ECSS-Q-ST-30C
6 March 2009

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Dependability

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

Foreword

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

This Standard has been prepared by the ECSS-Q-ST-30 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

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

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

Change log

ECSS-Q-30A 16 April 1996	First issue
ECSS-Q-30B 8 March 2002	Second issue
ECSS-Q-ST-30C 6 March 2009	Third issue The majority of changes introduced by issue C of this standard were aimed at streamlining the text of the document to improve readability and clarity. The main changes between this version and the previous issue are: • Inclusion of an annex dedicated to a "analyses applicability matrix", • Inclusion of DRDs for items not covered by level 3 documents, • Improved coherency with ECSS-Q-ST-40, • Clarification of the coverage of ground segment activities, the S/W dependability, the risk management and severity definition, • Consideration of the recommendations of the Task Force # 2.

Table of contents

Tables

1 Scope

This Standard defines the dependability assurance programme and the dependability requirements for space systems.

Dependability assurance is a continuous and iterative process throughout the project life cycle.

The ECSS dependability policy for space projects is applied by implementing a dependability assurance programme, which comprises:

- identification of all technical risks with respect to functional needs which can lead to non-compliance with dependability requirements,
- application of analysis and design methods to ensure that dependability targets are met,
- optimization of the overall cost and schedule by making sure that:
  - design rules, dependability analyses and risk reducing actions are tailored with respect to an appropriate severity categorisation,
  - risks reducing actions are implemented continuously since the early phase of a project and especially during the design phase.
- inputs to serial production activities.

The dependability requirements for functions implemented in software, and the interaction between hardware and software, are identified in this Standard.

NOTE 1 The requirements for the product assurance of software are defined in ECSS-Q-ST-80.

NOTE 2 The dependability assurance programme supports the project risk management process as described in ECSS-M-ST-80

This Standard applies to all European space projects. The provisions of this document apply to all project phases.

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

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-Q-ST-10	Space product assurance —Product assurance management
ECSS-Q-ST-10-04	Space product assurance – Critical-item control
ECSS-Q-ST-30-02	Space product assurance — Failure modes, effects (and criticality) analysis (FMEA/FMECA)
ECSS-Q-ST-30-11	Space product assurance – Derating - EEE components

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

For the purpose of this Standard, the terms and definitions from ECSS-ST-00-01 apply, in particular for the following terms:

space system

ground systems

3.2 Terms specific to the present standard

3.2.1 failure scenario

conditions and sequence of events, leading from the initial root cause, to an end failure

3.2.2 space element

product intended to be operated in space

[adapted from ECSS-S-ST-00-01]

3.2.3 space segment

one or more space elements

3.2.4 limited-life item

item with useful life duration or operating cycles limitation, prone to wear out, drift or degradation below the minimum required performance in less than the storage and mission time

3.3 Abbreviated terms

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

Abbreviation	Meaning
CCB	configuration control board
EEE	electrical, electronic and electromechanical

FDIR	failure detection isolation and recovery
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FTA	fault tree analysis
HSIA	hardware-software interaction analysis
MMI	man-machine interface
MRB	material review board
MTBF	mean time between failure
MTTR	mean time to repair
NRB	nonconformance review board
PA	product assurance
TRB	test review board
WCA	worst case analysis

4
Dependability programme

4.1 General

a. The dependability assurance shall be implemented by means of a systematic process for specifying requirements for dependability and demonstrating that these requirements are achieved.

b. The dependability assurance process shall be in conformance with the dependability assurance programme plan for the project.

4.2 Organization

a. The supplier shall coordinate, implement and integrate the dependability programme management with the PA programme management.

4.3 Dependability programme plan

a. The supplier shall develop, maintain and implement a dependability plan for all project phases in conformance with the DRD in Annex C.

b. The plan shall address the applicable requirements of this document.

NOTE The plan can be included in the PA programme plan.

c. The extent that dependability assurance is applied shall take account of the severity (as defined in Table 5-1) of the consequences of failures.

d. The establishment and implementation of the dependability programme plan shall be considered in conjunction with the safety aspects of the programme.

e. The Supplier shall ensure that any potential conflict between dependability and safety requirements are managed.

f. Responsibilities for carrying out all dependability tasks within each phase of the lifecycle shall be defined.

4.4 Dependability risk assessment and control

a. As part of the risk management process implemented on the project, the Dependability engineer shall be responsible for identifying and reporting dependability associated risks .

