organizational structure is defined for software development, and that individuals have defined tasks and responsibilities.

5.1.2 Responsibility and authority

5.1.2.1

ECSS-Q-ST-80_0720002

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

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR].*

5.1.2.2

ECSS-Q-ST-80_0720003

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

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR].*

5.1.2.3

ECSS-Q-ST-80_0720004

a. The delegation of software 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.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR].*

5.1.3 Resources

5.1.3.1

ECSS-Q-ST-80_0720005

a. The supplier shall provide adequate resources to perform the required software product assurance tasks.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR].

5.1.3.2

ECSS-Q-ST-80_0720006

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

5.1.4 Software product assurance manager/engineer

5.1.4.1

ECSS-Q-ST-80_0720007

a. The supplier shall identify the personnel responsible for software product assurance for the project (SW PA manager/engineer).

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR].

5.1.4.2

ECSS-Q-ST-80_0720008

a. The software product assurance manager/engineer shall

1. report to the project manager (through the project product assurance manager, if any);
2. have organisational authority and independence to propose and maintain a software product assurance programme in accordance with the project software product assurance requirements;
3. have unimpeded access to higher management as necessary to fulfil his/her duties.

5.1.5 Training

5.1.5.1

ECSS-Q-ST-80_0720009

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

EXPECTED OUTPUT: Training plan [MGT, -; SRR].

5.1.5.2

ECSS-Q-ST-80_0720010

a. The supplier shall maintain training records.

EXPECTED OUTPUT: *Records of training and experience [PAF, -; -].*

5.1.5.3

ECSS-Q-ST-80_0720011

a. The supplier shall ensure that the right composition and categories of appropriately trained personnel are available for the planned activities and tasks in a timely manner.

5.1.5.4

ECSS-Q-ST-80_0720012

a. The supplier shall determine the training subjects based on the specific tools, techniques, methodologies, and computer resources to be used in developing and managing software product.

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

ECSS-Q-ST-80_0720314

b. The supplier shall ensure that personnel involved in the planned activities and tasks are appropriately trained for:

1. software security analysis, security audits;
2. security engineering;
3. security assurance methods and tools;
4. security rules, policies and procedures applicable to the project.

NOTE It is good practice to make use of security certified organizations performing these types of training.

5.2 Software product assurance programme management

5.2.1 Software product assurance planning and control

5.2.1.1

ECSS-Q-ST-80_0720013

a. The supplier shall develop a software product assurance plan in response to the software product assurance requirements in conformance with DRD in annex B.

ECSS-Q-ST-80_0720014

b. The software product assurance plan shall be either a standalone document or a section of the supplier overall product assurance plan.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

5.2.1.2

ECSS-Q-ST-80_0720015

a. Any internal manuals, standards or procedures referred to by the software product assurance plan shall become an integral part of the supplier's software product assurance programme.

5.2.1.3

ECSS-Q-ST-80_0720016

a. The software product assurance plan shall be revisited and updated as needed at each milestone to ensure that the activities to be undertaken in the following phase are fully defined.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; CDR, QR, AR, ORR].*

5.2.1.4

ECSS-Q-ST-80_0720017

a. Before acceptance review, the supplier shall either supplement the software product assurance plan to specify the quality measures related to the operations and maintenance processes, or issue a specific software product assurance plan.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; AR].*

5.2.1.5

ECSS-Q-ST-80_0720018

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

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

ECSS-Q-ST-80_0720019

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

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

NOTE For compliance with the required DRDs a general statement of compliance is acceptable.

5.2.2 Software product assurance reporting

5.2.2.1

ECSS-Q-ST-80_0720020

a. The supplier shall report on a regular basis on the status of the software product assurance programme implementation, if appropriate as part of the overall product assurance reporting of the project.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

5.2.2.2

ECSS-Q-ST-80_0720021

a. The software product assurance report shall include:

1. an assessment of the current quality of the product and processes, based on measured properties, with reference to the metrication as defined in the software product assurance plan;
2. verifications undertaken;
3. problems detected;
4. problems resolved.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

5.2.2.3

ECSS-Q-ST-80_0720022

a. The supplier shall deliver at each milestone review a software product assurance milestone report, covering the software product assurance activities performed during the past project phases.

EXPECTED OUTPUT: Software product assurance milestone report [PAF, SPAMR; SRR, PDR, CDR, QR, AR, ORR].

5.2.3 Audits

ECSS-Q-ST-80_0720023

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

EXPECTED OUTPUT: Audit plan and schedule [PAF, -; SRR].

5.2.4 Alerts

ECSS-Q-ST-80_0720024

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

EXPECTED OUTPUT: The following outputs are expected:

a. Preliminary alert information [PAF, -; -];

b. Alert information [PAF, -; -].

5.2.5 Software problems

5.2.5.1

ECSS-Q-ST-80_0720025

a. The supplier shall define and implement procedures for the logging, analysis and correction of all software problems, encountered during software development.

EXPECTED OUTPUT: *Software problem reporting procedures [PAF, -; PDR].*

5.2.5.2

ECSS-Q-ST-80_0720026

a. The software problem report shall contain the following information:

1. identification of the software item;
2. description of the problem;
3. recommended solution;
4. final disposition;
5. modifications implemented (e.g. documents, code, and tools);
6. tests re-executed.

EXPECTED OUTPUT: *Software problem reporting procedures [PAF, -; PDR].*

5.2.5.3

ECSS-Q-ST-80_0720027

a. The procedures for software problems shall define the interface with the nonconformance system (i.e. the circumstances under which a problem qualifies as a nonconformance).

EXPECTED OUTPUT: *Software problem reporting procedures [PAF, -; PDR].*

5.2.5.4

ECSS-Q-ST-80_0720028

a. The supplier shall ensure the correct application of problem reporting procedures.

5.2.6 Nonconformances

5.2.6.1

ECSS-Q-ST-80_0720029

a. For software nonconformance handling, ECSS-Q-ST-10-09 shall apply.

EXPECTED OUTPUT: *The following outputs are expected:*

a. NCR SW procedure as part of the Software product assurance plan [PAF, SPAP; SRR];

b. Nonconformance reports [DJF, -; -].

ECSS-Q-ST-80_0720030

b. When dealing with software nonconformance, the NRB shall include, at least, a representative from the software product assurance and the software engineering organizations.

EXPECTED OUTPUT: *Identification of SW experts in NRB [MGT, -; SRR]*

ECSS-Q-ST-80_0720312

c. The NRB shall dispose software nonconformances according to the following criteria:

1. use "as-is", when the software is found to be usable without eliminating the nonconformance;
2. fix, when the software product can be made fully in conformance with all specified requirements, by:
   (a) correction of the software,
   (b) addition of software patches, or
   (c) re-design.
3. return to supplier, for procured software products (e.g. COTS).

EXPECTED OUTPUT: *Nonconformance reports [DJF, -; -].*

ECSS-Q-ST-80_0720315

d. When dealing with software nonconformance with a possible security impact, the NRB shall include a representative from the software security engineering organizations.

5.2.6.2

ECSS-Q-ST-80_0720031

a. The software product assurance plan shall specify the point in the software life cycle from which the nonconformance procedures apply.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

5.2.7 Quality requirements and quality models

5.2.7.1

ECSS-Q-ST-80_0720032

a. Quality models shall be used to specify the software quality requirements.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

5.2.7.2

ECSS-Q-ST-80_0720033

a. The following characteristics shall be used to specify the quality model:

1. functionality;
2. reliability;
3. maintainability;
4. reusability;

5. suitability for safety;
6. security;
7. usability;
8. efficiency;
9. portability;
10. software development effectiveness.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; PDR].

NOTE 1 Quality models are the basis for the identification of process metrics (see clause 6.2.5) and product metrics (see clause 7.1.4).

NOTE 2 Quality models are also addressed by ISO/IEC 25000 and ECSS-Q-HB-80-04.

NOTE 3 Software security vulnerabilities should be taken into account in the quality model.

5.3 Risk management and critical item control

5.3.1 Risk management

ECSS-Q-ST-80_0720034

a. Risk management for software shall be performed by cross-reference to the project risk policy, as specified in ECSS-M-ST-80.

5.3.2 Critical item control

5.3.2.1

ECSS-Q-ST-80_0720035

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

5.3.2.2

ECSS-Q-ST-80_0720036

a. The supplier shall identify the characteristics of the software items that qualify them for inclusion in the Critical Item List.

5.4 Supplier selection and control

5.4.1 Supplier selection

5.4.1.1

ECSS-Q-ST-80_0720037

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

EXPECTED OUTPUT: *The following outputs are expected:*

a. Results of pre-award audits and assessments [PAF, -; -];

b. Records of procurement sources [PAF, -; -].

5.4.1.2

ECSS-Q-ST-80_0720038

a. For the selection of suppliers of existing software, including software contained in OTS equipment and units, the expected output of clauses 6.2.7.2 to 6.2.7.6 shall be made available.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; -].*

5.4.2 Supplier requirements

5.4.2.1

ECSS-Q-ST-80_0720039

a. The supplier shall establish software product assurance requirements for the next level suppliers, tailored to their role in the project, including a requirement to produce a software product assurance plan.

EXPECTED OUTPUT: *Software product assurance requirements for suppliers [PAF, -; SRR].*

5.4.2.2

ECSS-Q-ST-80_0720040

a. The supplier shall provide the software product assurance requirements applicable to the next level suppliers for customer's acceptance.

EXPECTED OUTPUT: *Software product assurance requirements for suppliers [PAF, -; SRR].*

5.4.3 Supplier monitoring

5.4.3.1

ECSS-Q-ST-80_0720041

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

5.4.3.2

ECSS-Q-ST-80_0720042

a. 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.

5.4.3.3

ECSS-Q-ST-80_0720043

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

EXPECTED OUTPUT: *Next level suppliers' software product assurance plan [PAF, SPAP; PDR].*

5.4.3.4

ECSS-Q-ST-80_0720044

a. The supplier shall provide the next lower level suppliers' software product assurance plan for customer's acceptance.

EXPECTED OUTPUT: *Next level suppliers' software product assurance plan [PAF, SPAP; PDR].*

5.4.4 Criticality classification

ECSS-Q-ST-80_0720045

a. The supplier shall provide the lower level suppliers with the relevant results of the safety and dependability analyses performed at higher and his level (ref. clauses 6.2.2.1 and 6.2.2.2), including:

1. the criticality classification of the software products to be developed;
2. information about the failures that can be caused at higher level by the software products to be developed.

EXPECTED OUTPUT: *Safety and dependability analyses results for lower level suppliers [RB, -; SRR].*

5.4.5 Security sensitivity

ECSS-Q-ST-80_0720316

a. The supplier shall provide its suppliers with the relevant results of the security analyses performed at higher and his level as specified in 6.2.9.2), including:

1. the security sensitivity of the software products to be developed;
2. information about the failures, attacks and related security impacts that can be caused at higher level by the software products during development and operation.

EXPECTED OUTPUT: *Security analyses results for lower level suppliers [SF,-;SRR].*

5.5 Procurement

5.5.1 Procurement documents

ECSS-Q-ST-80_0720046

a. For procurement documents, ECSS-Q-ST-20 clause 5.4.2 shall apply.

5.5.2 Review of procured software component list

ECSS-Q-ST-80_0720047

a. The choice of procured software shall be described and submitted for customer review.

EXPECTED OUTPUT: *Software development plan [MGT, SDP; SRR, PDR].*

5.5.3 Procurement details

ECSS-Q-ST-80_0720048

a. For each of the software items the following data shall be provided:

1. ordering criteria
2. receiving inspection criteria;
3. back-up solutions if the product becomes unavailable;
4. contractual arrangements with the supplier for the development, maintenance and upgrades to new releases;
5. country source information if required by the customer.

EXPECTED OUTPUT: *Procurement data [MGT, -; SRR, PDR].*

NOTE Examples of ordering criteria are: versions, options, security certifications and extensions.

5.5.4 Identification

ECSS-Q-ST-80_0720049

a. All the procured software shall be identified and registered by configuration management.

5.5.5 Inspection

ECSS-Q-ST-80_0720050

a. The supplier shall subject the procured software to a planned receiving inspection, in accordance with ECSS-Q-ST-20 clause 5.4.4, and the receiving inspection criteria as required by clause 5.5.3.

EXPECTED OUTPUT: *Receiving inspection report [PAF, -; PDR, CDR, QR].*

5.5.6 Exportability

ECSS-Q-ST-80_0720051

a. Exportability constraints shall be identified.

NOTE Exportability constraints include constraints concerning applicable security export-control regulations.

5.6 Tools and supporting environment

5.6.1 Methods and tools

5.6.1.1

ECSS-Q-ST-80_0720052

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

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR, PDR].

5.6.1.2

ECSS-Q-ST-80_0720053

a. The choice of development methods and tools shall be justified by demonstrating through testing or documented assessment that:

1. the development team has appropriate experience or training to apply them,
2. the tools and methods are appropriate for the functional and operational characteristics of the product, and
3. the tools are available throughout the development and maintenance lifetime of the product,
4. the tools and methods are appropriate to the security sensitivity of the product as determined by the security analysis and as defined in the software security management plan.

EXPECTED OUTPUT: Software product assurance milestone report [PAF, SPAMR; SRR, PDR].

5.6.1.3

ECSS-Q-ST-80_0720054

a. The correct use of methods and tools shall be verified and reported.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

5.6.2 Development environment selection

5.6.2.1

ECSS-Q-ST-80_0720055

a. The software 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;
12. dependence on one specific supplier;
13. the assessment of the product with respect to the security sensitivity level of the products;
14. compliance with appropriate security requirements due to organizational or national security regulations, policies or directives.

EXPECTED OUTPUT: *Software development plan [MGT, SDP; SRR, PDR].*

5.6.2.2

ECSS-Q-ST-80_0720056

a. The suitability of the software development environment shall be justified.

EXPECTED OUTPUT: *Software development plan [MGT, SDP; SRR, PDR].*

5.6.2.3

ECSS-Q-ST-80_0720057

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

5.7 Assessment and improvement process

5.7.1 Process assessment

ECSS-Q-ST-80_0720058

a. The supplier shall monitor and control the capability of the processes used during the development of the software, including the relevant processes corresponding to the services called from other organizational entities outside the project team.

EXPECTED OUTPUT: *Software process assessment records: Overall assessments and improvement programme plan [PAF, -; -].*

NOTE 1 The process assessment and improvement performed at organization level can be used to provide evidence of compliance for the project.

NOTE 2 Process capability is the default process characteristic to be monitored and controlled. It is a characterization of the ability of a process to repeatability, predictability and consistently deliver its defined outcomes.

5.7.2 Assessment process

5.7.2.1

ECSS-Q-ST-80_0720059

a. The process assessment model and method to be used when performing any software process assessment shall be documented.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software process assessment record: assessment model [PAF, -; -];

b. Software process assessment record: assessment method [PAF, -; -].

5.7.2.2

ECSS-Q-ST-80_0720060

a. Assessments performed and process assessment models used shall be in conformance with ISO/IEC 33002:2015.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software process assessment record: evidence of conformance of the process assessment model [PAF, -; -];

b. Software process assessment record: assessment method [PAF, -; -].

NOTE 1 Currently the model and method documented in ECSS-Q-HB-80-02 are not fully conformant to ISO/IEC 33002, however they can also be used with the customer agreement.

NOTE 2 Currently the CMMI model is not fully conformant to ISO/IEC 15504, however it can be used, provided that the SCAMPI A method is applied.

NOTE 3 Organisations that meet the requirements to be designated as Very Small Entity (VSE): enterprises, organizations, departments or projects having up to 25 people, can choose to use a model and a method conformant to ISO/IEC 29110-6-1.

5.7.2.3

ECSS-Q-ST-80_0720061

a. The process assessment model, the method, the assessment scope, the results and the assessors shall be

1. established by the customer, and
2. verified that they are compliant with the project requirements.

EXPECTED OUTPUT: *Software process assessment record: Software process assessment recognition evidence [PAF, -; -].*

NOTE 1 Examples of assessment scopes are: organizational unit evaluated, and processes evaluated.

NOTE 2 ECSS-Q-HB-80-02 provides space specific process reference model and their indicators.

5.7.2.4

ECSS-Q-ST-80_0720062

a. Assessments, shall be performed by a competent assessor.

EXPECTED OUTPUT: *Software process assessment record: competent assessor justification [PAF, -; -].*

NOTE The competency of assessors could be established by the customer on the basis of ISO/IEC 33001 or through certification.

5.7.3 Process improvement

5.7.3.1

ECSS-Q-ST-80_0720063

a. The results of the assessment shall be used as feedback to improve as necessary the performed processes, to recommend changes in the direction of the project, and to determine technology advancement needs.

ECSS-Q-ST-80_0720064

b. The suppliers shall ensure that the results of previous assessments are used in its project activity

EXPECTED OUTPUT: *Software process assessment records: improvement plan [PAF, -; -].*

5.7.3.2

ECSS-Q-ST-80_0720065

a. The process improvement shall be conducted according to a documented process improvement process.

EXPECTED OUTPUT: *Software process assessment records: improvement process [PAF, -; -].*

NOTE 1 For the definition of the process improvement process, see ECSS-Q-HB-80-02.

NOTE 2 For CMMI, the process improvement is described in the OPF (Organizational Process Focus) process area.

5.7.3.3

ECSS-Q-ST-80_0720066

a. Evidence of the improvement in performed processes shall be provided.

EXPECTED OUTPUT: Software process assessment records: evidence of improvements [PAF, -; -].

NOTE 1 See ECSS-Q-HB-80-02.

NOTE 2 Depending on the context, improvements and changes at organisation level can be used to claim process improvement at project level.

6
Software process assurance

6.1 Software development life cycle

6.1.1 Life cycle definition

ECSS-Q-ST-80_0720067

a. The software development life cycle shall be defined or referenced in the software product assurance plan.

ECSS-Q-ST-80_0720068

b. The following characteristics of the software life cycle shall be defined:

1. phases;
2. input and output of each phase;
3. status of completion of phase output;
4. milestones;
5. dependencies;
6. responsibilities;
7. role of the customer at each milestone review, in conformance with ECSS-M-ST-10 and ECSS-M-ST-10-01.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

6.1.2 Process quality objectives

ECSS-Q-ST-80_0720069

a. In the definition of the life cycle and associated milestones and documents, the quality objectives shall be used.

6.1.3 Life cycle definition review

ECSS-Q-ST-80_0720070

a. The software life cycle shall be reviewed against the contractual software engineering, product assurance and security assurance requirements.

6.1.4 Life cycle resources

ECSS-Q-ST-80_0720071

a. The software life cycle shall be reviewed for suitability and for the availability of resources to implement it by all functions involved in its application.

ECSS-Q-ST-80_0720317

b. The disposal and release of the resources used after the software development concludes, shall be performed in accordance with the relevant security requirements.

6.1.5 Software validation process schedule

ECSS-Q-ST-80_0720072

a. A mandatory TRR, as specified in clause 5.3.5.1 of ECSS-E-ST-40, shall be held, in the form of a Project Review as specified in clause 5.3.3.2 ECSS-E-ST-40, before the beginning of the validation against the requirements baseline, to check that:

1. the software status is compatible with the commencement of validation activities;
2. the necessary resources, software product assurance plans, test and validation documentation, simulators or other technical means are available and ready for use.

EXPECTED OUTPUT: *Confirmation of readiness of test activities [DJF; TRR].*

6.2 Requirements applicable to all software engineering processes

6.2.1 Documentation of processes

6.2.1.1

ECSS-Q-ST-80_0720073

a. The following activities shall be covered either in software-specific plans or in project general plans:

1. development;
2. specification, design and customer documents to be produced;
3. configuration and documentation management;
4. verification, testing and validation activities;
5. maintenance and retirement;
6. security management.

EXPECTED OUTPUT: *Software project plans [MGT, MF, DJF, SF].*

6.2.1.2

ECSS-Q-ST-80_0720074

a. All plans shall be finalized before the start of the related activities.

EXPECTED OUTPUT: *Software project plans [MGT, MF, DJF].*

6.2.1.3

ECSS-Q-ST-80_0720075

a. All plans shall be updated for each milestone to reflect any changes during development.

EXPECTED OUTPUT: *Software project plans [MGT, MF, DJF].*

6.2.1.4

ECSS-Q-ST-80_0720076

a. The software product assurance plan shall identify all plans to be produced and used, the relationship between them and the time-scales for their preparation and update.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR, PDR].

6.2.1.5

ECSS-Q-ST-80_0720077

a. Each plan shall be reviewed against the relevant contractual requirements.

6.2.1.6

ECSS-Q-ST-80_0720078

a. Procedures and project standards shall address all types of software products included in the project.

EXPECTED OUTPUT: Procedures and standards [PAF, -; PDR].

6.2.1.7

ECSS-Q-ST-80_0720079

a. All procedures and project standards shall be finalized before starting the related activities.

EXPECTED OUTPUT: Procedures and standards [PAF, -; PDR].

6.2.1.8

ECSS-Q-ST-80_0720080

a. Each procedure or standard shall be reviewed against the relevant plans and contractual requirements.

6.2.1.9

ECSS-Q-ST-80_0720081

a. Before any activity is started, each procedure or standard for that activity shall be reviewed by all functions involved in its application, for suitability and for the availability of resources to implement it.

6.2.2 Software dependability and safety

6.2.2.1

ECSS-Q-ST-80_0720082

a. For the system-level analyses leading to the criticality classification of software products based on the severity of failures consequences, ECSS-Q-ST-40 clause 6.5.6.3, and ECSS-Q-ST-30 clause 5.4, shall apply.

EXPECTED OUTPUT: Criticality classification of software products [PAF, -; SRR, PDR].

6.2.2.2

ECSS-Q-ST-80_0720083

a. The supplier shall perform a software dependability and safety analysis of the software products, using the results of system-level safety and dependability analyses, in order to determine the criticality of the individual software components.

EXPECTED OUTPUT: *Software dependability and safety analysis report [PAF, -; PDR].*

6.2.2.3

ECSS-Q-ST-80_0720084

a. The supplier shall identify the methods and techniques for the software dependability and safety analysis to be performed at technical specification and design level.

ECSS-Q-ST-80_0720085

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

EXPECTED OUTPUT: *Criticality classification of software components [PAF, -; PDR].*

NOTE ECSS-Q-HB-80-03 provides indication on methods and techniques that can be applied such as:

- software failure modes and effects analysis (for the performing of this analysis, see also ECSS-Q-ST-30-02);
- software fault tree analysis;
- software common cause failure analysis.

6.2.2.4

ECSS-Q-ST-80_0720086

a. Based on the results of the software criticality analysis, the supplier shall apply engineering measures to reduce the number of critical software components and mitigate the risks associated with the critical software (ref. clause 6.2.3).

6.2.2.5

ECSS-Q-ST-80_0720087

a. The supplier shall report on the status of the implementation and verification of the SW dependability and safety analysis recommendations.

EXPECTED OUTPUT: *Software dependability and safety analysis report [PAF, -; CDR, QR, AR].*

6.2.2.6

ECSS-Q-ST-80_0720088

a. The supplier shall update the software dependability and safety analysis at each software development milestone, to confirm the criticality category of software components.

EXPECTED OUTPUT: *Software dependability and safety analysis report [PAF, -; CDR, QR, AR].*

6.2.2.7

ECSS-Q-ST-80_0720089

a. The supplier shall provide the results of the software dependability and safety analysis for integration into the system-level dependability and safety analyses, addressing in particular:

1. additional failure modes identified at software design level;
2. recommendations for system-level activities.

EXPECTED OUTPUT: *Software dependability and safety analysis report [PAF, -; PDR, CDR].*

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

6.2.2.8

ECSS-Q-ST-80_0720090

a. As part of the software requirements analysis activities (ref. clause 6.3.2), the supplier shall contribute to the Hardware-Software Interaction Analysis (HSIA) by identifying, for each hardware failure included in the HSIA, the requirements that specify the software behaviour in the event of that hardware failure.

6.2.2.9

ECSS-Q-ST-80_0720091

a. During the verification and validation of the software requirements resulting from the Hardware-Software Interaction Analysis, the supplier shall verify that the software reacts correctly to hardware failures, and no undesired software behaviour occurs that lead to system failures.

6.2.2.10

ECSS-Q-ST-80_0720313

a. If it cannot be prevented that software components cause failures of higher criticality components, due to failure propagation or use of shared resources, then all the involved components shall be classified at the highest criticality category among them.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; PDR, CDR];

b. Software dependability and safety analysis report [PAF, -; PDR, CDR, QR, AR].

NOTE Failures of higher-criticality software components caused by lower-criticality components can be prevented by design measures such as separate hardware platforms, isolation of software processes or prohibition of shared memory (segregation and partitioning).

6.2.3 Handling of critical software

6.2.3.1

ECSS-Q-ST-80_0720092

a. <<deleted>>

ECSS-Q-ST-80_0720093

b. <<deleted>>

6.2.3.2

ECSS-Q-ST-80_0720094

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

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; PDR, CDR].

NOTE These measures can include:

- use of software design or methods that have performed successfully in a similar application;
- insertion of features for failure isolation and handling (ref. ECSS-Q-HB-80-03, software failure modes and effects analysis);
- defensive programming techniques, such as input verification and consistency checks;
- use of a "safe subset" of programming language;
- use of formal design language for formal proof;
- 100 % code branch coverage at unit testing level;
- full inspection of source code;
- witnessed or independent testing;
- gathering and analysis of failure statistics;
- removing deactivated code or showing through a combination of analysis and testing that the means by which such code can be inadvertently executed are prevented, isolated, or eliminated;
- use of dynamic code verification techniques.

6.2.3.3

ECSS-Q-ST-80_0720095

a. The application of the chosen measures to handle the critical software shall be verified.

EXPECTED OUTPUT: Software product assurance milestone report [PAF, SPAMR; PDR, CDR, QR, AR].

6.2.3.4

ECSS-Q-ST-80_0720096

a. Critical software shall be subject to regression testing after:
   1. any change of functionality of the underlying platform hardware;
   2. any change of the tools that affect directly or indirectly the generation of the executable code.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; PDR, CDR].

NOTE 1 In case of minor changes in tools that affect the generation of the executable code, a binary comparison of the executable code generated by the different tools can be used to verify that no modifications are introduced.

NOTE 2 Example for item 1: instruction set of a processor.

6.2.3.5

ECSS-Q-ST-80_0720097

a. The need for additional verification and validation of critical software shall be analysed after:
   1. any change of functionality or performance of the underlying platform hardware;
   2. any change in the environment in which the software or the platform hardware operate.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; PDR, CDR].

6.2.3.6

ECSS-Q-ST-80_0720098

a. Identified unreachable code shall be removed and the need for re-verification and re-validation shall be analysed.

6.2.3.7

ECSS-Q-ST-80_0720099

a. Unit and integration testing shall be (re-)executed on non-instrumented code.

6.2.3.8

ECSS-Q-ST-80_0720100

a. Validation testing shall be (re-)executed on non-instrumented code.

6.2.4 Software configuration management

6.2.4.1

ECSS-Q-ST-80_0720101

a. ECSS-M-ST-40 shall be applied for software configuration management, complemented by the following requirements.

6.2.4.2

ECSS-Q-ST-80_0720102

a. The software configuration management system shall allow any reference version to be re-generated from backups.

EXPECTED OUTPUT: *Software configuration management plan [MGT, SCMP; SRR, PDR].*

6.2.4.3

ECSS-Q-ST-80_0720103

a. The software configuration file and the software release document shall be provided with each software delivery.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software configuration file [DDF, SCF; -];

b. Software release document [DDF, SRelD; -].

6.2.4.4

ECSS-Q-ST-80_0720104

a. The software configuration file shall be available and up to date for each project milestone.

EXPECTED OUTPUT: *Software configuration file [DDF, SCF; CDR, QR, AR, ORR].*

6.2.4.5

ECSS-Q-ST-80_0720105

a. Any components of the code generation tool that are customizable by the user shall be put under configuration control.

ECSS-Q-ST-80_0720106

b. The change control procedures defined for the project shall address the specific aspects of these components.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software configuration file [DDF, SCF; CDR, QR, AR, ORR];

b. Software configuration management plan [MGT, SCMP; SRR, PDR].

6.2.4.6

ECSS-Q-ST-80_0720107

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

EXPECTED OUTPUT: *Authorized changes - Software configuration file [DDF, SCF; CDR, QR, AR, ORR].*

6.2.4.7

ECSS-Q-ST-80_0720108

a. The following documents shall be controlled (see ECSS-Q-ST-10 clause 5.2.5):

1. procedural documents describing the quality system to be applied during the software life cycle;
2. planning documents describing the planning and progress of the activities;
3. documents describing a particular software product, 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) validation control documentation,
   (g) documentation for the software and system operators and users,
   (h) maintenance documentation, and
   (i) Retirement documentation.

6.2.4.8

ECSS-Q-ST-80_0720109

a. The supplier shall identify a method and tool to protect the supplied software against corruption.

NOTE For example: source code, executable and data.

ECSS-Q-ST-80_0720318

b. The supplier shall select methods and tools to protect the supplied software in accordance with the security analysis.

ECSS-Q-ST-80_0720319

c. The security analysis can define security requirements on software integrity checks.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; SRR, PDR];

b. Software configuration file [DDF, SCF; CDR, QR, AR, ORR];

c. Software security management plan [SF, SSMP; SRR, PDR].

6.2.4.9

ECSS-Q-ST-80_0720110

a. The supplier shall specify the necessary elements and mechanisms to prove integrity and authenticity of the SW product.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; SRR, PDR];

b. Software security management plan, [SF, SSMP; , SRR].

NOTE A valid method for integrity verification could be the use of checksum.

6.2.4.10

ECSS-Q-ST-80_0720111

a. The integrity verification value shall be provided in the software configuration file with each software delivery.

EXPECTED OUTPUT: *Software configuration file [DDF, SCF; -].*

6.2.4.11

ECSS-Q-ST-80_0720112

a. For every software delivery from the supplier to the customer, the following information shall be provided as a minimum:

1. the software name;
2. the version number;
3. the reference to the software configuration file;
4. information and media in accordance with any requirements for delivery and protective security marking;
5. any annotation and caveats used to indicate or further constraint the distribution limitations.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; SRR, PDR];

b. Labels [DDF, -; -];

c. Software security management plan [SF, SSMP; SRR];

d. Protective security markings [SF,-,-].

NOTE Protective security marking, e.g. security classification, is mandated by organisational or national security regulations, policies or directives.

6.2.4.12 .

ECSS-Q-ST-80_0720320

a. Procedures shall be established for software branching and merging and the corresponding use of software configuration management tools.

EXPECTED OUTPUT: *Software configuration management plan [MGT, SCMP; SRR, PDR].*

6.2.5 Process metrics

6.2.5.1

ECSS-Q-ST-80_0720113

a. Metrics shall be used to manage the development and to assess the quality of the development processes.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR, PDR].

NOTE Process metrics are based on quality models (see clause 5.2.7).

6.2.5.2

ECSS-Q-ST-80_0720114

a. Process metrics shall be collected, stored and analysed on a regular basis by applying quality models and procedures.

EXPECTED OUTPUT: Software product assurance plan [PAF, SPAP; SRR, PDR].

6.2.5.3

ECSS-Q-ST-80_0720115

a. The following basic process metrics shall be used within the supplier's organization:

1. duration: how phases and tasks are being completed versus the planned schedule;
2. effort: how much effort is consumed by the various phases and tasks compared to the plan.

EXPECTED OUTPUT: Internal metrics report.

6.2.5.4

ECSS-Q-ST-80_0720116

a. Process metrics shall be used within the supplier's organization and reported to the customer, including:

1. number of problems detected during verification;
2. number of problems detected during integration and validation testing and use.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

NOTE See also software problem reporting described in clause 5.2.5.

6.2.5.5

ECSS-Q-ST-80_0720117

a. Metrics reports shall be included in the software product assurance reports.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

6.2.6 Verification

6.2.6.1

ECSS-Q-ST-80_0720118

a. Activities for the verification of the quality requirements shall be specified in the definition of the verification plan.

EXPECTED OUTPUT: *Software verification plan [DJF, SVerP; SRR, PDR].*

NOTE Verification includes various techniques such as review, inspection, walk-through, cross-reading, desk-checking, model simulation, and many types of analysis such as traceability analysis, formal proof or fault tree analysis.

6.2.6.2

ECSS-Q-ST-80_0720119

a. The outputs of each development activity shall be verified for conformance against pre-defined criteria.

ECSS-Q-ST-80_0720120

b. Only outputs which have been subjected to planned verifications shall be used as inputs for subsequent activities.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.2.6.3

ECSS-Q-ST-80_0720121

a. A summary of the assurance activities concerning the verification process and their findings shall be included in software product assurance reports.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.2.6.4

ECSS-Q-ST-80_0720122

a. The completion of actions related to software problem reports generated during verification shall be verified and recorded.

EXPECTED OUTPUT: *Software problem reports [DJF, -; SRR, PDR, CDR, QR, AR, ORR].*

6.2.6.5

ECSS-Q-ST-80_0720123

a. Software containing deactivated code shall be verified specifically to ensure that the deactivated code cannot be activated or that its accidental activation cannot harm the operation of the system.

EXPECTED OUTPUT: *Software verification report [DJF, SVR; CDR, QR, AR].*

6.2.6.6

ECSS-Q-ST-80_0720124

a. Software containing configurable code shall be verified specifically to ensure that any unintended configuration cannot be activated at run time or included during code generation.

EXPECTED OUTPUT: *Software verification report [DJF, SVR; CDR, QR, AR].*

6.2.6.7

ECSS-Q-ST-80_0720125

a. The supplier shall ensure that:

1. the planned verification activities are adequate to confirm that the products of each phase are conformant to the applicable requirements;
2. the verification activities are performed according to the plan.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.2.6.8

ECSS-Q-ST-80_0720126

a. Reviews and inspections shall be carried out according to defined criteria, and according to the defined level of independence of the reviewer from the author of the reviewed item.

6.2.6.9

ECSS-Q-ST-80_0720127

a. Each review and inspection shall be based on a written plan or procedure.

EXPECTED OUTPUT: *Review and inspection plans or procedures [PAF, -; -].*

NOTE For projects reviews, ECSS-E-ST-40 clause 5.3.3.3, bullet b and Annex P are applicable.

6.2.6.10

ECSS-Q-ST-80_0720128

a. The review or inspection plans or procedures shall specify:

1. the reviewed or inspected items;
2. the person in charge;
3. the participants;
4. the means of review or inspection (e.g. tools or check list);
5. the nature of the report.

EXPECTED OUTPUT: *Review and inspection plans or procedures [PAF, -; -].*

6.2.6.11

ECSS-Q-ST-80_0720129

a. Review and inspection reports shall:

1. refer to the corresponding review/inspection procedure or plan;
2. identify the reviewed item, the author, the reviewer, the review criteria and the findings of the review.

EXPECTED OUTPUT: *Review and inspection reports [PAF, -; -].*

6.2.6.12

ECSS-Q-ST-80_0720130

a. Traceability matrices (as defined in ECSS-E-ST-40 clause 5.8) shall be verified at each milestone.

EXPECTED OUTPUT: *Software product assurance milestone report [PAF, SPAMR; SRR, PDR, CDR, QR, AR, ORR].*

6.2.6.13

ECSS-Q-ST-80_0720131

a. Independent software verification shall be performed by a third party.

NOTE This requirement is applicable where the risks associated with the project justify the costs involved. The customer can consider a less rigorous level of independence, e.g. an independent team in the same organization.

ECSS-Q-ST-80_0720132

b. Independent software verification shall be a combination of reviews, inspections, analyses, simulations, and auditing.

NOTE Guidance on ISVV purpose, scope, and activities is provided in CSW-ESAISVV-2022-GBK-02897.

ECSS-Q-ST-80_0720321

c. Independent software verification shall be performed in addition to, and shall not fully or partly replace, verification activities to be carried out by the supplier in accordance with ECSS-E-ST-40, clause 5.8.

EXPECTED OUTPUT: *The following outputs are expected:*

a. ISVV plan [DJF, -; SRR, PDR];

b. ISVV report [DJF, -; PDR, CDR, QR, AR].

6.2.7 Reuse of existing software

6.2.7.1 General

The requirements in 6.2.7 do not apply to tools and software development environment, for which requirements of clause 5.6 apply.

6.2.7.2

ECSS-Q-ST-80_0720133

a. Analyses of the advantages to be obtained with the selection of existing software (ref. 3.2.10) instead of new development shall be carried out.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software reuse approach, including approach to delta qualification [PAF, SPAP; SRR, PDR];

b. Software reuse file [DJF, SRF; SRR, PDR].

6.2.7.3

ECSS-Q-ST-80_0720134

a. The existing software shall be assessed with regards to the applicable functional, performance and quality requirements.

ECSS-Q-ST-80_0720322

b. The existing software shall be assessed with regards to the applicable security requirements, addressing the following aspects:

1. Authorisation for use;
2. Security sensitivity;
3. Security assurance requirements;
4. Security evaluations, certifications and accreditations.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software reuse approach, including approach to delta qualification [PAF, SPAP; SRR, PDR];

b. Software reuse file [DJF, SRF; SRR, PDR].