NOTE ECSS-M-ST-80 describes the risk management process.

b. Dependability risk analysis reduction and control shall include the following steps:

1. identification and classification of undesirable events according to the severity of their consequences;
2. analysis of failure scenarios, determination of related failure modes, failure origins or causes;
3. classification of the criticality of the functions and associated products according to the severity of relevant failure consequences;
4. definition of actions and recommendations for detailed risk assessment, risk elimination, or risk reduction and control to an acceptable level;
5. status of risk reduction and risk acceptance;
6. implementation of risk reduction;
7. verification of risk reduction and assessment of residual risks.

NOTE The process of risk identification and assessment implies both qualitative and quantitative approaches.

c. Risk reduction measures that are proposed for dependability shall be assessed at system level in order to select the optimum solution to reduce the system level risk.

4.5 Dependability critical items

a. Dependability critical items shall be identified by dependability analyses performed to support the risk reduction and control process performed on the project.

NOTE The criteria for identifying dependability critical items are given in clause 6.5.

b. Dependability critical items, as part of the Critical Items List, shall be subject to risk assessment and critical items control in conformance with ECSS-Q-ST-10-04.

c. The control measures shall include:

1. a review of all design, manufacturing and test documentation related to critical functions, critical items and procedures;

2. dependability representation on relevant Review Boards to ensure that the disposition takes account of their criticality level.

d. The dependability aspects shall be considered during the entire verification process for dependability critical items until closeout.

4.6 Design reviews

a. The supplier shall ensure that all dependability data for a design review are presented to the customer in accordance with the project review schedule.

b. All dependability data submitted shall indicate the design baseline and shall be coherent with all other supporting technical documentation.

c. All design changes shall be assessed for their impact on dependability and a reassessment of the dependability shall be performed

4.7 Dependability Lessons learnt

a. Dependability lessons learnt shall be collected during the project life cycle including operational and disposal phases.

NOTE Dependability lessons learnt consider:

- the impact of newly imposed requirements;
- assessment of all malfunctions, anomalies, deviations and waivers;
- effectiveness of strategies of the project;
- new dependability tools and methods that have been developed or demonstrated;
- effective versus ineffective verifications that have been performed.

4.8 Progress reporting

a. The supplier shall report dependability progress to the customer as part of product assurance activities in conformance with ECSS-Q-ST-10.

4.9 Documentation

a. The supplier shall maintain all data used for the dependability programme.

5 Dependability engineering

5.1 Integration of dependability in the project

a. Dependability shall be integrated as part of the design process.

b. The dependability characteristics shall be traded off with other system attributes such as mass, size, cost and performance during the optimization of the design in all phases of the project.

NOTE Dependability is an inherent characteristic of a system or product.

c. Manufacture, assembly, integration, test and operations shall not degrade dependability attributes introduced into the design.

5.2 Dependability requirements in technical specification

a. The dependability requirement specification shall be part of the overall project requirements.

b. Dependability requirements shall be apportioned, in a top-down process, to establish dependability requirements for lower level elements.

c. Dependability requirements shall be applied during the preparation and review of design and test specifications.

d. The dependability requirements shall be included into the technical specifications.

NOTE The technical specifications typically include:

- functional, operational and environmental requirements,
- test requirements including stress levels, test parameters, and accept or reject criteria,
- design performance margins, derating factors, quantitative dependability requirements, and qualitative dependability requirements (identification and classification of undesirable events), under specified environmental conditions,

- the identification of human factors and how they can influence dependability during the project lifecycle,
- the identification of external, internal and installation factors that can influence dependability during the project lifecycle,
- the degree of tolerance to hardware failures or software malfunctions,
- the detection, isolation, diagnosis, and recovery of the system from failures and its restoration to an acceptable state,
- the requirement for the prevention of failures crossing interfaces with unacceptable consequences,
- definition of the maintenance concept,
- maintenance tasks and requirements for special skills,
- requirements for preventive maintenance, special tools, and special test equipment,
- requirements for process and technology margin demonstration and qualification,
- requirement on sampling strategy in serial production and for periodical demonstration of qualification preservation.

5.3 Dependability design criteria

5.3.1 General

a. The identification of critical areas of design and the assessment of the severity of failure consequences shall be interpreted by the level at which the analysis is made.