NOTE For example, Common Criteria (CC), FIPS, system accreditation, council approval.

6.2.7.4

ECSS-Q-ST-80_0720135

a. The quality level of the existing software shall be analysed with respect to the project requirements, according to the criticality and sensitivity of the system function implemented, taking into account the following aspects:

1. software requirements documentation;
2. software architectural and detailed design documentation;
3. forward and backward traceability between system requirements, software requirements, design and code;
4. unit tests documentation and coverage;
5. integration tests documentation and coverage;
6. validation documentation and coverage;

7. verification reports;
8. performance;
9. operational performances;
10. residual nonconformances, waivers; and alerts;
11. user operational documentation;
12. code quality (adherence to coding standards, metrics);
13. known security vulnerabilities in the reused product, including vulnerabilities introduced by dependencies at all levels between components.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software reuse approach, including approach to delta qualification [PAF, SPAP; SRR, PDR];

b. Software reuse file [DJF, SRF; SRR, PDR].

NOTE 1 Examples of performance are memory occupation, CPU load.

NOTE 2 Example of user operation documentation is a user manual.

6.2.7.5

ECSS-Q-ST-80_0720136

a. The results of the reused software analysis shall be recorded in the software reuse file, together with an assessment of the possible level of reuse and a description of the assumptions and the methods applied when estimating the level of reuse.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software reuse approach, including approach to delta qualification [PAF, SPAP; SRR, PDR];

b. Software reuse file [DJF, SRF; SRR, PDR].

NOTE Results of the reused software analysis, such as detailed reference to requirement and design documents, test reports and coverage results.

6.2.7.6

ECSS-Q-ST-80_0720137

a. The analysis of the suitability of existing software for reuse shall be complemented by an assessment of the following aspects:

1. the acceptance and warranty conditions;
2. the available support documentation;
3. the conditions of installation, preparation, training and use;
4. the identification and registration by configuration management;
5. maintenance responsibility and conditions, including the possibilities of changes;
6. the durability and validity of methods and tools used in the initial development, that are envisaged to be used again;

7. the copyright and intellectual property rights constraints (modification rights);
8. the licensing conditions;
9. exportability constraints.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; SRR, PDR].*

6.2.7.7

ECSS-Q-ST-80_0720138

a. Corrective actions shall be identified, documented in the reuse file and applied to the reused software not meeting the applicable requirements related to the aspects as specified in clauses 6.2.7.2 to 6.2.7.6.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; SRR, PDR].*

6.2.7.8

ECSS-Q-ST-80_0720139

a. Reverse engineering techniques shall be applied to generate missing documentation and to reach the required verification and validation coverage.

ECSS-Q-ST-80_0720140

b. For software products whose life cycle data from previous development are not available and reverse engineering techniques are not fully applicable, the following methods shall be applied:
   1. generation of validation and verification documents based on the available user documentation (e.g. user manual) and execution of tests in order to achieve the required level of test coverage;
   2. use of the product service history to provide evidence of the product's suitability for the current application, including information about:
      (a) relevance of the product service history for the new operational environment;
      (b) configuration management and change control of the software product;
      (c) effectiveness of problem reporting;
      (d) actual error rates and maintenance records;
      (e) impact of modifications;
      (f) number, types, priorities and correction rates of vulnerabilities.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; SRR, PDR].*

6.2.7.9

ECSS-Q-ST-80_0720141

a. The software reuse file shall be updated at project milestones to reflect the results of the identified corrective actions for reused software not meeting the project requirements.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; CDR, QR, AR].*

6.2.7.10

ECSS-Q-ST-80_0720142

a. All the reused software shall be kept under configuration control.

6.2.7.11

ECSS-Q-ST-80_0720143

a. The detailed configuration status of the reused software baseline shall be provided to the customer in the reuse file for acceptance.

EXPECTED OUTPUT: *Software reuse file [DJF, SRF; SRR, PDR, CDR, QR, AR].*

6.2.8 Automatic code generation

6.2.8.1

ECSS-Q-ST-80_0720144

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

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 standards;
3. portability requirements for the generated code;
4. collection of the required design and code metrics;
5. verification of software components containing generated code;
6. configuration control of the tools including the parameters for customisation;
7. compliance with open standards.

NOTE Examples for item 1: compilers or code management systems.

6.2.8.2

ECSS-Q-ST-80_0720145

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

EXPECTED OUTPUT: *Validation and testing documentation [DJF, SValP; PDR], [DJF, SVS; CDR, QR, AR], [DJF, SUITP; PDR, CDR].*

6.2.8.3

ECSS-Q-ST-80_0720146

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

6.2.8.4

ECSS-Q-ST-80_0720147

a. Modelling standards for automatic code generation tools shall be defined and applied.

EXPECTED OUTPUT: *Modelling standards [PAF, -; SRR, PDR].*

6.2.8.5

ECSS-Q-ST-80_0720148

a. Adherence to modelling standards shall be verified.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.2.8.6

ECSS-Q-ST-80_0720149

a. Clause 6.3.4 shall apply to automatically generated code, unless the supplier demonstrates that the automatically generated code does not need to be manually modified.

6.2.8.7

ECSS-Q-ST-80_0720150

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

EXPECTED OUTPUT: *Validation and testing documentation [DJF, SValP; PDR], [DJF, SVS; CDR, QR, AR], [DJF, SUITP; PDR, CDR].*

6.2.9 Software security

6.2.9.1 .

ECSS-Q-ST-80_0720323

a. The software product assurance plan shall include security assurance.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR, CDR].*

6.2.9.2 .

ECSS-Q-ST-80_0720324

a. The supplier shall perform a software security analysis of the software products, using the results of system-level security analyses, where software products are part of a system, in order to determine the sensitivity of the individual software components.

EXPECTED OUTPUT: *Software security analysis report [SF, -; PDR].*

6.2.9.3 .

ECSS-Q-ST-80_0720325

a. The supplier shall identify the methods and techniques for the software security analysis.

ECSS-Q-ST-80_0720326

b. Methods and techniques for software security analysis shall be agreed between the supplier and customer.

NOTE Examples of software security analysis are: Requirements analysis, security risk analysis, design analysis and code analysis.

6.2.9.4 .

ECSS-Q-ST-80_0720327

a. Based on the results of the software security analysis, the supplier shall apply engineering measures to reduce the number of security sensitive software components and mitigate the risks associated with security sensitive software (ref. clause 6.2.10).

6.2.9.5 .

ECSS-Q-ST-80_0720328

a. The supplier shall report on the status of the implementation and verification of the software security analysis recommendations.

EXPECTED OUTPUT: Software security analysis report [SF, -; CDR, QR, AR]

6.2.9.6 .

ECSS-Q-ST-80_0720329

a. The supplier shall update the software security analysis at each software development milestone, to confirm the security sensitivity and related security risks of software components.

EXPECTED OUTPUT: Software security analysis report [SF, -; CDR, QR, AR].

6.2.9.7 .

ECSS-Q-ST-80_0720330

a. The supplier shall provide the results of the software security analysis for integration into the system-level security analyses, addressing in particular:

1. additional security failure modes or vulnerabilities identified at software level;
2. recommendations for system-level security activities and changes to the system including requirements

EXPECTED OUTPUT: Software security analysis report [SF, -; PDR, CDR].

6.2.10 Handling of security sensitive software

6.2.10.1 .

ECSS-Q-ST-80_0720331

a. The supplier shall define and implement measures to avoid propagation of failures, including the ones caused by deliberate action, between software components.

NOTE This can be achieved by design measures such as separate hardware platforms, fail secure isolation of software processes or prohibition of shared memory (segregation and partitioning).

ECSS-Q-ST-80_0720332

b. The consequences for security of the malfunction of higher criticality components, and the consequences for safety and dependability of the malfunction of higher sensitivity components shall be analysed and any conflict resolved.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software dependability and safety analysis report [PAF, -; PDR, CDR, QR, AR];

b. Software security analysis report [SF, -; PDR, CDR, QR, AR].

6.2.10.2 .

ECSS-Q-ST-80_0720333

a. For security sensitive software, measures shall be defined, justified and applied, in addition to those in clause 6.2.3.2.

EXPECTED OUTPUT: *Software security management plan [SF, , SSMP;; PDR, CDR, QR, AR].*

NOTE These measures can include:

- use of secure coding practices;
- use of security baseline(s);
- use of fuzzing, static, dynamic security testing;
- use of vulnerability assessment and penetration testing.

6.2.10.3 .

ECSS-Q-ST-80_0720334

a. Security sensitive software shall be subject to regression testing after:

1. any change of functionality of the underlying platform hardware;
2. any change of the tools that affect directly or indirectly the generation of the executable code;
3. any change in the security of the target operating environment.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; PDR, CDR];

b. Software security management plan [SF, SSMP; PDR, CDR].

NOTE 1 This can be the result of changing security characteristics of the existing environment. Alternatively, this can be due to the migration of the software from one operating environment to another.

NOTE 2 In case of minor changes in tools that affect the generation of the executable code, a binary comparison of the executable code generated by the different tools can be used to verify that no modifications are introduced.

NOTE 3 Example for item 1: instruction set of a processor.

6.2.10.4 .

ECSS-Q-ST-80_0720335

a. The need for additional V&V of security sensitive software shall be analysed after:

1. any change of functionality or performance of the underlying platform hardware;
2. any change in the environment in which the software or the platform hardware operate;
3. any change in knowledge of security threats, security vulnerabilities or security sensitivity of the system;
4. any change in the infrastructure and tools used to build environment.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; PDR, CDR];

b. Software security management plan [SF, SSMP; PDR, CDR].

6.3 Requirements applicable to individual software engineering processes or activities

6.3.1 Software related system requirements process

6.3.1.1

ECSS-Q-ST-80_0720151

a. For the definition of the software related system requirements to be specified in the requirements baseline, ECSS-E-ST-40 clause 5.2 shall apply.

6.3.1.2

ECSS-Q-ST-80_0720152

a. The requirements baseline shall be subject to documentation control and configuration management as part of the development documentation.

6.3.1.3

ECSS-Q-ST-80_0720153

a. For the definition of the requirements baseline, all results from the safety and dependability analyses (including results from the HSIA ECSS-Q-ST-30 clause 6.4.2.3) shall be used.

ECSS-Q-ST-80_0720336

b. For the definition of the requirements baseline, all results from the security analysis shall be used.

6.3.2 Software requirements analysis

6.3.2.1

ECSS-Q-ST-80_0720154

a. The requirements baseline shall be analyzed to fully and unambiguously define the software requirements in the technical specification.

6.3.2.2

ECSS-Q-ST-80_0720155

a. The technical specification shall be subject to documentation control and configuration management as part of the development documentation.

6.3.2.3

ECSS-Q-ST-80_0720156

a. For the definition of the technical specification, all results from the safety and dependability analyses (including results from the HSIA ECSS-Q-ST-30 clause 6.4.2.3) shall be used.

ECSS-Q-ST-80_0720337

b. For the definition of the technical specification, all results from the software security analysis shall be used.

6.3.2.4

ECSS-Q-ST-80_0720157

a. In addition to the functional requirements, the technical specification shall include all non-functional requirements necessary to satisfy the requirements baseline, including, as a minimum, the following:

1. performance,
2. safety,
3. reliability,
4. robustness,
5. quality,
6. maintainability,
7. configuration management,

8. security,
9. privacy,
10. metrication, and
11. verification and validation.

EXPECTED OUTPUT: *Software requirements specification [TS, SRS; PDR].*

NOTE Performance requirements include requirements on numerical accuracy.

6.3.2.5

ECSS-Q-ST-80_0720158

a. Prior to the technical specification elaboration, customer and supplier shall agree on the following principles and rules as a minimum:
   1. assignment of persons (on both sides) responsible for establishing the technical specification;
   2. methods and tools for agreeing on requirements and approving changes;
   3. efforts to prevent misunderstandings such as definition of terms, explanations of background of requirements;
   4. recording and reviewing discussion results on both sides.

6.3.3 Software architectural design and design of software items

6.3.3.1

ECSS-Q-ST-80_0720159

a. The design definition file shall be subject to documentation control and configuration management.

6.3.3.2

ECSS-Q-ST-80_0720160

a. Mandatory and advisory design standards shall be defined and applied.

EXPECTED OUTPUT: *Design standards [PAF, -; SRR, PDR].*

6.3.3.3

ECSS-Q-ST-80_0720161

a. For software in which numerical accuracy is relevant to mission success specific rules on design and code shall be defined to ensure that the specified level of accuracy is obtained.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

NOTE For example: for an attitude and orbit control subsystem, scientific data generation components.

6.3.3.4

ECSS-Q-ST-80_0720162

a. Adherence to design standards shall be verified.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.3.3.5

ECSS-Q-ST-80_0720163

a. The supplier shall define means, criteria and tools to ensure that the complexity and modularity of the design meet the quality requirements.

ECSS-Q-ST-80_0720164

b. The design evaluation shall be performed in parallel with the design process, in order to provide feedback to the software design team.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

6.3.3.6

ECSS-Q-ST-80_0720165

a. Synthesis of the results obtained in the software complexity and modularity evaluation and corrective actions implemented shall be described in the software product assurance reports.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.3.3.7

ECSS-Q-ST-80_0720166

a. The supplier shall review the design documentation to ensure that it contains the appropriate level of information for maintenance activities.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; PDR];

b. Software product assurance reports [PAF, -; -].

6.3.4 Coding

6.3.4.1

ECSS-Q-ST-80_0720167

a. Coding standards (including security, consistent naming conventions and adequate commentary rules) shall be specified and observed.

EXPECTED OUTPUT: *Coding standards [PAF, -; PDR].*

6.3.4.2

ECSS-Q-ST-80_0720168

a. The standards shall be consistent with the product quality requirements.

EXPECTED OUTPUT: *Coding standards [PAF, -; PDR].*

NOTE Coding standards depend on the software quality objectives (see clause 5.2.7).

6.3.4.3

ECSS-Q-ST-80_0720169

a. The tools to be used in implementing and checking conformance with coding standards shall be identified in the product assurance plan before coding activities start.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

6.3.4.4

ECSS-Q-ST-80_0720170

a. Coding standards shall be reviewed with the customer to ensure that they reflect product quality and security requirements.

EXPECTED OUTPUT: *Coding standards and description of tools [PAF, -; PDR].*

6.3.4.5

ECSS-Q-ST-80_0720171

a. Use of low-level programming languages shall be justified.

EXPECTED OUTPUT: *Software development plan [MGT, SDP; PDR].*

6.3.4.6

ECSS-Q-ST-80_0720172

a. The supplier shall define measurements, criteria and tools to ensure that the software code meets the quality and security requirements.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

ECSS-Q-ST-80_0720173

b. The code evaluation shall be performed in parallel with the coding process, in order to provide feedback to the software programmers.

6.3.4.7

ECSS-Q-ST-80_0720174

a. Synthesis of the code analysis results and corrective actions implemented shall be described in the software product assurance reports.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.3.4.8

ECSS-Q-ST-80_0720175

a. The code shall be put under configuration control immediately after successful unit testing.

6.3.5 Testing and validation

6.3.5.1

ECSS-Q-ST-80_0720176

a. Testing shall be performed in accordance with a strategy for each testing level (i.e. unit, integration, validation against the technical specification, validation against the requirements baseline, acceptance), which includes:
   1. the types of tests to be performed;
   2. the tests to be performed in accordance with the plans and procedures;
   3. the means and organizations to perform assurance function for testing and validation.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR, CDR].*

NOTE For examples for item 1 are: functional, boundary, performance, security, and usability tests.

6.3.5.2

ECSS-Q-ST-80_0720177

a. Based on the dependability and safety criticality, and the security sensitivity of the software, test coverage goals for each testing level shall be agreed between the customer and the supplier and their achievement monitored by metrics:
   1. for unit level testing;
   2. for integration level testing;
   3. for validation against the technical specification and validation against the requirements baseline.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR, CDR].*

6.3.5.3

ECSS-Q-ST-80_0720178

a. The supplier shall ensure through internal review that the test procedures and data are adequate, feasible and traceable and that they satisfy the requirements.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.3.5.4

ECSS-Q-ST-80_0720179

a. Test readiness reviews shall be held before the commencement of test activities, as defined in the software development plan.

EXPECTED OUTPUT: *Test readiness review reports [DJF, -; TRR].*

6.3.5.5

ECSS-Q-ST-80_0720180

a. Test coverage shall be checked with respect to the stated goals.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

ECSS-Q-ST-80_0720181

b. Feedback from the results of test coverage evaluation shall be continuously provided to the software developers.

6.3.5.6

ECSS-Q-ST-80_0720182

a. The supplier shall ensure that nonconformances and software problem reports detected during testing are properly documented and reported to those concerned.

EXPECTED OUTPUT: *Nonconformance reports and software problem reports [DJF, -; CDR, QR, AR, ORR].*

6.3.5.7

ECSS-Q-ST-80_0720183

a. The test coverage of configurable code shall be checked to ensure that the stated requirements are met in each tested configuration.

EXPECTED OUTPUT: *Statement of compliance with test plans and procedures [PAF, -; CDR, QR, AR, ORR].*

6.3.5.8

ECSS-Q-ST-80_0720184

a. The completion of actions related to software problem reports generated during testing and validation shall be verified and recorded.

EXPECTED OUTPUT: *Software problem reports [DJF, -; SRR, PDR, CDR, QR, AR, ORR].*

6.3.5.9

ECSS-Q-ST-80_0720185

a. Provisions shall be made to allow witnessing of tests by the customer.

6.3.5.10

ECSS-Q-ST-80_0720186

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

NOTE For example: specialist software product assurance personnel.

6.3.5.11

ECSS-Q-ST-80_0720187

a. The supplier shall ensure that:

1. tests are conducted in accordance with approved test procedures and data,

2. the configuration under test is correct,
3. the tests are properly documented, and
4. the test reports are up to date and valid.

EXPECTED OUTPUT: *Statement of compliance with test plans and procedures [PAF, -; CDR, QR, AR, ORR].*

6.3.5.12

ECSS-Q-ST-80_0720188

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

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

6.3.5.13

ECSS-Q-ST-80_0720189

a. The supplier shall confirm in writing that the tests are successfully completed.

EXPECTED OUTPUT: *Testing and validation reports [DJF, -; CDR, QR, AR, ORR].*

6.3.5.14

ECSS-Q-ST-80_0720190

a. Review boards looking to engineering and product assurance aspects shall be convened after the completion of test phases, as defined in the software development plan.

ECSS-Q-ST-80_0720338

b. Review boards looking to security aspects shall be convened after the completion of test phases, as defined in the software security management plan.

6.3.5.15

ECSS-Q-ST-80_0720191

a. Areas affected by any modification shall be identified and re-tested (regression testing).

6.3.5.16

ECSS-Q-ST-80_0720192

a. In case of re-testing, all test related documentation (test procedures, data and reports) shall be updated accordingly.

EXPECTED OUTPUT: *Updated test documentation [DJF, -; CDR, QR, AR, ORR].*

6.3.5.17

ECSS-Q-ST-80_0720193

a. The need for regression testing and additional verification of the software shall be analysed after any change of the platform hardware.

EXPECTED OUTPUT: *Updated test documentation [DJF, -; CDR, QR, AR, ORR].*

6.3.5.18

ECSS-Q-ST-80_0720194

a. The need for regression testing and additional verification of the software shall be analysed after a change or update of any tool used to generate it.

EXPECTED OUTPUT: *Updated test documentation [DJF, -; CDR, QR, AR, ORR].*

NOTE For example: source code or object code.

6.3.5.19

ECSS-Q-ST-80_0720195

a. Validation shall be carried out by staff who have not taken part in the design or coding of the software being validated.

NOTE This can be achieved at the level of the whole software product, or on a component by component basis.

6.3.5.20

ECSS-Q-ST-80_0720196

a. Validation of the flight software against the requirement baseline on the flight equipment model shall be performed on a software version without any patch.

6.3.5.21

ECSS-Q-ST-80_0720197

a. The supplier shall review the test documentation to ensure that it is up to date and organized to facilitate its reuse for maintenance.

6.3.5.22

ECSS-Q-ST-80_0720198

a. Tests shall be organized as activities in their own right in terms of planning, resources and team composition.

EXPECTED OUTPUT: *Test and validation documentation [DJF, SValP; PDR], [DJF, SUITP; PDR, CDR].*

6.3.5.23

ECSS-Q-ST-80_0720199

a. The necessary resources for testing shall be identified early in the life cycle, taking into account the operating and maintenance requirements.

EXPECTED OUTPUT: *Test and validation documentation [DJF, SValP; PDR], [DJF, SUITP; PDR, CDR].*

6.3.5.24

ECSS-Q-ST-80_0720200

a. Test tool development or acquisition (hardware and software) shall be planned for in the overall project plan.

EXPECTED OUTPUT: *Test and validation documentation [DJF, SValP; PDR], [DJF, SUITP; PDR, CDR].*

6.3.5.25

ECSS-Q-ST-80_0720201

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

EXPECTED OUTPUT: *Test and validation documentation [DJF, SValP; PDR], [DJF, SVS; CDR, QR, AR], [DJF, SUITP; PDR, CDR].*

6.3.5.26

ECSS-Q-ST-80_0720202

a. Before offering the product for delivery and customer acceptance, the supplier shall validate its operation as a complete product, under conditions similar to the application environment as specified in the requirements baseline.

6.3.5.27

ECSS-Q-ST-80_0720203

a. When testing under the operational environment is performed, the following concerns shall be addressed:

1. the features to be tested in the operational environment;
2. the specific responsibilities of the supplier and customer for carrying out and evaluating the test;
3. restoration of the previous operational environment (after test).

EXPECTED OUTPUT: *Test and validation documentation [DJF, -; AR].*

6.3.5.28

ECSS-Q-ST-80_0720204

a. Independent software validation shall be performed by a third party.

NOTE This requirement is applicable where the risks associated with the project justify the costs involved. The customer can consider a less rigorous level of independence, e.g. an independent team in the same organization.

ECSS-Q-ST-80_0720339

b. Independent software validation shall be performed in addition to, and not fully or partly replace, validation activities to be carried out by the supplier in accordance with ECSS-E-ST-40, clause 5.6.

EXPECTED OUTPUT: *The following outputs are expected:*

a. ISVV plan [DJF, -; SRR, PDR];

b. ISVV report [DJF, -; PDR, CDR, QR, AR].

NOTE Guidance on ISVV purpose, scope, and activities is provided in CSW-ESAISVV-2022-GBK-02897.

6.3.5.29

ECSS-Q-ST-80_0720205

a. 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.

EXPECTED OUTPUT: *Test and validation documentation [DJF, SValP; PDR], [DJF, SVS; CDR, QR, AR].*

6.3.5.30

ECSS-Q-ST-80_0720206

a. Software containing deactivated code shall be validated specifically to ensure that the deactivated code cannot be activated or that its accidental activation cannot harm the operation of the system.

EXPECTED OUTPUT: *Testing and validation reports [DJF, -; CDR, QR, AR].*

6.3.5.31

ECSS-Q-ST-80_0720207

a. Software containing configurable code shall be validated specifically to ensure that unintended configuration cannot be activated at run time or included during code generation.

EXPECTED OUTPUT: *Testing and validation reports [DJF, -; CDR, QR, AR].*

6.3.5.32

ECSS-Q-ST-80_0720208

a. Activities for the validation of the quality requirements shall be specified in the definition of the validation specification.

EXPECTED OUTPUT: *Software validation specification [DJF, SVS; CDR, QR, AR].*

6.3.5.33 .

ECSS-Q-ST-80_0720340

a. The software validation control information, as specified in clause 5.6.5 of ECSS-E-ST-40, shall be reviewed by the supplier and made available to the customer at milestone reviews.

EXPECTED OUTPUT: *Software validation control information [DJF, -; CDR, QR, AR].*

NOTE This information is expected to be provided in electronic format.

6.3.6 Software delivery and installation

6.3.6.1 .

ECSS-Q-ST-80_0720341

a. The Delivery Review Board convened for software deliveries, as specified in clause 5.3.5.3 of ECSS-E-ST-40, shall include a representative from the software product assurance and the software engineering organizations.

ECSS-Q-ST-80_0720342

b. The software product assurance reporting to be provided to the Delivery Review Board, including product metrics measurement results, shall be defined based on delivery's purpose and scope.

6.3.6.2

ECSS-Q-ST-80_0720209

a. The roles, responsibilities and obligations of the supplier and customer during installation shall be established.

EXPECTED OUTPUT: Installation procedure [DDF, SCF; AR].

6.3.6.3 .

ECSS-Q-ST-80_0720343

a. The customer shall verify that the executable code was regenerated from configuration managed source code components and installed in accordance with predefined procedures on the target environment.

6.3.6.4

ECSS-Q-ST-80_0720210

a. The installation shall be performed in accordance with the installation procedure.

6.3.7 Software acceptance

6.3.7.1

ECSS-Q-ST-80_0720211

a. The customer shall establish an acceptance test plan specifying the intended acceptance tests including specific tests suited to the target environment (see ECSS-E-ST-40 clause 5.7.3.1).

EXPECTED OUTPUT: Acceptance test plan [DJF, -; QR, AR].

NOTE 1 The acceptance tests can be partly made up of tests used during previous test activities.

NOTE 2 The acceptance test plan takes into account the requirement for operational demonstration, either as part of acceptance or after acceptance.

ECSS-Q-ST-80_0720344

b. The customer shall confirm whether the residual security risks are acceptable.

EXPECTED OUTPUT: Joint review report [DJF, -; AR].

NOTE The confirmation could be based on acceptance testing and other software analysis techniques: for example, analysis and penetration testing.

6.3.7.2

ECSS-Q-ST-80_0720212

a. The customer shall ensure that the acceptance tests are performed in accordance with the approved acceptance test plan (see ECSS-E-ST-40 clause 5.7.3.2).

6.3.7.3

ECSS-Q-ST-80_0720213

a. Before the software is presented for customer acceptance, the supplier shall ensure that:
   1. the delivered software complies with the contractual requirements (including any specified content of the software acceptance data package);
   2. the source and object code supplied correspond to each other;
   3. all agreed changes are implemented;
   4. all nonconformances are either resolved or declared.

6.3.7.4

ECSS-Q-ST-80_0720214

a. <<deleted>>

6.3.7.5

ECSS-Q-ST-80_0720215

a. Any discovered problems shall be documented in nonconformance reports.

   EXPECTED OUTPUT: Nonconformance reports [DJF, -; AR].

6.3.7.6

ECSS-Q-ST-80_0720216

a. On completion of the acceptance tests, a report shall be drawn up and be signed by the supplier's representatives, the customer's representatives, the software quality engineers of both parties and the representative of the organization charged with the maintenance of the software product.

   EXPECTED OUTPUT: Acceptance test report [DJF, -; AR].

6.3.7.7

ECSS-Q-ST-80_0720217

a. The customer shall certify conformance to the procedures and state the conclusion concerning the test result for the software product under test (accepted, conditionally accepted, rejected).

   EXPECTED OUTPUT: Acceptance test report [DJF, -; AR].

6.3.8 Operations

6.3.8.1

ECSS-Q-ST-80_0720218

a. During operations, the quality of the mission products related to software shall be agreed with the customer and users.

EXPECTED OUTPUT: Software operation support plan [OP, -; ORR].

NOTE Quality of mission products can include parameters such as: error-free data, availability of data and permissible outages; permissible information degradation.

6.3.8.2

ECSS-Q-ST-80_0720219

a. During the demonstration that the software conforms to the operational requirements, the following shall be covered as a minimum:

1. availability and maintainability of the host system (including reboot after maintenance interventions);
2. safety features;
3. human-computer interface;
4. operating procedures;
5. ability to meet the mission product quality requirements.

EXPECTED OUTPUT: Validation of the operational requirements [PAF, -; ORR].

NOTE Operating procedures can include specific security operating procedures (SECOPS).

6.3.8.3

ECSS-Q-ST-80_0720220

a. The product assurance plan for system operations shall include consideration of software.

EXPECTED OUTPUT: Input to product assurance plan for systems operation [PAF, -; ORR]

6.3.9 Maintenance

6.3.9.1

ECSS-Q-ST-80_0720221

a. The organization responsible for maintenance shall be identified to allow a smooth transition into the operations and maintenance.

EXPECTED OUTPUT: Maintenance plan [MF, -; QR, AR, ORR].

NOTE An organization, with representatives from both supplier and customer, can be set up to support the maintenance activities. Attention is drawn to the importance of the flexibility of this organization to cope with the unexpected

occurrence of problems and the identification of facilities and resources to be used for the maintenance activities.

6.3.9.2

ECSS-Q-ST-80_0720222

a. The maintenance organization shall specify the assurance, verification, validation and security analysis activities applicable to maintenance interventions.

EXPECTED OUTPUT: Maintenance plan [MF, -; QR, AR, ORR].

6.3.9.3

ECSS-Q-ST-80_0720223

a. The maintenance plans shall be verified against specified requirements for maintenance of the software product.

NOTE The maintenance plans and procedures can address corrective, improving, adaptive and preventive maintenance, differentiating between "routine" and "emergency" maintenance activities.

6.3.9.4

ECSS-Q-ST-80_0720224

a. The maintenance plans and procedures shall include the following as a minimum:

1. scope of maintenance;
2. identification of the first version of the software product for which maintenance is to be done;
3. support organization;
4. maintenance life cycle;
5. maintenance activities;
6. quality measures to be applied during the maintenance;
7. security measures to be applied during the maintenance.
8. maintenance records and reports.

EXPECTED OUTPUT: Maintenance plan [MF, -; QR, AR, ORR].

6.3.9.5

ECSS-Q-ST-80_0720225

a. Rules for the submission of maintenance reports shall be established and agreed as part of the maintenance plan.

EXPECTED OUTPUT: Maintenance plan [MF, -; QR, AR, ORR].

6.3.9.6

ECSS-Q-ST-80_0720226

a. All maintenance activities shall be logged in predefined formats and retained.

EXPECTED OUTPUT: Maintenance records [MF, -; -].

6.3.9.7

ECSS-Q-ST-80_0720227

a. Maintenance records shall be established for each software product, including, as a minimum, the following information,:

1. list of requests for assistance or problem reports that have been received and the current status of each;
2. security related aspects of requests for assistance or problem reports and the current status of each;
3. organization responsible for responding to requests for assistance or implementing the appropriate corrective actions;
4. priorities assigned to the corrective actions;
5. results of the corrective actions;
6. statistical data on failure occurrences and maintenance activities.

EXPECTED OUTPUT: Maintenance records [MF, -; -].

NOTE 1 The record of the maintenance activities can be utilized for evaluation and enhancement of the software product and for improvement of the quality system itself.

NOTE 2 Related to item 2, problem reports include evidence of specific security issues (for example data leakage and presence of malware) and incident description while preserving the privacy of the case.

7
Software product quality assurance

7.1 Product quality objectives and metrication

7.1.1 Deriving of requirements

ECSS-Q-ST-80_0720228

a. The software quality requirements (including security, safety and dependability requirements) shall be derived from the requirements defined at system level.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Requirement baseline [RB, SSS; SRR];

b. Technical specification [TS, SRS; PDR].

7.1.2 Quantitative definition of quality requirements

ECSS-Q-ST-80_0720229

a. Quality requirements shall be expressed in quantitative terms or constraints.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Requirement baseline [RB, SSS; SRR];

b. Technical specification [TS, SRS; PDR].

7.1.3 Assurance activities for product quality requirements

ECSS-Q-ST-80_0720230

a. The supplier shall define assurance activities to ensure that the product meets the quality requirements as specified in the technical specification.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

7.1.4 Product metrics

ECSS-Q-ST-80_0720231

a. In order to verify the implementation of the product quality requirements, the supplier shall define a metrication programme based on the identified quality model (see clause 5.2.7), specifying:

1. the metrics to be collected and stored;
2. the means to collect metrics (measurements);
3. the target values, with reference to the product quality requirements;

4. the analyses to be performed on the collected metrics, including the ones to derive:
   (a) descriptive statistics;
   (b) trend analysis (such as trends in software problems).
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 software life cycle.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

NOTE 1 Guidance for software metrication programme implementation can be found in ECSS-Q-HB-80-04.

NOTE 2 Example to item 4(a): the number of units at each level of complexity.

7.1.5 Basic metrics

ECSS-Q-ST-80_0720232

a. The following basic products metrics shall be used:
   1. size (code);
   2. complexity (design, code);
   3. fault density and failure intensity;
   4. test coverage;
   5. number of failures.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; SRR, PDR].*

7.1.6 Reporting of metrics

ECSS-Q-ST-80_0720233

a. The results of metrics collection and analysis shall be included in the software product assurance reports, in order to provide the customer with an insight into the level of quality obtained.

EXPECTED OUTPUT: *Software product assurance reports [PAF, -; -].*

7.1.7 Numerical accuracy

ECSS-Q-ST-80_0720234

a. Numerical accuracy shall be estimated and verified.

EXPECTED OUTPUT: *Numerical accuracy analysis [DJF, SVR; PDR, CDR, QR].*

7.1.8 Analysis of software maturity

ECSS-Q-ST-80_0720235

a. The supplier shall define the organization and means implemented to collect and analyse data required for the study of software maturity.

EXPECTED OUTPUT: Software product assurance reports [PAF, -; -].

NOTE For example: failures, corrections, duration of runs.

7.2 Product quality requirements

7.2.1 Requirements baseline and technical specification

7.2.1.1

ECSS-Q-ST-80_0720236

a. The software quality requirements shall be documented in the requirements baseline and technical specification.

EXPECTED OUTPUT: The following outputs are expected:

a. Requirement baseline [RB, SSS; SRR];

b. Technical specification [TS, SRS; PDR].

7.2.1.2

ECSS-Q-ST-80_0720237

a. The software requirements shall be:

1. correct;
2. unambiguous;
3. complete;
4. consistent;
5. verifiable;
6. traceable.

7.2.1.3

ECSS-Q-ST-80_0720238

a. For each requirement the method for verification and validation shall be specified.

EXPECTED OUTPUT: The following outputs are expected:

a. Requirement baseline [RB, SSS; SRR];

b. Technical specification [TS, SRS; PDR].

7.2.2 Design and related documentation

7.2.2.1

ECSS-Q-ST-80_0720239

a. The software design shall meet the non-functional requirements as documented in the technical specification.

7.2.2.2

ECSS-Q-ST-80_0720240

a. The software shall be designed to facilitate testing.

7.2.2.3

ECSS-Q-ST-80_0720241

a. Software with a long planned lifetime shall be designed with minimum dependency on the operating system and the hardware, in order to aid portability.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Software product assurance plan [PAF, SPAP; SRR, PDR];

b. Justification of design choices [DDF, SDD; PDR, CDR].

NOTE This requirement is applicable to situations where the software lifetime can lead to the obsolescence and non-availability of the original operating system and/or hardware, thereby jeopardizing the maintainability of the software.

7.2.3 Test and validation documentation

7.2.3.1

ECSS-Q-ST-80_0720242

a. Detailed test and validation documentation (data, procedures and expected results) defined in the ECSS-E-ST-40 DJF shall be consistent with the defined test and validation strategy (see clause 6.3.5 and ECSS-E-ST-40 clauses 5.5.3, 5.5.4, 5.6 and 5.8).

7.2.3.2

ECSS-Q-ST-80_0720243

a. The test documentation shall cover the test environment, tools and test software, personnel required and associated training requirements.

7.2.3.3

ECSS-Q-ST-80_0720244

a. The criteria for completion of each test and any contingency steps shall be specified.

7.2.3.4

ECSS-Q-ST-80_0720245

a. Test procedures, data and expected results shall be specified.

7.2.3.5

ECSS-Q-ST-80_0720246

a. The hardware and software configuration shall be identified and documented as part of the test documentation.

7.2.3.6

ECSS-Q-ST-80_0720247

a. For any requirements not covered by testing a verification report shall be drawn up documenting or referring to the verification activities performed.

EXPECTED OUTPUT: *Software verification report [DJF, SVR; CDR, QR, AR].*

7.3 Software intended for reuse

7.3.1 Customer requirements

ECSS-Q-ST-80_0720248

a. For the development of software intended for reuse, ECSS-E-ST-40 clauses 5.2.4.7 and 5.4.3.6 shall apply.

7.3.2 Separate documentation

ECSS-Q-ST-80_0720249

a. The information related to the components developed for reuse shall be separated from the others in the technical specification, design justification file, design definition file and product assurance file.

7.3.3 Self-contained information

ECSS-Q-ST-80_0720250

a. The information related to components developed for reuse in the technical specification, the design justification file, the design definition file and the product assurance file shall be self-contained.

7.3.4 Requirements for intended reuse

ECSS-Q-ST-80_0720251

a. The technical specification of components developed for reuse shall include requirements for maintainability, portability and verification of those components.