NOTE The Space System level can be broken down into Space Segment and Ground Segment where separate requirements can be provided. The Space Segment and Ground Segment can be further broken down, dependant on particular contractual requirements, into lower levels elements (e.g. subsystem, equipment…).

b. The success criteria (sometimes referred to as “mission success criteria”) shall be defined at each level to be analysed.

5.3.2 Consequences

a. A severity classification (either severity name or level) shall be assigned in accordance with Table 5-1 to each identified failure mode analysed according to the failure effect (consequence).

b. Severity categories shall be assigned without consideration of existing compensating provisions to provide a qualitative measure of the worst potential consequences resulting from item failure.

c. For analyses lower than system level, the severity due to possible failure propagation shall be identified as level 1 for dependability.

NOTE For example, for analysis at subsystem, and equipment level

d. The number identifying the severity category shall be followed by a suffix to indicate either redundancy (R) single point failures (SP) or safety hazards (SH).

e. An understanding to these criteria identified in table 1 shall be agreed between customer and supplier.

Table 5-1: Severity of consequences

SEVERITY	LEVEL	DEPENDABILITY (ECSS-Q-ST-30)	SAFETY (ECSS-Q-ST-40) *Extract from ECSS-Q-ST-40C*
Catastrophic	1	Failures propagation (refer to point 5.3.2.c)	*"Loss of life, life-threatening or permanently disabling injury or occupational illness.*
			Loss of an interfacing manned flight system
			Severe detrimental environmental effects.
			Loss of launch site facilities.
			Loss of system
Critical	2	Loss of mission	*Temporarily disabling but not life-threatening injury, or temporary occupational illness .*
			Major detrimental environmental effects.
			Major damage to public or private properties.
			Major damage to interfacing flight systems,
			Major damage to ground facilities."
Major	3	Major mission degradation	
Minor or Negligible	4	Minor mission degradation or any other effect.	

5.3.3 Failure tolerance

a. Failure tolerance requirements shall be defined in the performance specifications.

b. The verification of the failure tolerance shall address all failure modes whose severity of consequence is classified as catastrophic, critical and major.

5.3.4 Design approach

a. The supplier shall confirm that reliability is built into the design using fault tolerance and design margins.

b. The supplier shall analyse the failure characteristics of systems in order to identify areas of design weakness and propose corrective solutions.

c. In order to implement dependability aspects into the design, the following approaches shall apply:

1. functional design:

(a) the preferred use of software designs or methods that have performed successfully in similar applications

(b) the implementation of failure tolerance;

(c) the implementation of fault detection, isolation and recovery, allowing proper failure processing by dedicated flight and ground measures, and considering detection or reconfiguration times in relation with propagation times of events under worst case conditions;

(d) the implementation of monitoring of the parameters that are essential for mission performance, considering the failure modes of the system in relation to the actual capability of the detection devices, and considering the acceptable environmental conditions to be maintained on the product.

2. physical design:

(a) the application of proven design rules;

(b) the selective use of designs that have performed successfully in the same intended mission environment;

(c) the selection of parts having a quality level in accordance with project specification;

(d) the use of EEE parts derating and stress margins for mechanical parts;

(e) the use of design techniques for optimising redundancy (while keeping system design complexity as low as possible);

(f) the assurance that built-in equipment can be inspected and tested;

(g) the provision of accessibility to equipment.

NOTE Functional design is intended to imply non-physical design which includes software.

5.4 Classification of critical functions and products

a. During the preliminary design phase, the contractor shall classify functions, operations and products in accordance with their criticality level.

b. Classification shall be approved by the customer.

c. The criticality of functions (hardware and/or software) and operations shall be directly related to the severity of the consequences resulting from failure of the function as defined in Table 5-1.

NOTE For example, a function whose failure induces a catastrophic consequence is required to be classified with the highest criticality level.

d. The criticality of a product (hardware and software) shall be identified at the highest criticality of the functions associated to that product.

e. The classification shall be used to focus efforts on the most critical areas during the project phases.

5.5 Involvement in testing process

a. The supplier shall ensure that dependability aspects are covered in all development, qualification and acceptance test planning and reviews, including the preparation of test specifications and procedures and the evaluation of test results.

b. The dependability discipline shall support:

1. definition of test characteristics and test objectives,

2. selection of measurement parameters, and

3. statistical evaluation of test results.

5.6 Involvement in operational aspects

a. The supplier shall ensure that dependability cognizant and qualified staff:

1. contribute to definition of operations manual and procedures,

2. review operations manual and procedures for verification of consistency with dependability analyses.

b. Procedures for operations shall be analysed to identify and assess the risks associated with operations, sequences and situations that can affect dependability performance.

c. The analyses mentioned in 5.6b shall take into account the technical and human environment, and verify that the procedures:

1. include dispositions to face abnormal situations and supply the necessary safeguard measures;

2. do not compromise equipment reliability;

3. are in accordance with established maintenance dispositions;

4. include dispositions to minimize failures due to human errors.

5.7 Dependability recommendations

a. The supplier shall establish and maintain a system to track the dependability recommendations, in order to support the risk reduction process.

NOTE These recommendations are derived from the dependability analyses, and trade–off studies (typically during Phases A and B). The dependability recommendations can be tracked in combination with safety recommendations.

b. All recommendations from 5.7a shall be justified, documented and tracked.

c. Formal evidence of acceptance or rejection of the recommendation by the supplier’s management shall be provided.

d. An accepted dependability recommendation shall be implemented into the relevant corresponding documentation .

NOTE Example of corresponding documentation are: design documents, and operation manuals.

6
Dependability analyses

6.1 Identification and classification of undesirable events

a. The supplier shall identify undesirable events that lead to the loss or degradation of product performances, together with their classification into categories related to the severity of their failures consequences (see Table 5-1).

b. Preliminary identification and classification of undesirable events shall be determined from analysis of criteria for mission success, during conceptual and preliminary design phases.

c. All undesirable events, whose occurrence can jeopardize, compromise, or degrade the mission success shall be assessed at the highest product level (overall system including space and ground segments).

d. The undesirable events, at lower levels of the product tree, shall be the product failure effects which can induce the undesirable events identified for the highest product level.

NOTE For example, at space segment, ground segment, subsystem, and equipment level.

e. Identification and classification of undesirable events shall be finalised after assessment of failure scenarios (see clause 6.2).

6.2 Assessment of failure scenarios

a. The supplier shall analyse the possible scenarios leading to the occurrence of undesirable events,

b. The supplier shall identify failure modes, failure origins and causes, detailed failure effects leading to undesirable events.

6.3 Dependability analyses and the project life cycle

a. Dependability analyses shall be performed on all space projects throughout the project life cycle to support the tasks and requirements specified in clause 5.

b. Dependability analyses shall be performed initially to contribute to the definition of the conceptual design and the system requirements.

c. The analyses shall be performed to support the conceptual, preliminary and detailed development and optimization of the design, including the testing phase that leads to design qualification.

d. Dependability analyses shall be implemented in order to:

1. ensure conformance to reliability, availability and maintainability requirements, and

2. identify all potential failure modes and technical risks with respect to functional requirements that can lead to non-compliance to the dependability requirements,

3. provide inputs to risk assessment and risk reduction and their control measures in line with the risk management process implemented on the project.

e. The results of dependability analyses shall be incorporated into the design justification file in order to support improvements to the design.

6.4 Dependability analyses - methods

6.4.1 General

a. Dependability analyses shall be conducted on all levels of the space system and be performed in respect of the level that is being assessed i.e. System, Subsystem and Equipment levels.

NOTE The main purpose of all dependability analyses is to improve the design by providing timely feedback to the designer, to reduce risks within the processes used to realize the products and to verify conformance to the specified dependability requirement.

b. The analyses identified in clauses 6.4.2 to 6.4.4 shall be:

1. conducted as required by the contract,

2. tailored to match the generic requirements on each project,

3. taking into account the hardware, software and human functions comprising the system.

NOTE As it is not possible to quantitatively assess the software functions, only a qualitative assessment can be made as the dependability of software is influenced by the software development process.

c. A set of analyses selected from clauses 6.4.2 to 6.4.4 shall be defined as part of the contract requirement.

6.4.2 Reliability analyses

6.4.2.1 Reliability prediction

a. Reliability prediction techniques shall be used with the following objectives:

1. to optimize the reliability of a design against competing constraints such as cost and mass,
2. to predict the in–service reliability of a product,
3. to provide failure probability data for purposes such as risk assessment.

b. The reliability data sources and methods used in reliability predictions shall be as specified by the customer.

c. If the reliability data sources and methods are not specified by the customer, the supplier shall justify the selected data sources and methods used, for customer approval.