EXPECTED OUTPUT: *Technical specification for reusable components [TS, -; PDR].*

7.3.5 Configuration management for intended reuse

ECSS-Q-ST-80_0720252

a. The configuration management system shall include provisions for handling specific aspects of software 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 software.

EXPECTED OUTPUT: *Software configuration management plan [MGT, SCMP; SRR, PDR].*

7.3.6 Testing on different platforms

ECSS-Q-ST-80_0720253

a. Where the components developed for reuse are developed to be reusable on different platforms, the testing of the software shall be performed on all those platforms.

EXPECTED OUTPUT: *Verification and validation documentation for reusable components [DJF, -; CDR].*

7.3.7 Certificate of conformance

ECSS-Q-ST-80_0720254

a. The supplier shall provide a certificate of conformance that the tests have been successfully completed on all the relevant platforms.

EXPECTED OUTPUT: *Verification and validation documentation for reusable components [DJF, -; CDR].*

NOTE In case not all platforms are available, the certificate of conformance states the limitations of the validation performed.

7.4 Standard ground hardware and services for operational system

7.4.1 Hardware procurement

ECSS-Q-ST-80_0720255

a. The subcontracting and procurement of hardware shall be carried out according to the requirements of ECSS-Q-ST-20 clause 5.4.

EXPECTED OUTPUT: *The following outputs are expected:*

a. Justification of selection of operational ground equipment [DJF, -; SRR, PDR];

b. Receiving inspection reports [PAF, -; SRR, PDR].

7.4.2 Service procurement

ECSS-Q-ST-80_0720256

a. The procurement of support services to be used in operational phases shall be justified as covering service level agreements, quality of services and escalation procedures, as needed for system exploitation and maintenance.

EXPECTED OUTPUT: *Justification of selection of operational support services [DJF, -; SRR, PDR].*

7.4.3 Constraints

ECSS-Q-ST-80_0720257

a. The choice of procured hardware and services shall address the constraints associated with both the development and the actual use of the software.

EXPECTED OUTPUT: *Justification of selection of operational ground equipment [DJF, -; SRR, PDR].*

7.4.4 Selection

ECSS-Q-ST-80_0720258

a. The ground computer equipment and supporting services for implementing the final system shall be selected according to the project requirements regarding:

1. performance;
2. maintenance;
3. durability and technical consistency with the operational equipment;
4. the assessment of the product with respect to requirements, including the criticality category;
5. the assessment of the product with respect to security sensitivity of the product;
6. compliance with applicable organizational, national or international standards, security regulations, policies or directives;
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 constraints;
12. availability;
13. compatibility;
14. site operational constraints.

EXPECTED OUTPUT: *Justification of selection of operational ground equipment [DJF, -; SRR, PDR].*

NOTE to item 5: The security sensitivity of the product is determined by the security analysis.

7.4.5 Maintenance

ECSS-Q-ST-80_0720259

a. Taking account of the provider's maintenance and product policy, it shall be ensured that the hardware and support services can be maintained throughout the specified life of the software product within the operational constraints.

7.5 Programmable devices

7.5.1 Device programming

ECSS-Q-ST-80_0720260

a. The supplier shall establish procedures for device programming and duplication of programmed services.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

7.5.2 Marking

ECSS-Q-ST-80_0720261

a. The programmed device shall be indelibly marked to allow the identification (by reference) of the hardware component and of the software component.

ECSS-Q-ST-80_0720345

b. Where protective security marking is required, devices and all software configuration items shall be marked accordingly.

EXPECTED OUTPUT: *Software product assurance plan [PAF, SPAP; PDR].*

7.5.3 Calibration

ECSS-Q-ST-80_0720262

a. The supplier shall ensure that the programming equipment is calibrated.

Annex A (informative) Software documentation

This annex defines the structure of the software documents to be produced, as depicted in Figure A-1.

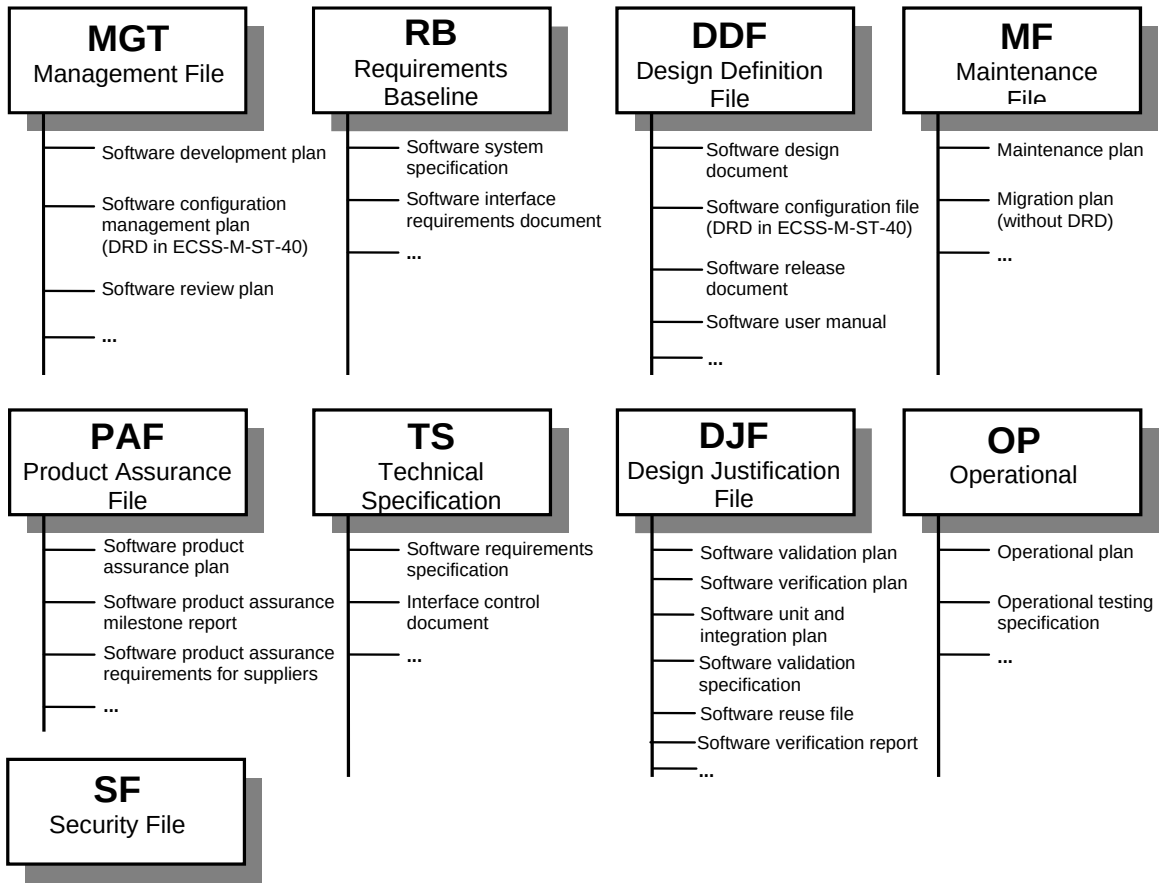

Figure A-1: Overview of software documents

Table A-1 represents the document requirements list, identifying the software documentation to be produced in accordance with the requirements defined in this Standard and in ECSS-E-ST-40 as output of the relevant processes.

Table A-1: ECSS-E-ST-40 and ECSS-Q-ST-80 Document requirements list (DRL)

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	DRL item having a DRD	SRR	PDR	CDR	QR	AR	ORR
RB	Software system specification (SSS)	ECSS-E-ST-40 Annex B	✔					
	Interface requirements document (IRD)	ECSS-E-ST-40 Annex C	✔					
	Safety and dependability analysis results for lower-level suppliers	-	✔					
TS	Software requirements specification (SRS)	ECSS-E-ST-40 Annex D		✔				
	Software interface control document (ICD)	ECSS-E-ST-40 Annex E		✔	✔			
DDF	Software design document (SDD)	ECSS-E-ST-40 Annex F		✔	✔			
	Software configuration file (SCF)	ECSS-M-ST-40 Annex E		✔	✔	✔	✔	✔
	Software release document (SRelD)	ECSS-E-ST-40 Annex G				✔	✔	
	Software user manual (SUM)	ECSS-E-ST-40 Annex H			✔	✔	✔	
	Software source code and media labels	-			✔			
	Software product and media labels	-				✔	✔	✔
	Training material	-				✔		
DJF	Software verification plan (SVerP)	ECSS-E-ST-40 Annex I	✔	✔				
	Software validation plan (SValP)	ECSS-E-ST-40 Annex J		✔				
	Independent software verification & validation plan	-	✔	✔				
	Software integration test plan (SUITP)	ECSS-E-ST-40C Annex K		✔	✔			

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	DRL item having a DRD	SRR	PDR	CDR	QR	AR	ORR
	Software unit test plan (SUITP)	ECSS-E-ST-40 Annex K			✔			
	Software validation specification (SVS) with respect to TS	ECSS-E-ST-40 Annex L			✔			
	Software validation specification (SVS) with respect to RB	ECSS-E-ST-40 Annex L				✔	✔	
	Acceptance test plan	-				✔	✔	
	Software unit test report	-			✔			
	Software integration test report	-			✔			
	Software validation report with respect to TS	-			✔			
	Software validation report with respect to RB	-				✔	✔	
	Acceptance test report	-					✔	
	Installation report	-					✔	
	Software verification report (SVR)	ECSS-E-ST-40 Annex M	✔	✔	✔	✔	✔	✔
	Independent software verification & validation report	-		✔	✔	✔	✔	✔
	Software reuse file (SRF)	ECSS-E-ST-40 Annex N	✔	✔	✔			
	Software problem reports and nonconformance reports	-	✔	✔	✔	✔	✔	✔
	Joint review report	-	✔	✔	✔	✔	✔	
	Justification of selection of operational ground equipment and services	-	✔	✔				

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	DRL item having a DRD	SRR	PDR	CDR	QR	AR	ORR
MGT	Software development plan (SDP)	ECSS-E-ST-40 Annex O	✔	✔				
	Software review plan (SRevP)	ECSS-E-ST-40 Annex P	✔	✔				
	Software configuration management plan	ECSS-M-ST-40 Annex A	✔	✔				
	Training plan	-	✔					
	Interface management procedures	-	✔					
	Identification of NRB SW members	-	✔					
	Procurement data	-	✔	✔				
MF	Software maintenance plan	ECSS-E-ST-40 Annex T				✔	✔	✔
	Maintenance records	-				✔	✔	✔
	SPR and NCR - Modification analysis report - Problem analysis report - Modification documentation - Baseline for change - Joint review reports	-						
	Migration plan and notification	-						
	Retirement plan and notification	-						
OP	Software operation support plan	-						✔
	Operational testing results	-						✔
	SPR and NCR - User's request record - Post operation review report	-						✔

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	DRL item having a DRD	SRR	PDR	CDR	QR	AR	ORR
SF	Software security management plan (SSMP)		✔	✔				
	Software security analysis report (SSAR)		✔	✔	✔	✔	✔	
	Security analyses results for lower level suppliers		✔					
	Security risk treatment plan (SRTP)	-	✔	✔	✔	✔	✔	✔
PAF	Software product assurance plan (SPAP)	ECSS-Q-ST-80 Annex B	✔	✔	✔	✔	✔	✔
	Software product assurance requirements for suppliers	-	✔					
	Audit plan and schedule	-	✔					
	Review and inspection plans or procedures	-						
	Procedures and standards	-		✔				
	Modelling and design standards		✔	✔				
	Coding standards and description of tools	-		✔				
	Software problem reporting procedures	-		✔				
	Software dependability and safety analysis report - Criticality classification of software components	-		✔	✔	✔	✔	
	Software product assurance reports	-						
	Software product assurance milestone report (SPAMR)	ECSS-Q-ST-80 Annex C	✔	✔	✔	✔	✔	✔
	Statement of compliance with test plans and procedures	-			✔	✔	✔	✔
	Records of training and experience	-						

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	DRL item having a DRD	SRR	PDR	CDR	QR	AR	ORR
	(Preliminary) alert information	-						
	Result of pre-award audits and assessments, and of procurement sources	-						
	Software process assessment plan	-						
	Software process assessment records	-						
	Review and inspection reports	-						
	Receiving inspection reports	-	✔	✔	✔	✔		
	Input to product assurance plan for systems operation	-						✔

Annex B (normative) Software product assurance plan (SPAP) - DRD

B.1 DRD identification

B.1.1 Requirement identification and source document

The software product assurance plan (SPAP) is called from the normative provisions summarized in Table B-1.

Table B-1: SPAP traceability to ECSS-E-ST-40 and ECSS-Q-ST-80 clauses

ECSS Standard	Clause	DRD section
ECSS-Q-ST-80	5.1.2.1	<5.1>.a, <5.1>.b
	5.1.2.2	<5.1>.a, <5.1>.b
	5.1.2.3	<5.1>.b
	5.1.3.1	<5.3>
	5.1.4.1	<5.1>.b
	5.2.1.1	All
	5.2.1.3	All
	5.2.1.4	<5.10>
	5.2.1.5	<8>
	5.2.6.1c	<6.5>
	5.2.7.2	<5.5>
	5.4.3.3	All
	5.4.3.4	All
	5.6.1.1	<5.8>
	6.1.1	<6.1>
	6.2.1.4	<6.2>
	6.2.3.2	<6.3>.c
	6.2.3.4	<6.3>.c
	6.2.3.5	<6.3>.c
	6.2.4.8	<6.5>.d

ECSS Standard	Clause	DRD section
	6.2.4.9	<6.5>.d
	6.2.5.1	<6.6>.e
	6.2.5.2	<6.6>.e
	6.2.7.2	<6.7>.f
	6.2.7.3	<6.7>.f
	6.2.7.4	<6.7>.f
	6.2.7.5	<6.7>.f
	6.2.9.1	<6.4>.a
	6.2.10.3	<6.4>.a
	6.2.10.4	<6.4>.a
	6.3.3.3	<6.8>.a.2.h.3
	6.3.3.5	<6.8>.a.2.g.2
	6.3.3.7	<6.8>.a.2.g.2
	6.3.4.3	<6.8>.a.3.h.2
	6.3.4.6	<6.8>.a.3.g.3
	6.3.5.1	<6.8>.a.4.g.4
	6.3.5.2	<6.8>.a.4.g.4
	7.1.3	<7.b.6>.b.4
	7.1.5	<7>.b.1
	7.1.6	<7>.b.1
	7.2.2.3	<7>.a
	7.5.1	<6.9>.c.19.h.3
	7.5.2	<6.9>.c.19.h.3

B.1.2 Purpose and objective

The software product assurance plan is a constituent of the product assurance file (PAF).

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

B.2 Expected response

B.2.1 Scope and content

<1> Introduction

ECSS-Q-ST-80_0720263

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

<2> Applicable and reference documents

ECSS-Q-ST-80_0720264

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

<3> Terms, definitions and abbreviated terms

ECSS-Q-ST-80_0720265

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

<4> System Overview

ECSS-Q-ST-80_0720266

a. The SPAP shall include or refer to a description of the system and software products being developed.

<5> Software product assurance programme implementation

<5.1> Organization

ECSS-Q-ST-80_0720267

a. The SPAP shall describe the organization of software product assurance activities, including responsibility, authority and the interrelation of personnel who manage, perform and verify work affecting software quality.

ECSS-Q-ST-80_0720268

b. The following topics shall be included:

1. organizational structure;
2. interfaces of each organisation, either external or internal, involved in the project;
3. relationship to the system level product assurance and safety;
4. independence of the software product assurance function;
5. delegation of software product assurance tasks to a lower level supplier, if any.

<5.2> Responsibilities

ECSS-Q-ST-80_0720269

a. The SPAP shall describe the responsibilities of the software product assurance function.

<5.3> Resources

ECSS-Q-ST-80_0720270

a. The SPAP shall describe the resources to be used to perform the software product assurance function.

ECSS-Q-ST-80_0720271

b. The description in B.2.1<5.3>a. shall include human resources and skills, hardware and software tools.

<5.4> Reporting

ECSS-Q-ST-80_0720272

a. The SPAP shall describe the reporting to be performed by software product assurance.

<5.5> Quality models

ECSS-Q-ST-80_0720273

a. The SPAP shall describe the quality models applicable to the project and how they are used to specify the quality requirements.

<5.6> Risk management

ECSS-Q-ST-80_0720274

a. The SPAP shall describe the contribution of the software product assurance function to the project risk management.

<5.7> Supplier selection and control

ECSS-Q-ST-80_0720275

a. The SPAP shall describe the contribution of the software product assurance function to the next level suppliers selection and control.

<5.8> Methods and tools

ECSS-Q-ST-80_0720276

a. The SPAP shall describe the methods and tools used for all the activities of the development cycle, and their level of maturity.

<5.9> Process assessment and improvement

ECSS-Q-ST-80_0720277

a. The SPAP shall state the scope and objectives of process assessment.

ECSS-Q-ST-80_0720278

b. The SPAP shall describe the methods and tools to be used for process assessment and improvement.

<5.10> Operations and maintenance (optional)

ECSS-Q-ST-80_0720279

a. The SPAP shall specify the quality measures related to the operations and maintenance processes (alternatively, a separate SPAP is produced).

<6> Software process assurance

<6.1> Software development cycle

ECSS-Q-ST-80_0720280

a. The SPAP shall refer to the software development cycle description in the software development plan.

ECSS-Q-ST-80_0720281

b. If not covered in the software development plan, the life cycle shall be described.

ECSS-Q-ST-80_0720282

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

<6.2> Projects plans

ECSS-Q-ST-80_0720283

a. The SPAP shall describe all plans to be produced and used in the project.

ECSS-Q-ST-80_0720284

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

<6.3> Software dependability and safety

ECSS-Q-ST-80_0720285

a. The SPAP shall contain a description and justification of the measures to be applied for the handling of critical software, including the dependability and safety analyses to be performed and the standards applicable for critical software.

<6.4> Software security

ECSS-Q-ST-80_0720346

a. The SPAP shall contain a description of and justification of the measures to be applied for handling of security related software, including the security analysis to be performed and the standards applicable to sensitive software.

ECSS-Q-ST-80_0720347

b. The SPAP shall contain at least a security assurance section containing at least references to the documents and section titles that capture the related security and any additional security assurance activities documented in the security file.

<6.5> Software documentation and configuration management

ECSS-Q-ST-80_0720286

a. The SPAP shall describe the contribution of the software product assurance function to the proper implementation of documentation and configuration management.

ECSS-Q-ST-80_0720287

b. The nonconformance control system shall be described or referenced. The point in the software life cycle from which the nonconformance procedures apply shall be specified.