NOTE ECSS-Q-HB-30-08 is a guideline for the selection of reliability data sources and their use.

d. Reliability models shall be prepared to support predictions and FMEA/FMECA.

6.4.2.2 FMEA/FMECA

a. Failure Modes and Effects Analysis (FMEA) / Failure Modes, Effects and Criticality Analysis (FMECA) shall be performed on the functional and physical design (Functional FMECA and Product FMECA respectively) and, if required by the contract, the processes used to realize the final product (Process FMECA).

b. All potential failure modes shall be identified and classified according to the severity (FMEA) or criticality (FMECA) of their consequences.

c. Measures shall be proposed in the analysis and introduced in the product design and in the control of processes to render all such consequences acceptable to the project.

d. When any design or process changes are made, the FMEA/FMECA shall be updated and the effects of new failure modes introduced by the changes shall be assessed.

e. Provisions for failure detection and recovery actions shall be identified as part of the FMEA/FMECA.

f. The FMEA/FMECA shall be used to support the verification of the reliability modelling, the reliability and safety analyses, maintainability analysis, logistic support activity, test and maintenance planning, and the Failure Detection, Isolation and Recovery (FDIR) policy.

g. As part of the FMEA/FMECA, potential failure propagation shall be assessed.

NOTE For FMEA/FMECA refer to ECSS-Q-ST-30-02.

6.4.2.3 Hardware-software interaction analysis (HSIA)

a. HSIA shall be performed to ensure that the software reacts in an acceptable way to hardware failure.

b. HSIA shall be performed at the level of the technical specification of the software.

NOTE HSIA can be included in the FMEA/FMECA (refer to ECSS-Q-ST-30-02).

6.4.2.4 Contingency analysis

a. Contingency analysis shall be performed in conformance with Annex D in order to:

1. identify the failure, identify the cause, control the effect and indicate how recovery of the mission integrity can be achieved

2. identify the methods of recovery of the nominal or degraded functionalities, with respect to project dependability policy,

NOTE 1 For example, availability targets.

NOTE 2 The contingency analysis is typically a system level task.

NOTE 3 FMEA/FMECA is an input to contingency analysis.

6.4.2.5 Fault tree analysis (FTA)

a. A Fault Tree Analysis shall be performed to ensure that the design conforms to the failure tolerance requirements for combinations of failures.

NOTE 1 ECSS-Q-ST-40-12 is a guideline for FTA.

NOTE 2 The system supplier performs FTA to identify possible event combinations leading to the undesirable end event (e.g. “loss of mission”). Subsystem supplier provides input to this activity by establishing FTA at subsystem level with respect to the top events:

- loss of function of the subsystem, and
- inadvertent activation of the subsystem function.

6.4.2.6 Common-cause analysis

a. Common-cause analyses shall be performed on reliability and safety critical items in conformance with Annex I, to identify the root cause of failures that have a potential to negate failure tolerance levels (see clause 5.3.3).

NOTE 1 The analyses can be accomplished as part of FMEA/FMECA or FTA.

NOTE 2 An example of check list of generic common-cause parameters is provided in Annex L.

6.4.2.7 Worst case analysis (WCA)

a. Worst case analysis shall be performed on electrical equipment in conformance with Annex J, to demonstrate that it performs within specification despite variations in its constituent part parameters and the imposed environment.

b. The WCA report shall contain all baseline information (assumptions, methods and techniques) used for the preparation of the analysis, the results obtained and a comparison of the specified parameters as derived from the specification of the equipment or module.

c. If not specified in the project requirement, the supplier shall propose the component aging parameter drifts for customer approval.

NOTE 1 The document ECSS-Q-TM-30-12 is a source for component aging parameter drifts, but is to be complemented with others inputs as it does not cover exhaustively the EEE parts.

NOTE 2 ECSS-Q-HB-30-01 describes the WCA methodology.

6.4.2.8 Part stress analysis

a. Part derating shall be implemented in conformance with ECSS-Q-ST-30-11 to assure that the stress levels applied to all EEE parts are within the limits.

b. Part stress analyses shall be performed at part level to verify that the derating rules have been implemented.

6.4.2.9 Zonal analysis

a. Zonal analysis shall be performed in conformance with Annex G, in order to evaluate the consequences due to potential subsystem-to-subsystem interactions inherent in the system installation.

6.4.2.10 Failure Detection Isolation and Recovery (FDIR) analysis

a. FDIR analysis shall be performed at System level in conformance with Annex F, to ensure that the autonomy and failure tolerance requirements are fulfilled.

NOTE ECSS-E-ST-70-11 provides the description of FDIR process.

6.4.3 Maintainability analyses

a. Maintainability requirements shall be apportioned to set maintainability requirements for lower level products to conform to the maintenance concept and maintainability requirements of the system.

b. Maintainability prediction shall be performed at system level in conformance with Annex H, and used as a design tool to assess and compare design alternatives with respect to specified maintainability quantitative requirements:

1. the time to diagnose (i.e. detect and isolate) item failures,
2. the time to remove and replace the defective item,
3. the time to return the system or subsystem to its nominal configuration and to perform the necessary checks, and
4. the item failure rates.

c. Preventive maintenance analysis shall be performed at system level to determine the maintenance plan.

NOTE Each preventive maintenance action is based on the results of the application of systematic decision logic approved by the customer.

d. The maintainability analysis shall identify maintainability critical items.

NOTE Maintainability critical items include:

- products that cannot be checked and tested after integration,
- limited–life products,
- products that do not meet, or cannot be validated as compliant to the maintainability requirements.

6.4.4 Availability analysis

a. The supplier shall perform availability analysis or simulations in order to assess the availability of the system.

NOTE The results are used to:

- optimize the system concept with respect to design, operations and maintenance,
- verify conformance to availability requirements,
- provide inputs to estimate the overall cost of operating the system.

b. The supplier shall perform an analysis of outages in order to supply input data for availability analysis.

c. The availability analysis output shall include a list of all potential outages identified (as defined in the project), their causes, probabilities of occurrence and duration.

NOTE Instead of outage probabilities, failure rates associated with outages can be provided.

d. The means of outage detection and the recovery methods shall be identified in the analysis.

e. The availability analysis shall be carried out at system level using the system reliability and maintainability models as well as the data from the outages.

NOTE For availability analysis, refer to ECSS-Q-ST-30-09.

6.5 Dependability Critical Items List

a. The Dependability critical items identified by the dependability analyses shall be documented in conformance with ECSS-Q-ST-10-04.

b. Items identified as single-point failure with at least a failure consequence severity classified as catastrophic, critical or major, shall be included in the dependability critical items list.

c. Items that have a criticality number greater than or equal to 6 shall be included in the dependability critical items list in conformance with ECSS-Q-ST-30-02.

d. All items that have failure consequences classified as catastrophic shall be included in the dependability critical items list.

e. Products that cannot be checked and tested after integration, limited–life products, products that do not meet - or cannot be verified as meeting - applicable maintainability requirements, shall be included in the dependability critical items list.

f. The documentation for each dependability critical item shall include a justification for retention of that item and be subject to approval by the customer.

NOTE Further criteria for the classification of dependability critical items can be specified by the customer in line with the risk management policy defined on the project.

7 Dependability testing, demonstration and data collection

7.1 Reliability testing and demonstration

a. Reliability testing and demonstration shall be performed according to the project requirements in order to:

1. validate failure modes and effects,
2. check failure tolerance, failure detection and recovery,
3. obtain statistical failure data to support predictions and risk assessment,
4. consolidate reliability assessments,
5. validate the capability of the hardware to operate with software or to be operated by a human being in accordance with the specifications,
6. demonstrate the reliability of critical items, and
7. validate or justify data bases used for theoretical demonstrations.

7.2 Availability testing and demonstration

a. Availability testing and demonstration shall be performed according to the project requirements in order to validate or justify data bases used for theoretical demonstrations (duration of outages and probability of occurrence).

7.3 Maintainability demonstration

a. Maintainability demonstration shall be performed by performing the verification of the applicable maintainability requirements and by ensuring that preventive and corrective maintenance activities are successfully performed within the scope of the maintenance concept.

b. “The maintainability demonstration” shall verify the ability to:

1. detect, diagnose and isolate each faulty line replaceable unit or orbit replaceable unit;

2. remove and replace each line replaceable unit or orbit replaceable unit;
3. perform mission–essential repairs on units that are not intended to be replaced;
4. check that the product is fully functional after maintenance actions have been completed;
5. demonstrate that no safety hazard is introduced as a result of maintenance actions;
6. demonstrate that the maintenance operations can be performed within the applicable constraints, including the operations necessary to prepare a system during the launch campaign

   NOTE 1 Example of such a constraints are time and volume or accessibility.