ECSS-Q-ST-80_0720288

c. The SPAP shall identify method and tool to protect the supplied software, a checksum-type key calculation for the delivered operational software, and a labelling method for the delivered media.

<6.6> Process metrics

ECSS-Q-ST-80_0720289

a. The SPAP shall describe the process metrics derived from the defined quality models, the means to collect, store and analyze them, and the way they are used to manage the development processes.

<6.7> Reuse of software

ECSS-Q-ST-80_0720290

a. The SPAP shall describe the approach for the reuse of existing software, including delta qualification.

<6.8> Product assurance planning for individual processes and activities

ECSS-Q-ST-80_0720291

a. The following processes and activities shall be covered, taking into account the project scope and life cycle:
   1. software requirements analysis;
   2. software architectural design and design of software items;
   3. coding;
   4. testing and validation (including regression testing);
   5. verification;
   6. software delivery and acceptance;
   7. operations and maintenance.

<6.9> Procedures and standards

ECSS-Q-ST-80_0720292

a. The SPAP shall describe or list by reference all procedures and standards applicable to the development of the software in the project.

ECSS-Q-ST-80_0720293

b. The software product assurance measures to ensure adherence to the project procedures and standards shall be described.

ECSS-Q-ST-80_0720294

c. The standards and procedures to be described or listed in accordance with B.2.1<6.9>a shall be as a minimum those covering the following aspects:
   1. project management;
   2. risk management;
   3. configuration and documentation management;
   4. verification and validation;
   5. requirements engineering;
   6. design;
   7. coding;
   8. metrication;
   9. nonconformance control;

10. audits;
11. alerts;
12. procurement;
13. reuse of existing software;
14. use of methods and tools;
15. numerical accuracy;
16. delivery, installation and acceptance;
17. operations;
18. maintenance;
19. device programming and marking.

<7> Software product quality assurance

ECSS-Q-ST-80_0720295

a. The SPAP shall describe the approach taken to ensure the quality of the software product.

ECSS-Q-ST-80_0720296

b. The description of the approach specified in B.2.1<7>a shall include the:
   1. specification of the product metrics, their target values and the means to collect them;
   2. definition of a timely metrication programme;
   3. analyses to be performed on the collected metrics;
   4. way the results are fed back to the development team;
   5. documentation quality requirements;
   6. assurance activities meant to ensure that the product meets the quality requirements.

<8> Compliance matrix to software product assurance requirements

ECSS-Q-ST-80_0720297

a. The SPAP shall include the compliance matrix to the applicable software product assurance requirements (e.g. ECSS-Q-ST-80 clauses, as tailored by a product assurance requirements document), or provide a reference to it.

ECSS-Q-ST-80_0720298

b. For each software product assurance requirement, the following information shall be provided:
   1. requirement identifier;
   2. compliance
      (C = compliant, NC = non–compliant, NA = not applicable);
   3. reference to the project documentation covering the requirement (e.g. section of the software product assurance plan);
   4. remarks.

B.2.2 Special remarks

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

Annex C (normative) Software product assurance milestone report (SPAMR) - DRD

C.1 DRD identification

C.1.1 Requirement identification and source document

The software product assurance milestone report (SPAMR) is called from the normative provisions summarized in Table C-1.

Table C-1: SPAMR traceability to ECSS-Q-ST-80 clauses

ECSS Standard	Clause	DRD section
ECSS-Q-ST-80	5.2.2.3	All
	5.6.1.2	<5>.a
	5.6.1.3	<5>.b
	6.2.5.4	<7>
	6.2.5.5	<7>
	6.2.6.3	<4>
	6.2.6.7	<4>
	6.2.8.5	<6>
	6.3.3.4	<6>
	6.3.3.6	<6>.a.1
	6.3.3.7	<6>.a.2
	6.3.4.7	<6>
	6.3.5.3	<8>
	6.3.5.5	<8>
	6.3.5.12	<8>
	7.1.6	<7>
	7.1.8	<7>

C.1.2 Purpose and objective

The software product assurance milestone report is a constituent of the product assurance file (PAF).

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

C.2 Expected response

C.2.1 Scope and content

<1> Introduction

ECSS-Q-ST-80_0720299

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

<2> Applicable and reference documents

ECSS-Q-ST-80_0720300

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

<3> Terms, definitions and abbreviated terms

ECSS-Q-ST-80_0720301

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

<4> Verification activities performed

ECSS-Q-ST-80_0720302

a. The SPAMR shall contain reporting on verification activities performed by the product assurance function, including:
   1. reviews;
   2. inspections;
   3. walk-throughs;
   4. review of traceability matrices;
   5. documents reviewed.

ECSS-Q-ST-80_0720303

b. The SPAMR shall contain reporting on the verification of the measures applied for the handling of critical software.

<5> Methods and tools

ECSS-Q-ST-80_0720304

a. The SPAMR 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, software specification, design, coding, validation, testing, configuration management, verification and product assurance.

ECSS-Q-ST-80_0720305

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

<6> Adherence to design and coding standards

ECSS-Q-ST-80_0720306

a. The SPAMR shall include reporting on the adherence of software products to the applicable modelling, design and coding standards, including:

1. reporting on the application of measures meant to ensure that the design complexity and modularity meet the quality requirements;
2. reporting on design documentation w.r.t. suitability for maintenance.

<7> Product and process metrics

ECSS-Q-ST-80_0720307

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

ECSS-Q-ST-80_0720308

b. The results of the software maturity analysis shall also be reported.

<8> Testing and validation

ECSS-Q-ST-80_0720309

a. The SPAMR shall include reporting on adequacy of the testing and validation documentation (including feasibility, traceability repeatability), and on the achieved test coverage w.r.t. stated goals.

<9> SPRs and SW NCRs

ECSS-Q-ST-80_0720310

a. The SPAMR shall include reporting on the status of software problem reports and nonconformances relevant to software.

<10> References to progress reports

ECSS-Q-ST-80_0720311

a. 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.

C.2.2 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.

Annex D (normative) Tailoring of this Standard based on software criticality

D.1 Software criticality categories

Criticality categories are assigned to software products as specified in ECSS-Q-ST-30 clause 5.4, and ECSS-Q-ST-40 clause 6.5.6.3.

Table D-1 describes the relationship between the criticality category of the software products, the highest criticality of the functions implemented by the software and the existing system compensating provisions, as described in ECSS-Q-ST-30, clause 5.4, and ECSS-Q-ST-40, clause 6.5.6.3.

To any software product type described in the right column, the corresponding criticality category in the left column is assigned. E.g. both "Software involved in category I functions AND: no compensating provisions exist" and "Software included in compensating provisions for category I functions" are category A software.

For criticality classification of software components, clause 6.2.2 of this Standard applies.

Table D-1: Software criticality categories

Software criticality category	Definition
A	Software involved in category I functions AND: no compensating provisions exist
	Software included in compensating provisions for category I functions
B	Software 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 and ECSS-Q-ST-40 clause 6.5.6.3: - A hardware implementation - A software implementation; this software implementation shall be classified as criticality A - An operational procedure
	Software involved in category II functions AND: no compensating provisions exist
	Software included in compensating provisions for category II functions

Software criticality category	Definition
C	Software 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 and ECSS-Q-ST-40 clause 6.5.6.3: - A hardware implementation - A software implementation; this software implementation shall be classified as criticality B - An operational procedure
	Software involved in category III functions AND: no compensating provisions exist
	Software included in compensating provisions for category III functions
D	Software 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 and ECSS-Q-ST-40 clause 6.5.6.3: - A hardware implementation - A software implementation; this software implementation shall be classified as criticality C - An operational procedure
	Software involved in category IV functions AND: no compensating provisions exist

D.2 Applicability matrix

The following applicability matrix represents a tailoring of the requirements of this Standard based on the software criticality categories defined as per D.1.

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

Security is a transversal activity that might be applied independently of software criticality.

Table D-2: Applicability matrix based on software criticality

Clause	Description	A	B	C	D
5	**Software product assurance programme implementation**	-	-	-	-
5.1	Organization and responsibility	-	-	-	-
5.1.1	Organization	Y	Y	Y	Y

Clause	Description	A	B	C	D
5.1.2	Responsibility and authority	-	-	-	-
5.1.2.1		Y	Y	Y	Y
5.1.2.2		Y	Y	Y	Y
5.1.2.3		Y	Y	Y	Y
5.1.3	Resources	-	-	-	-
5.1.3.1		Y	Y	Y	Y
5.1.3.2		Y	Y	Y	N
5.1.4	Software product assurance manager/engineer	-	-	-	-
5.1.4.1		Y	Y	Y	Y
5.1.4.2		Y	Y	Y	Y
5.1.5	Training	-	-	-	-
5.1.5.1		Y	Y	Y	Expected output not required
5.1.5.2		Y	Y	Y	N
5.1.5.3		Y	Y	Y	Y
5.1.5.4		Y	Y	Y	Y
5.2	Software product assurance programme management	-	-	-	-
5.2.1	Software product assurance planning and control	-	-	-	-
5.2.1.1		Y	Y	Y	Y
5.2.1.2		Y	Y	Y	Y
5.2.1.3		Y	Y	Y	Y
5.2.1.4		Y	Y	Y	Y
5.2.1.5		Y	Y	Y	Y
5.2.2	Software product assurance reporting	-	-	-	-
5.2.2.1		Y	Y	Y	Y
5.2.2.2		Y	Y	Y	Y
5.2.2.3		Y	Y	Y	Y
5.2.3	Audits	Y	Y	Y	Audits planned and performed only when necessary
5.2.4	Alerts	Y	Y	Y	Y
5.2.5	Software problems	-	-	-	-
5.2.5.1		Y	Y	Y	Y
5.2.5.2		Y	Y	Y	Y
5.2.5.3		Y	Y	Y	Y
5.2.5.4		Y	Y	Y	Y

Clause	Description	A	B	C	D
5.2.6	Nonconformances	-	-	-	-
5.2.6.1		Y	Y	Y	Y
5.2.6.2		Y	Y	Y	Y
5.2.7	Quality requirements and quality models	-	-	-	-
5.2.7.1		Y	Y	Y	Y
5.2.7.2		Y	Y	Y	Relevant characteristics only (e.g. suitability for safety is not relevant for cat. D software)
5.3	Risk management and critical item control	-	-	-	-
5.3.1	Risk management	Y	Y	Y	Y
5.3.2	Critical item control	-	-	-	-
5.3.2.1		Y	Y	Y	Y
5.3.2.2		Y	Y	Y	Y
5.4	Supplier selection and control	-	-	-	-
5.4.1	Supplier selection	-	-	-	-
5.4.1.1		Y	Y	Y	Expected output not required
5.4.1.2		Y	Y	Y	Y
5.4.2	Supplier requirements	-	-	-	-
5.4.2.1		Y	Y	Y	Y
5.4.2.2		Y	Y	Y	N
5.4.3	Supplier monitoring	-	-	-	-
5.4.3.1		Y	Y	Y	Y
5.4.3.2		Y	Y	Y	Y
5.4.3.3		Y	Y	Y	Y
5.4.3.4		Y	Y	Y	N
5.4.4	Criticality classification	Y	Y	Y	Y
5.4.5	Security sensitivity	Y	Y	Y	Y
5.5	Procurement	-	-	-	-
5.5.1	Procurement documents	Y	Y	Y	Y
5.5.2	Review of procured software component list	Y	Y	Y	Y
5.5.3	Procurement details	Y	Y	Y	Y
5.5.4	Identification	Y	Y	Y	Y
5.5.5	Inspection	Y	Y	Y	Y
5.5.6	Exportability	Y	Y	Y	Y

Clause	Description	A	B	C	D
5.6	Tools and supporting environment	-	-	-	-
5.6.1	Methods and tools	-	-	-	
5.6.1.1		Y	Y	Y	The proposed methods and tools shall have been successfully used at least in one project before (possibly a non-space project)
5.6.1.2		Y	Y	Y	Expected output not required
5.6.1.3		Y	Y	Y	Expected output not required
5.6.2	Development environment selection	-	-	-	-
5.6.2.1		Y	Y	Y	Expected output not required
5.6.2.2		Y	Y	Y	Expected output not required
5.6.2.3		Y	Y	Y	Y
5.7	Assessment and improvement process	-	-	-	-
5.7.1	Process assessment	Y	Y	Y	N
5.7.2	Assessment process	-	-	-	-
5.7.2.1		Y	Y	Y	N
5.7.2.2		Y	Y	Y	N
5.7.2.3		Y	Y	Y	N
5.7.2.4		Y	Y	Y	N
5.7.3	Process improvement	-	-	-	-
5.7.3.1		Y	Y	Y	N
5.7.3.2		Y	Y	Y	N
5.7.3.3		Y	Y	Y	N
6	**Software process assurance**	-	-	-	-
6.1	Software development life cycle	-	-	-	-
6.1.1	Life cycle definition	Y	Y	Y	Y
6.1.2	Quality objectives	Y	Y	Y	Y
6.1.3	Life cycle definition review	Y	Y	Y	Y
6.1.4	Life cycle resources	Y	Y	Y	Y
6.1.5	Software validation process schedule	Y	Y	Y	Y
6.2	Requirements applicable to all software engineering processes	-	-	-	-
6.2.1	Documentation of processes	-	-	-	-

Clause	Description	A	B	C	D
6.2.1.1		Y	Y	Y	Y
6.2.1.2		Y	Y	Y	Y
6.2.1.3		Y	Y	Y	Y
6.2.1.4		Y	Y	Y	Y
6.2.1.5		Y	Y	Y	Y
6.2.1.6		Y	Y	Y	Y
6.2.1.7		Y	Y	Y	Y
6.2.1.8		Y	Y	Y	Y
6.2.1.9		Y	Y	Y	N
6.2.2	Software dependability and safety	-	-	-	-
6.2.2.1		Y	Y	Y	Y
6.2.2.2		Y	Y	Y	N
6.2.2.3		Y	Y	Y	N
6.2.2.4		Y	Y	Y	N
6.2.2.5		Y	Y	Y	N
6.2.2.6		Y	Y	Y	N
6.2.2.7		Y	Y	Y	N
6.2.2.8		Y	Y	Y	Y
6.2.2.9		Y	Y	Y	Y
6.2.2.10		Y	Y	Y	Y
6.2.3	Handling of critical software	-	-	-	-
6.2.3.2		Y	Y	Y	N
6.2.3.3		Y	Y	Y	N
6.2.3.4		Y	Y	Y	N
6.2.3.5		Y	Y	Y	N
6.2.3.6		Y	Y	Y	N
6.2.3.7		Y	Y	N	N
6.2.3.8		Y	Y	Y	N
6.2.4	Software configuration management	-	-	-	-
6.2.4.1		Y	Y	Y	Y
6.2.4.2		Y	Y	Y	Y
6.2.4.3		Y	Y	Y	Y
6.2.4.4		Y	Y	Y	Y
6.2.4.5		Y	Y	Y	Y
6.2.4.6		Y	Y	Y	Y
6.2.4.7		Y	Y	Y	Y
6.2.4.8		Y	Y	Y	Y
6.2.4.9		Y	Y	Y	Y

Clause	Description	A	B	C	D
6.2.4.10		Y	Y	Y	Y
6.2.4.11		Y	Y	Y	Y
6.2.4.12		Y	Y	Y	Y
6.2.5	Process metrics	-	-	-	-
6.2.5.1		Y	Y	Y	Y
6.2.5.2		Y	Y	Y	Y
6.2.5.3		Y	Y	Y	Y
6.2.5.4		Y	Y	Y	Limited to number of problems detected during validation
6.2.5.5		Y	Y	Y	Y
6.2.6	Verification	-	-	-	-
6.2.6.1		Y	Y	Y	Y
6.2.6.2		Y	Y	Y	Y
6.2.6.3		Y	Y	Y	Y
6.2.6.4		Y	Y	Y	Y
6.2.6.5		Y	Y	Y	N
6.2.6.6		Y	Y	Y	N
6.2.6.7		Y	Y	Y	Y
6.2.6.8		Y	Y	Y	Y
6.2.6.9		Y	Y	Y	Y
6.2.6.10		Y	Y	Y	Y
6.2.6.11		Y	Y	Y	Y
6.2.6.12		Y	Y	Y	Y
6.2.6.13		Y	Y	N	N
6.2.7	Reuse of existing software	-	-	-	-
6.2.7.1		Y	Y	Y	Y
6.2.7.2		Y	Y	Y	Y
6.2.7.3		Y	Y	Y	Y
6.2.7.4		Y	Y	Y	Bullets 3, 4, 5 and 7 not applicable. Bullet 2 limited to architectural design
6.2.7.5		Y	Y	Y	Y
6.2.7.6		Y	Y	Y	Y

Clause	Description	A	B	C	D
6.2.7.7		Y	Y	Y	Limited to the extent to ensure maintainability of the software
6.2.7.8		Y	Y	Y	Limited to the extent to ensure maintainability of the software
6.2.7.9		Y	Y	Y	Y
6.2.7.10		Y	Y	Y	Y
6.2.7.11		Y	Y	Y	Y
6.2.8	Automatic code generation	-	-	-	-
6.2.8.1		Y	Y	Y	Y
6.2.8.2		Y	Y	Y	Y
6.2.8.3		Y	Y	Y	Y
6.2.8.4		Y	Y	Y	Y
6.2.8.5		Y	Y	Y	Y
6.2.8.6		Y	Y	Y	Y
6.2.8.7		Y	Y	Y	Y
6.2.9	Software security	-	-	-	-
6.2.9.1		To be applied based on security assurance and sensitivity levels.			
6.2.9.2		To be applied based on security assurance and sensitivity levels.			
6.2.9.3		To be applied based on security assurance and sensitivity levels.			
6.2.9.4		To be applied based on security assurance and sensitivity levels.			
6.2.9.5		To be applied based on security assurance and sensitivity levels.			
6.2.9.6		To be applied based on security assurance and sensitivity levels.			
6.2.9.7		To be applied based on security assurance and sensitivity levels.			
6.2.10	Handling of security sensitive software	-	-	-	-
6.2.10.1		To be applied based on security assurance and sensitivity levels.			
6.2.10.2		To be applied based on security assurance and sensitivity levels.			
6.2.10.3		To be applied based on security assurance and sensitivity levels.			