   NOTE 2 Example of such operations are "remove–before–flight" items or replacement of batteries.

7.4 Dependability data collection and dependability performance monitoring

a. Dependability data as specified in the contract, shall be collected for a period agreed with the customer from sources such as non-conformance and problem or failure reports, and maintenance reports.

   NOTE Dependability data can be used for dependability performances monitoring through agreed or specified models.

Annex A (informative) Relationship between dependability activities and project phases

A.1 Mission analysis / Needs identification phase (phase 0)

In this phase no specific dependability assurance task is typically performed.

A.2 Feasibility phase (phase A)

In this phase the dependability assurance tasks are typically to:

a. develop and establish the project dependability policy to fulfil the dependability requirements;

b. support design trade–off and perform preliminary dependability analyses to identify and compare the dependability critical aspects of each design option; perform initial availability assessments where required;

c. perform preliminary risk identification and classification;

d. plan the dependability assurance tasks for the project definition phase.

A.3 Preliminary definition phase (phase B)

In this phase the dependability assurance tasks are typically to:

a. to support the trade off studies towards the selection of a preliminary design;

b. establish the failure effect severity categories for the project and allocate quantitative dependability requirements to all levels of the system;

c. perform the preliminary assessment of risk scenarios;

d. establish the applicable failure–tolerance requirements;

e. perform preliminary dependability analyses;

f. define actions and recommendations for risk reduction, provide preliminary dependability critical item list;

g. provide criticality classifications of functions and products;

h. support the definition of the maintenance concept and the maintenance plan;

i. plan the dependability assurance tasks for the detailed design and development phase and prepare the dependability plan as part of the PA plan.

A.4 Detailed definition and production/ground qualification testing phases (phase C/D)

In this phase the dependability assurance tasks are typically to:

a. perform detailed risk assessment, and detailed dependability analyses;

b. refine criticality classifications of functions and products;

c. define actions and recommendations for risk reduction, perform verification of risk reduction;

d. update and refine the dependability critical items list and the rationale (for retention);

e. define reliability and maintainability design criteria;

f. support the identification of key and mandatory inspection points, identify critical parameters of dependability critical items and initiate and monitor the dependability critical items control programme;

g. perform contingency analyses in conjunction with design and operations engineering;

h. support design reviews and monitor changes for impact on dependability;

i. define tool requirement and perform maintainability training and maintainability demonstration;

j. support quality assurance during manufacture, integration and test;

k. support NRBs and failure review boards;

l. review design and test specifications and procedures;

m. review operational procedures to evaluate human reliability problems related to MMI, check compatibility with the assumptions made in preparing the dependability analysis or determine the impact of incompatibilities;

n. collect dependability data.

A.5 Utilization phase (phase E)

In this phase the dependability assurance tasks are typically to:

a. support flight readiness reviews;

b. support ground and flight operations;

c. assess the impact on dependability resulting from design evolution;

d. investigate dependability related flight anomalies;

e. collect dependability data during operations.

A.6 Disposal phase (phase F)

In this phase the dependability assurance tasks are typically to:

a. review operations for total or partial cessation of use of the system and its constituent products and their final disposal;

b. provide criticality classification of functions and products;

c. define actions and recommendations for risk reduction.

Annex B (informative) Document requirement list (DRL)

The document requirement list is used as dependability programme input to the overall project document requirement list.

A recommended practice is to check that there is no duplication of supplier–generated documentation within the dependability and the safety programmes.

The customer can specify, or can agree, that two or more documentation items are combined into a single report.

The following list covers the documentation established by this Standard:

- dependability plan;
- failure modes, effects (and criticality) analysis - FMEA/FMECA;
- reliability prediction;
- hardware–software interaction analysis;
- common-cause analysis;
- fault tree analysis;
- contingency analysis;
- maintainability analysis;
- availability analysis;
- zonal analysis;
- worst case analysis;
- part stress analysis;
- failure detection identification and recovery
- dependability critical items list;
- report on risk identification, assessment, reduction and control.

The DRL tailoring is dependant on the project contractual clauses.