Clause	Description	A	B	C	D
6.2.10.4		To be applied based on security assurance and sensitivity levels.			
6.3	Requirements applicable to individual software engineering processes or activities	-	-	-	-
6.3.1	Software related system requirements process	-	-	-	-
6.3.1.1		Y	Y	Y	Y
6.3.1.2		Y	Y	Y	Y
6.3.1.3		Y	Y	Y	Y
6.3.2	Software requirements analysis	-	-	-	-
6.3.2.1		Y	Y	Y	Y
6.3.2.2		Y	Y	Y	Y
6.3.2.3		Y	Y	Y	Y
6.3.2.4		Y	Y	Y	Y
6.3.2.5		Y	Y	Y	Y
6.3.3	Software architectural design and design of software items	-	-	-	-
6.3.3.1		Y	Y	Y	Documentation control only
6.3.3.2		Y	Y	Y	Only recommended
6.3.3.3		Y	Y	Y	N
6.3.3.4		Y	Y	Y	Only if design standards are applied (6.3.3.2)
6.3.3.5		Y	Y	Y	N
6.3.3.6		Y	Y	Y	N
6.3.3.7		Y	Y	Y	Y
6.3.4	Coding	-	-	-	-
6.3.4.1		Y	Y	Y	Y
6.3.4.2		Y	Y	Y	Y
6.3.4.3		Y	Y	Y	N
6.3.4.4		Y	Y	Y	N – This is Y for security sensitive software
6.3.4.5		Y	Y	Y	Y
6.3.4.6		Y	Y	Y	Y
6.3.4.7		Y	Y	Y	Y

Clause	Description	A	B	C	D
6.3.4.8		Y	Y	Y	The code shall be put under configuration control at the beginning of validation testing
6.3.5	Testing and validation	-	-	-	-
6.3.5.1		Y	Y	Y	No formal unit testing and integration activity required
6.3.5.2		Y	Y	Y	No formal unit testing and integration activity required This is Y for security sensitive software
6.3.5.3		Y	Y	Y	Test procedures and data verified by sample
6.3.5.4		Y	Y	Y	Applicable to validation and acceptance tests only
6.3.5.5		Y	Y	Y	Y
6.3.5.6		Y	Y	Y	Y
6.3.5.7		Y	Y	Y	Y
6.3.5.8		Y	Y	Y	Y
6.3.5.9		Y	Y	Y	N
6.3.5.10		Y	Y	Y	N
6.3.5.11		Y	Y	Y	Y
6.3.5.12		Y	Y	Y	Y
6.3.5.13		Y	Y	Y	Y
6.3.5.14		Y	Y	Y	Applicable to validation and acceptance tests only
6.3.5.15		Y	Y	Y	Y
6.3.5.16		Y	Y	Y	Y
6.3.5.17		Y	Y	Y	Y
6.3.5.18		Y	Y	Y	Y
6.3.5.19		Y	Y	Y	N

Clause	Description	A	B	C	D
6.3.5.20		Y	Y	Y	Y
6.3.5.21		Y	Y	Y	Y
6.3.5.22		Y	Y	Y	Y
6.3.5.23		Y	Y	Y	Y
6.3.5.24		Y	Y	Y	Y
6.3.5.25		Y	Y	Y	Y
6.3.5.26		Y	Y	Y	Y
6.3.5.27		Y	Y	Y	Y
6.3.5.28		Y	Y	N	N
6.3.5.29		Y	Y	Y	Y
6.3.5.30		Y	Y	Y	N
6.3.5.31		Y	Y	Y	N
6.3.5.32		Y	Y	Y	Y
6.3.5.33		Y	Y	Y	Y
6.3.6	Software delivery and installation	-	-	-	-
6.3.6.1		Y	Y	Y	Y
6.3.6.2		Y	Y	Y	Y
6.3.6.3		Y	Y	Y	Y
6.3.6.4		Y	Y	Y	Y
6.3.7	Software acceptance	-	-	-	-
6.3.7.1		Y	Y	Y	Y
6.3.7.2		Y	Y	Y	Y
6.3.7.3		Y	Y	Y	Y
6.3.7.5		Y	Y	Y	Y
6.3.7.6		Y	Y	Y	Y
6.3.7.7		Y	Y	Y	Y
6.3.8	Operations	-	-	-	-
6.3.8.1		Y	Y	Y	Y
6.3.8.2		Y	Y	Bullet on safety features not applicable	Bullet on safety features not applicable
6.3.8.3		Y	Y	Y	Y
6.3.9	Maintenance	-	-	-	-
6.3.9.1		Y	Y	Y	Y
6.3.9.2		Y	Y	Y	Y
6.3.9.3		Y	Y	Y	Y
6.3.9.4		Y	Y	Y	Y

Clause	Description	A	B	C	D
6.3.9.5		Y	Y	Y	Y
6.3.9.6		Y	Y	Y	Y
6.3.9.7		Y	Y	Y	Statistical data not collected
7	**Software product quality assurance**	-	-	-	-
7.1	Product quality objectives and metrication	-	-	-	-
7.1.1	Deriving of requirements	Y	Y	Y	Y
7.1.2	Quantitative definition of quality requirements	Y	Y	Y	Y
7.1.3	Assurance activities for product quality requirements	Y	Y	Y	Y
7.1.4	Product metrics	Y	Y	Y	Bullet 4.(a) not applicable
7.1.5	Basic metrics	Y	Y	Y	Design-relevant and fault density/failure intensity metrics not required
7.1.6	Reporting of metrics	Y	Y	Y	Y
7.1.7	Numerical accuracy	Y	Y	Y	Y
7.1.8	Analysis of software maturity	Y	Y	Y	N
7.2	Product quality requirements	-	-	-	-
7.2.1	Requirements baseline and technical specification	-	-	-	-
7.2.1.1		Y	Y	Y	Y
7.2.1.2		Y	Y	Y	Y
7.2.1.3		Y	Y	Y	Y
7.2.2	Design and related documentation	-	-	-	-
7.2.2.1		Y	Y	Y	Y
7.2.2.2		Y	Y	Y	Y
7.2.2.3		Y	Y	Y	Y
7.2.3	Test and validation documentation	-	-	-	-
7.2.3.1		Y	Y	Y	Y
7.2.3.2		Y	Y	Y	Y
7.2.3.3		Y	Y	Y	Y
7.2.3.4		Y	Y	Y	Y
7.2.3.5		Y	Y	Y	Y
7.2.3.6		Y	Y	Y	Y
7.3	Software intended for reuse	-	-	-	-
7.3.1	Customer requirements	Y	Y	Y	Y

Clause	Description	A	B	C	D
7.3.2	Separate documentation	Y	Y	Y	Y
7.3.3	Self-contained information	Y	Y	Y	Y
7.3.4	Requirements for intended reuse	Y	Y	Y	Y
7.3.5	Configuration management for intended reuse	Y	Y	Y	Y
7.3.6	Testing on different platforms	Y	Y	Y	Y
7.3.7	Certificate of conformance	Y	Y	Y	Y
7.4	Standard hardware for operational system	-	-	-	-
7.4.1	Hardware procurement	Y	Y	Y	Y
7.4.2	Service procurement	Y	Y	Y	Y
7.4.3	Constraints	Y	Y	Y	Y
7.4.4	Selection	Y	Y	Y	Y
7.4.5	Maintenance	Y	Y	Y	Y
7.5	Programmable devices	-	-	-	-
7.5.1	Device programming	Y	Y	Y	Y
7.5.2	Marking	Y	Y	Y	Y
7.5.3	Calibration	Y	Y	Y	Y

Annex E (informative) List of requirements with built-in tailoring capability

The following requirements are applicable under specific conditions, as described in the requirement's text.

5.1.4.2	The software product assurance *manager/engineer* shall report to the project manager (through the project product assurance manager, *if any*)
5.2.2.1	The supplier shall report on a regular basis on the status of the software product assurance programme implementation, *if appropriate* as part of the overall product assurance reporting of the project.
6.2.3.4	*In case* of minor changes in tools that affect the generation of the executable code, a binary comparison of the executable code generated by the different tools can be used to verify that no modifications are introduced
6.2.6.13	This requirement is applicable *where* the risks associated with the project justify the costs involved. The customer *may* consider a less rigorous level of independence, e.g. an independent team in the same organization.

The following requirements foresee an agreement between the customer and the supplier.

6.3.2.5	Prior to the technical specification elaboration, customer and supplier shall agree on the following principles and rules as a minimum: […].
6.3.5.2	Based on the criticality of the software, test coverage goals for each testing level shall be agreed between the customer and the supplier and their achievement monitored by metrics: […].

Annex F (informative) Document organization and content at each milestone

F.1 Introduction

The following table shows the organization of the Expected Output of the clauses of this Standard, sorted per review, then per destination file, then per DRD.

When no DRD is available, "-" is shown.

F.2 ECSS-Q-ST-80 Expected Output at SRR

Clause	Expected Output	Dest. File	DRD	Section
7.1.1.a	Requirement baseline	RB	SSS	<5.9>
7.1.2.a	Requirement baseline	RB	SSS	<5.9>
7.2.1.1.a	Requirement baseline	RB	SSS	<5.9>
7.2.1.3.a	Requirement baseline	RB	SSS	<5.1>
5.4.4	Safety and dependability analyses results for lower level suppliers	RB	-	
5.4.5	Security analysis for lower level suppliers	SF	-	
6.2.4.8.c	Software security management plan	SF	-	
6.2.4.9.b	Software security management plan	SF	-	
6.2.4.11.c	Software security management plan	SF	-	
5.1.2.1	Software product assurance plan	PAF	SPAP	<5.1>
5.1.2.2	Software product assurance plan	PAF	SPAP	<5.1>, <5.2>
5.1.2.3	Software product assurance plan	PAF	SPAP	<5.1>
5.1.3.1	Software product assurance plan	PAF	SPAP	<5.3>
5.1.3.2	Software product assurance plan	PAF	SPAP	<5.1>, <5.3>

Clause	Expected Output	Dest. File	DRD	Section
5.1.4.1	Software product assurance plan	PAF	SPAP	<5.1>, <5.3>
5.2.1.1	Software product assurance plan	PAF	SPAP	All
5.2.1.5	Software product assurance plan	PAF	SPAP	<8>
5.2.6.1.a	NCR SW procedure as part of the Software product assurance plan	PAF	SPAP	
5.2.6.2.	Software product assurance plan	PAF	SPAP	<6.5>
5.6.1.1	Software product assurance plan	PAF	SPAP	<5.8>
6.1.1	Software product assurance plan	PAF	SPAP	<6.1>
6.1.5	Software product assurance plan	PAF	SPAP	<6.1>
6.2.1.4	Software product assurance plan	PAF	SPAP	<6.2>
6.2.4.8.a	Software product assurance plan	PAF	SPAP	<6.5>
6.2.4.9.a	Software product assurance plan	PAF	SPAP	<6.5>
6.2.4.11.a	Software product assurance plan	PAF	SPAP	<6.55>
6.2.5.1	Software product assurance plan	PAF	SPAP	<6.6>
6.2.5.2	Software product assurance plan	PAF	SPAP	<6.6>
6.2.9.1	Software product assurance plan	PAF	SPAP	<6.4>
6.2.7.2.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.3.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.4.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.5.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>

Clause	Expected Output	Dest. File	DRD	Section
7.1.3	Software product assurance plan	PAF	SPAP	<7>
7.1.4	Software product assurance plan	PAF	SPAP	<7>
7.1.5	Software product assurance plan	PAF	SPAP	<7>
7.2.2.3.a	Software product assurance plan	PAF	SPAP	<6.8>
5.2.2.3	Software product assurance milestone report	PAF	SPAMR	All
5.6.1.2	Software product assurance milestone report	PAF	SPAMR	<5>
6.2.6.12	Software product assurance milestone report	PAF	SPAMR	<4>
5.2.3	Audit plan and schedule	PAF	-	
5.4.2.1	Software product assurance requirements for suppliers	PAF	-	
5.4.2.2	Software product assurance requirements for suppliers	PAF	-	
6.2.2.1	Criticality classification of software products	PAF	-	
6.2.8.4	Modelling standards	PAF	-	
6.3.3.2	Design standards	PAF	-	
7.4.1.b	Receiving inspection report	PAF	-	
5.5.2	Software development plan	MGT	SDP	<4.8>
5.6.2.1	Software development plan	MGT	SDP	<5.4>
5.6.2.2	Software development plan	MGT	SDP	<5.4>
6.2.4.2	Software configuration management plan	MGT	SCMP	
6.2.4.12	Software configuration management plan	MGT	SCMP	
7.3.5	Configuration management for reusable components	MGT	SCMP	
5.1.5.1	Training plan	MGT	-	
5.2.6.1.b	Identification of SW experts in NRB	MGT	-	
5.5.3	Procurement data	MGT	-	
6.2.7.2.b	Software reuse file	DJF	SRF	<6>
6.2.7.3.b	Software reuse file	DJF	SRF	<4>, <5>
6.2.7.4.b	Software reuse file	DJF	SRF	<5>
6.2.7.5.b	Software reuse file	DJF	SRF	<6>

Clause	Expected Output	Dest. File	DRD	Section
6.2.7.6	Software reuse file	DJF	SRF	<4>, <5>
6.2.7.7	Software reuse file	DJF	SRF	<8>
6.2.7.8	Software reuse file	DJF	SRF	<8>
6.2.7.11	Software reuse file	DJF	SRF	<9>
6.2.6.4	Software problem reports	DJF	-	
6.2.6.13.a	ISVV plan	DJF	-	
6.3.5.8	Software problem reports	DJF	-	
6.3.5.28.a	ISVV plan	DJF	-	
7.4.1.a	Justification of selection of operational ground equipment	DJF	-	
7.4.2	Justification of selection of operational support services	DJF	-	
7.4.3	Justification of selection of operational ground equipment	DJF	-	
7.4.4	Justification of selection of operational ground equipment	DJF	-	

F.3 ECSS-Q-ST-80 Expected Output at PDR

Clause	Expected output	Dest. File	DRD	Section
6.3.2.4	Software requirements specification	TS	SRS	<5>
7.1.1.b	Technical specification	TS	SRS	<5.10>
7.1.2.b	Technical specification	TS	SRS	<5.10>
7.2.1.1.b	Technical specification	TS	SRS	<5.10>
7.2.1.3.b	Technical specification	TS	SRS	<6>
7.3.4	Technical specification for reusable components	TS	-	
6.2.4.8	Software security management plan	SF	-	
6.2.6.13.d	Software security management plan	SF	-	
6.2.10.2	Software security management plan	SF	-	
6.2.10.3.b	Software security management plan	SF	-	
6.2.10.4.b	Software security management plan	SF	-	

Clause	Expected output	Dest. File	DRD	Section
6.3.5.28.c	Software security management plan	SF	-	
6.2.9.2	Software security analysis report	SF	-	
6.2.9.7	Software security analysis report	SF	-	-
6.2.10.1.b	Software security analysis report	SF	-	
5.2.1.1	Software product assurance plan	PAF	SPAP	All
5.2.1.5	Software product assurance plan	PAF	SPAP	<8>
5.2.6.2.	Software product assurance plan	PAF	SPAP	<6.4>
5.2.7.1	Software product assurance plan	PAF	SPAP	<5.5>
5.2.7.2	Software product assurance plan	PAF	SPAP	<5.5>
5.4.3.3	Next level suppliers' software product assurance plan	PAF	SPAP	All
5.4.3.4	Next level suppliers' software product assurance plan	PAF	SPAP	All
5.6.1.1	Software product assurance plan	PAF	SPAP	<5.8>
6.1.1	Software product assurance plan	PAF	SPAP	<6.1>
6.1.5	Software product assurance plan	PAF	SPAP	<6.1>
6.2.1.4	Software product assurance plan	PAF	SPAP	<6.2>
6.2.2.5.a	Software product assurance plan	PAF	SPAP	<6.3>
6.2.2.10.a	Software product assurance plan	PAF	SPAP	<6.3>
6.2.3.2	Software product assurance plan	PAF	SPAP	<6.3>
6.2.3.4	Software product assurance plan	PAF	SPAP	<6.8>
6.2.3.5	Software product assurance plan	PAF	SPAP	<6.8>

Clause	Expected output	Dest. File	DRD	Section
6.2.4.8.a	Software product assurance plan	PAF	SPAP	<6.5>
6.2.4.9	Software product assurance plan	PAF	SPAP	<6.5>
6.2.4.11.a	Software product assurance plan	PAF	SPAP	<6.5>
6.2.5.1	Software product assurance plan	PAF	SPAP	<6.6>
6.2.5.2	Software product assurance plan	PAF	SPAP	<6.6>
6.2.7.2.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.3.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.4.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.7.5.a	Software reuse approach, including approach to delta qualification	PAF	SPAP	<6.7>
6.2.9.1	Software product assurance plan	PAF	SPAP	<6.4>
6.2.10.3.a	Software product assurance plan	PAF	SPAP	<6.4>
6.2.10.4.a	Software product assurance plan	PAF	SPAP	<6.4>
6.3.3.3	Software product assurance plan	PAF	SPAP	<6.9>
6.3.3.5	Software product assurance plan	PAF	SPAP	<6.8>
6.3.3.7.a	Software product assurance plan	PAF	SPAP	<6.8>
6.3.4.3	Software product assurance plan	PAF	SPAP	<6.7>
6.3.4.6	Software product assurance plan	PAF	SPAP	<6.7>
6.3.5.1	Software product assurance plan	PAF	SPAP	<6.6>
6.3.5.2	Software product assurance plan	PAF	SPAP	<6.6>

Clause	Expected output	Dest. File	DRD	Section
7.1.3	Software product assurance plan	PAF	SPAP	<7>
7.1.4	Software product assurance plan	PAF	SPAP	<7>
7.1.5	Software product assurance plan	PAF	SPAP	<7>
7.2.2.3.a	Software product assurance plan	PAF	SPAP	<6.8>
7.5.1	Software product assurance plan	PAF	SPAP	<6.9>
7.5.2	Software product assurance plan	PAF	SPAP	<6.8>
5.2.2.3	Software product assurance milestone report	PAF	SPAMR	All
5.6.1.2	Software product assurance milestone report	PAF	SPAMR	<5>
6.2.3.3	Software product assurance milestone report	PAF	SPAMR	<4>
6.2.6.12	Software product assurance milestone report	PAF	SPAMR	<4>
5.2.5.1	Software problem reporting procedures	PAF	-	
5.2.5.2	Software problem reporting procedures	PAF	-	
5.2.5.3	Software problem reporting procedures	PAF	-	
5.5.5	Receiving inspection report	PAF	-	
6.2.1.6	Procedures and standards	PAF	-	
6.2.1.7	Procedures and standards	PAF	-	
6.2.2.1	Criticality classification of software products	PAF	-	
6.2.2.2	Software dependability and safety analysis report	PAF	-	
6.2.2.3	Criticality classification of software components	PAF	-	
6.2.2.7	Software dependability and safety analysis report	PAF	-	
6.2.2.10.b	Software dependability and safety analysis report	PAF	-	
6.2.10.1.a	Software dependability and safety analysis report	PAF	-	
6.2.8.4	Modelling standards	PAF	-	

Clause	Expected output	Dest. File	DRD	Section
6.3.3.2	Design standards	PAF	-	
6.3.4.1	Coding standards	PAF	-	
6.3.4.2	Coding standards	PAF	-	
6.3.4.4	Coding standards and description of tools	PAF	-	
7.4.1.b	Receiving inspection report	PAF	-	
5.5.2	Software development plan	MGT	SDP	<4.8>
5.6.2.1	Software development plan	MGT	SDP	<5.4>
5.6.2.2	Software development plan	MGT	SDP	<5.4>
6.3.4.5	Software development plan	MGT	SDP	<5.4>
6.2.4.2	Software configuration management plan	MGT	SCMP	
7.3.5	Configuration management for reusable components	MGT	SCMP	
5.5.3	Procurement data	MGT	-	
7.1.7	Numerical accuracy analysis	DJF	SVR	<6>
6.2.6.1	Software verification plan	DJF	SVerP	<6.3>
6.2.8.2	Validation and testing documentation	DJF	SValP	<4.1>
6.2.8.7	Validation and testing documentation	DJF	SValP	<4.1>
6.3.5.22	Test and validation documentation	DJF	SValP	<4>
6.3.5.23	Test and validation documentation	DJF	SValP	<4.4>
6.3.5.24	Test and validation documentation	DJF	SValP	<4.6>
6.3.5.25	Test and validation documentation	DJF	SValP	<5>
6.3.5.29	Test and validation documentation	DJF	SValP	<6>
6.2.8.2	Validation and testing documentation	DJF	SUITP	<7.6>
6.2.8.7	Validation and testing documentation	DJF	SUITP	<7.6>
6.3.5.22	Test and validation documentation	DJF	SUITP	<5>
6.3.5.23	Test and validation documentation	DJF	SUITP	<5.3>
6.3.5.24	Test and validation documentation	DJF	SUITP	<5.5>

Clause	Expected output	Dest. File	DRD	Section
6.3.5.25	Test and validation documentation	DJF	SUITP	<9.2>, <10>
6.2.7.2.b	Software reuse file	DJF	SRF	<6>
6.2.7.3.b	Software reuse file	DJF	SRF	<4>, <5>
6.2.7.4.b	Software reuse file	DJF	SRF	<5>
6.2.7.5.b	Software reuse file	DJF	SRF	<6>
6.2.7.6	Software reuse file	DJF	SRF	<4>, <5>
6.2.7.7	Software reuse file	DJF	SRF	<8>
6.2.7.8	Software reuse file	DJF	SRF	<8>
6.2.7.11	Software reuse file	DJF	SRF	<9>
6.2.6.4	Software problem reports	DJF	-	
6.2.6.13.a	ISVV plan	DJF	-	
6.2.6.13.b	ISVV report	DJF	-	
6.3.5.8	Software problem reports	DJF	-	
6.3.5.28.a	ISVV plan	DJF	-	
6.3.5.28.b	ISVV report	DJF	-	
7.4.1.a	Justification of selection of operational ground equipment	DJF	-	
7.4.2	Justification of selection of operational support services	DJF	-	
7.4.3	Justification of selection of operational ground equipment	DJF	-	
7.4.4	Justification of selection of operational ground equipment	DJF	-	
7.2.2.3.b	Justification of design choices	DDF	SDD	<4.5>

F.4 ECSS-Q-ST-80 Expected Output at CDR

Clause	Expected output	Dest. File	DRD	Section
6.2.9.5	Software security analysis report	SF	-	-
6.2.9.6	Software security analysis report	SF	-	-
6.2.9.7	Software security analysis report	SF	-	-
6.2.10.1.b	Software security analysis report	SF	-	
6.3.5.28.c	Software security analysis report	SF	-	

Clause	Expected output	Dest. File	DRD	Section
6.2.10.2	Software security management plan	SF	-	
6.2.10.3.b	Software security management plan	SF	-	
6.2.10.4.b	Software security management plan	SF	-	
5.2.1.3	Software product assurance plan	PAF	SPAP	All
6.2.2.5.a	Software product assurance plan	PAF	SPAP	<6.3>
6.2.3.2	Software product assurance plan	PAF	SPAP	<6.3>
6.2.3.4	Software product assurance plan	PAF	SPAP	<6.8>
6.2.3.5	Software product assurance plan	PAF	SPAP	<6.8>
5.2.2.3	Software product assurance milestone report	PAF	SPAMR	All
6.2.3.3	Software product assurance milestone report	PAF	SPAMR	<4>
6.2.6.12	Software product assurance milestone report	PAF	SPAMR	<4>
5.5.5	Receiving inspection report	PAF	-	
6.2.2.5	Software dependability and safety analysis report	PAF	-	
6.2.2.6	Software dependability and safety analysis report	PAF	-	
6.2.2.7	Software dependability and safety analysis report	PAF	-	
6.2.2.10.b	Software dependability and safety analysis report	PAF	-	
6.2.10.1.a	Software dependability and safety analysis report	PAF	-	
6.2.2.10.a	Software product assurance plan	PAF	SPAP	<6.3>
6.2.9.1	Software product assurance plan	PAF	SPAP	<6.4>
6.2.10.3.a	Software product assurance plan	PAF	SPAP	<6.4>
6.2.10.4.a	Software product assurance plan	PAF	SPAP	<6.4>
6.3.5.7	Statement of compliance with test plans and procedures	PAF	-	
6.3.5.11	Statement of compliance with test plans and procedures	PAF	-	
6.2.8.2	Validation and testing documentation	DJF	SVS	<5.6>
6.2.8.7	Validation and testing documentation	DJF	SVS	<5.6>

Clause	Expected output	Dest. File	DRD	Section
6.3.5.25	Test and validation documentation	DJF	SVS	<7.2>, <8>
6.3.5.29	Test and validation documentation	DJF	SVS	<6>
6.3.5.33	Software validation control information	DJF	-	
6.3.5.32	Software validation specification	DJF	SVS	<5>
6.2.6.5	Software verification report	DJF	SVR	<4.4>
6.2.6.6	Software verification report	DJF	SVR	<4.4>
7.1.7	Numerical accuracy analysis	DJF	SVR	<6>
7.2.3.6	Software verification report	DJF	SVR	<4.5>
6.2.8.2	Validation and testing documentation	DJF	SUITP	<7.6>
6.2.8.7	Validation and testing documentation	DJF	SUITP	<7.6>
6.3.5.22	Test and validation documentation	DJF	SUITP	<5>
6.3.5.23	Test and validation documentation	DJF	SUITP	<5.3>
6.3.5.24	Test and validation documentation	DJF	SUITP	<5.5>
6.3.5.25	Test and validation documentation	DJF	SUITP	<9.2>, <10>
6.2.7.9	Software reuse file	DJF	SRF	<8>
6.2.7.11	Software reuse file	DJF	SRF	<9>
6.2.6.4	Software problem reports	DJF	-	
6.2.6.13.b	ISVV report	DJF	-	
6.3.5.6	Nonconformance reports and software problem reports	DJF	-	
6.3.5.8	Software problem reports	DJF	-	
6.3.5.13	Testing and validation reports	DJF	-	
6.3.5.16	Updated test documentation	DJF	-	
6.3.5.17	Updated test documentation	DJF	-	
6.3.5.18	Updated test documentation	DJF	-	
6.3.5.28.b	ISVV report	DJF	-	
6.3.5.30	Testing and validation reports	DJF	-	
6.3.5.31	Testing and validation reports	DJF	-	
7.3.6	Verification and validation documentation for reusable components	DJF	-	

Clause	Expected output	Dest. File	DRD	Section
7.3.7	Verification and validation documentation for reusable components	DJF	-	
6.2.4.4	Software configuration file	DDF	SCF	All
6.2.4.5	Software configuration file	DDF	SCF	All
6.2.4.8.b	Software configuration file	DDF	SCF	All
7.2.2.3.b	Justification of design choices	DDF	SDD	<4.5>

F.5 ECSS-Q-ST-80 Expected Output at QR

Clause	Expected output	Dest. File	DRD	Section
6.2.9.5	Software security analysis report	SF	-	-
6.2.9.6	Software security analysis report	SF	-	-
6.2.10.1.b	Software security analysis report	SF	-	
6.2.10.2	Software security management plan	SF	-	
5.2.1.3	Software product assurance plan	PAF	SPAP	All
5.2.2.3	Software product assurance milestone report	PAF	SPAMR	All
6.2.3.3	Software product assurance milestone report	PAF	SPAMR	<4>
6.2.6.12	Software product assurance milestone report	PAF	SPAMR	<4>
5.5.5	Receiving inspection report	PAF	-	
6.2.2.5	Software dependability and safety analysis report	PAF	-	
6.2.2.6	Software dependability and safety analysis report	PAF	-	
6.2.2.10.b	Software dependability and safety analysis report	PAF	-	
6.2.10.1.a	Software dependability and safety analysis report	PAF	-	
6.3.5.7	Statement of compliance with test plans and procedures	PAF	-	
6.3.5.11	Statement of compliance with test plans and procedures	PAF	-	
6.3.8.1	Maintenance plan	MF	-	
6.3.8.2	Maintenance plan	MF	-	
6.3.8.4	Maintenance plan	MF	-	

Clause	Expected output	Dest. File	DRD	Section
6.3.8.5	Maintenance plan	MF	-	
6.3.7.1	Acceptance test plan	DJF	-	
6.2.8.2	Validation and testing documentation	DJF	SVS	<5.6>
6.2.8.7	Validation and testing documentation	DJF	SVS	<5.6>
6.3.5.25	Test and validation documentation	DJF	SVS	<7.2>, <8>
6.3.5.29	Test and validation documentation	DJF	SVS	<6>
6.3.5.32	Software validation specification	DJF	SVS	<5>
6.2.6.5	Software verification report	DJF	SVR	<4.4>
6.2.6.6	Software verification report	DJF	SVR	<4.4>
7.1.7	Numerical accuracy analysis	DJF	SVR	<6>
7.2.3.6	Software verification report	DJF	SVR	<4.5>
6.2.7.9	Software reuse file	DJF	SRF	<8>
6.2.7.11	Software reuse file	DJF	SRF	<9>
6.2.6.4	Software problem reports	DJF	-	
6.2.6.13.c	ISVV report	DJF	-	
6.3.5.6	Nonconformance reports and software problem reports	DJF	-	
6.3.5.8	Software problem reports	DJF	-	
6.3.5.13	Testing and validation reports	DJF	-	
6.3.5.16	Updated test documentation	DJF	-	
6.3.5.17	Updated test documentation	DJF	-	
6.3.5.18	Updated test documentation	DJF	-	
6.3.5.28.b	ISVV report	DJF	-	
6.3.5.30	Testing and validation reports	DJF	-	
6.3.5.31	Testing and validation reports	DJF	-	
6.2.4.4	Software configuration file	DDF	SCF	All
6.2.4.5	Software configuration file	DDF	SCF	All
6.2.4.8.b	Software configuration file	DDF	SCF	All

F.6 ECSS-Q-ST-80 Expected Output at AR

Clause	Expected output	Dest. File	DRD	Section
6.2.6.13.d	Software security analysis report	SF	-	-
6.2.9.5	Software security analysis report	SF	-	-
6.2.9.6	Software security analysis report	SF	-	-
6.2.10.1.b	Software security analysis report	SF	-	-
6.2.10.2	Software security management plan	SF	-	
5.2.1.3	Software product assurance plan	PAF	SPAP	All
5.2.1.4	Software product assurance plan	PAF	SPAP	<5.10>
5.2.2.3	Software product assurance milestone report	PAF	SPAMR	All
6.2.3.3	Software product assurance milestone report	PAF	SPAMR	<4>
6.2.6.12	Software product assurance milestone report	PAF	SPAMR	<4>
6.2.2.5	Software dependability and safety analysis report	PAF	-	
6.2.2.6	Software dependability and safety analysis report	PAF	-	
6.2.2.10	Software dependability and safety analysis report	PAF	-	
6.2.10.1.a	Software dependability and safety analysis report	PAF	-	
6.3.5.7	Statement of compliance with test plans and procedures	PAF	-	
6.3.5.11	Statement of compliance with test plans and procedures	PAF	-	
6.3.8.1	Maintenance plan	MF	-	
6.3.8.2	Maintenance plan	MF	-	
6.3.8.4	Maintenance plan	MF	-	
6.3.8.5	Maintenance plan	MF	-	
6.2.8.2	Validation and testing documentation	DJF	SVS	<5.6>
6.2.8.7	Validation and testing documentation	DJF	SVS	<5.6>
6.3.5.25	Test and validation documentation	DJF	SVS	<7.2>, <8>
6.3.5.29	Test and validation documentation	DJF	SVS	<6>
6.3.7.1	Joint review report	DJF	-	
6.3.5.32	Software validation specification	DJF	SVS	<5>

Clause	Expected output	Dest. File	DRD	Section
6.2.6.5	Software verification report	DJF	SVR	<4.4>
6.2.6.6	Software verification report	DJF	SVR	<4.4>
7.2.3.6	Software verification report	DJF	SVR	<4.5>
6.2.7.9	Software reuse file	DJF	SRF	<8>
6.2.7.11	Software reuse file	DJF	SRF	<9>
6.2.6.4	Software problem reports	DJF	-	
6.2.6.13.c	ISVV report	DJF	-	
6.3.5.6	Nonconformance reports and software problem reports	DJF	-	
6.3.5.8	Software problem reports	DJF	-	
6.3.5.13	Testing and validation reports	DJF	-	
6.3.5.16	Updated test documentation	DJF	-	
6.3.5.17	Updated test documentation	DJF	-	
6.3.5.18	Updated test documentation	DJF	-	
6.3.5.27	Test and validation documentation	DJF	-	
6.3.5.28.b	ISVV report	DJF	-	
6.3.5.30	Testing and validation reports	DJF	-	
6.3.5.31	Testing and validation reports	DJF	-	
6.3.7.1	Acceptance test plan	DJF	-	
6.3.7.5	Nonconformance reports	DJF	-	
6.3.7.6	Acceptance test report	DJF	-	
6.3.7.7	Acceptance test report	DJF	-	
6.2.4.4	Software configuration file	DDF	SCF	All
6.2.4.5	Software configuration file	DDF	SCF	All
6.2.4.8.b	Software configuration file	DDF	SCF	All
6.3.6.2	Installation procedure	DDF	SCF	<4.2>

F.7 ECSS-Q-ST-80 Expected Output not associated with any specific milestone review

Clause	Expected output	Dest. File	DRD	Section
6.2.4.11.d	Protective security markings	SF	-	
5.1.5.2	Records of training and experience	PAF	-	
5.2.2.1	Software product assurance report	PAF	-	
5.2.2.2	Software product assurance report	PAF	-	
5.2.4.a	Preliminary alert information	PAF	-	

Clause	Expected output	Dest. File	DRD	Section
5.2.4.b	Alert information	PAF	-	
5.4.1.1.a	Results of pre-award audits and assessments	PAF	-	
5.4.1.1.b	Records of procurement sources	PAF	-	
5.6.1.3	Software product assurance reports	PAF	-	
5.7.1	Software process assessment records: Overall assessments and improvement programme plan	PAF	-	
5.7.2.1.a	Software process assessment record: assessment model	PAF	-	
5.7.2.1.b	Software process assessment record: assessment method	PAF	-	
5.7.2.2.a	Software process assessment record: evidence of conformance of the process assessment model	PAF	-	
5.7.2.2.b	Software process assessment record: assessment method	PAF	-	
5.7.2.3	Software process assessment record: Software process assessment recognition evidence	PAF	-	
5.7.2.4	Software process assessment record: competent assessor justification	PAF	-	
5.7.3.1	Software process assessment records: improvement plan	PAF	-	
5.7.3.2	Software process assessment records: improvement process	PAF	-	
5.7.3.3	Software process assessment records: evidence of improvements	PAF	-	
6.2.5.4	Software product assurance reports	PAF	-	
6.2.5.5	Software product assurance reports	PAF	-	
6.2.6.2	Software product assurance reports	PAF	-	
6.2.6.3	Software product assurance reports	PAF	-	
6.2.6.7	Software product assurance reports	PAF	-	
6.2.6.9	Review and inspection plans or procedures	PAF	-	
6.2.6.10	Review and inspection plans or procedures	PAF	-	
6.2.6.11	Review and inspection reports	PAF	-	
6.2.8.5	Software product assurance reports	PAF	-	
6.3.3.4	Software product assurance reports	PAF	-	
6.3.3.6	Software product assurance reports	PAF	-	

Clause	Expected output	Dest. File	DRD	Section
6.3.3.7.b	Software product assurance reports	PAF	-	
6.3.4.7	Software product assurance reports	PAF	-	
6.3.5.3	Software product assurance reports	PAF	-	
6.3.5.5	Software product assurance reports	PAF	-	
6.3.5.12	Software product assurance reports	PAF	-	
7.1.6	Software product assurance reports	PAF	-	
7.1.7	Software product assurance reports	PAF	-	
6.3.8.6	Maintenance records	MF	-	
6.3.8.7	Maintenance records	MF	-	
5.2.6.1.a.b	Nonconformance reports	DJF	-	
5.4.1.2	Software reuse file	DJF	SRF	All
6.2.4.3.a	Software configuration file	DDF	SCF	All
6.2.4.3.b	Software release document	DDF	SRelD	All
6.2.4.10	Software configuration file	DDF	SCF	All
6.2.4.11.b	Labels	DDF	-	

Bibliography

ECSS-S-ST-00	ECSS system — Description, implementation and general requirement
ECSS-Q-HB-80-02	Space product assurance — Software process assessment and improvement
ECSS-Q-HB-80-03	Space product assurance — Software dependability and safety methods and techniques
ECSS-Q-HB-80-04	Space product assurance — Software metrication programme definition and implementation
ECSS-Q-ST-30-02	Space product assurance — Failure modes, effects (and criticality) analysis
IEEE 610.12:1990	IEEE Standard Glossary of software engineering terminology
IEEE 1028-1997	IEEE Standard for Software Reviews
ISO 9000:2000	Quality management systems — Fundamentals and vocabulary
ISO/IEC 25000:2014	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRESQuaRE
ISO/IEC 25010:2011	Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models
ISO/IEC/IEEE 24765:2017	Systems and software engineering — Vocabulary (https://www.iso.org/standard/71952.html)
RTCA/DO-178B	Software considerations in airborne systems and equipment certification
CMU/SEI-92-TR-022	Software Quality Measurement: A framework for counting problems and defects
CMU/SEI-2006-TR-008	CMMI for Development, Version 1.2