The DRDs in following dedicated annexes are intended to address only those analyses which are not covered by level 3 ECSS Standards.

Refer to Annex K for cross-reference to level 3 ECSS Standards or DRDs.

Annex C (normative) Dependability plan - DRD

C.1 Introduction

The dependability plan provides a response to the customer dependability requirements.

C.2 Scope and applicability

The purpose of the dependability plan is to provide information on the organisational aspects and the technical approach to the execution of the dependability programme.

C.3 Normative references

ECSS-Q-ST-30	Space product assurance – Dependability
ECSS-Q-ST-10	Space product assurance – Product assurance management

C.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

C.5 Description and purpose

The aim of the dependability plan is to describe how the relevant disciplines and activities will be coordinated and integrated to fully comply with the requirements.

A consistent approach to the management of dependability processes will be adopted to ensure a timely and cost effective programme.

This plan will identify and tie together all the tasks including planning, predictions, analyses, demonstrations and will define the methods and the techniques to accomplish the dependability requirements.

C.6 Application and interrelationships

This paragraph will identify the prime responsible for the dependability programme. It will also include details of the applicable phases, products and associated hardware or software relevant to the programme.

This paragraph will also describe how dependability will be managed through out the project phases.

NOTE The dependability plan may be part of the product assurance plan.

C.7 Content

a. The dependability plan shall include as a minimum:

- list of the applicable and reference documents,
- applicable dependability requirements,
- description of the dependability organisation and management,
- contractor / supplier management,
- details of the dependability tasks for each phase,
- dependability activities status reporting.

Annex D (normative) Contingency analysis - DRD

D.1 Introduction

The purpose of the contingency analysis is to identify all contingencies arising from failures of the system.

D.2 Scope and applicability

This DRD establishes the data content requirements for contingency analysis.

D.3 Normative references

ECSS-Q-ST-ST-30	Space product assurance – Dependability

D.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

D.5 Description and purpose

The purposes of contingency analysis are:

- to identify the failure, to identify the cause, to control the effect and to indicate how recovery of the mission integrity can be achieved
- to identify the methods of recovery of the nominal or degraded functionalities, with respect to project dependability policy (availability targets for example).

The contingency analysis is typically a system level task.

D.6 Application and interrelationships

The contingency analysis is linked with other dependability analyses such as:

- Reliability prediction,
- Fault tree analysis,
- FDIR,
- Maintainability analysis,
- FMEA/FMECA.

D.7 Content

a. The contingency analysis document shall include:

   — a description of the system,

   — a description of the method to perform contingency analysis,

   — details of the failure detection method,

   — details of the diagnostics,

   — details of the recovery actions or procedures,

   — actions and recommendations for project team.

Annex E (normative) Reliability prediction - DRD

E.1 Introduction

The goals of reliability prediction are:

- to compare possible architecture solutions regarding reliability criteria during trade-off,
- to provide failure probability data in order to compare with the reliability targets and to provide inputs for risk assessment.

The preliminary reliability prediction will provide an indication of the reliability apportionment result used in the prediction.

E.2 Scope and applicability

This DRD establishes the data content requirements for Reliability Prediction.

E.3 References

E.3.1 Normative references

ECSS-Q-ST-30	Space product assurance - Dependability

E.3.2 Handbooks References

ECSS-Q-HB-30-08	Space product assurance – component reliability data sources and their use

E.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

E.5 Description and purpose

The reliability prediction is based on 2 items:

- the reliability model: considering the possible redundancy types,
- determination of the failure rate or equivalent of each item under analysis.

There are many ways to compute the predictive failure rate, such as:

- in-service experience, based on either accelerated tests or in-service data collection. In this case, relevance of data collection should be justified,
- engineering judgement,
- reliability databases: in order to calculate a failure rate according to parameters such as utilisation (e.g. duty cycle), physical features (e.g. numbers of gates for integrated circuit), environment (e.g. temperature) and quality levels (e.g. screening),
- manufacturer's data.

E.6 Application and interrelationships

The reliability prediction may be linked as either an input source or an output to other dependability analyses such as:

- FMEA, FMECA and Fault tree analysis: reliability prediction is an input (providing failure rates for dedicated items) but FMEA, FMECA and Fault tree analysis also provide inputs for the reliability prediction,
- Part stress analysis provides inputs for failure rate calculation,
- Inputs for availability analysis,
- Reliability critical item list is based on reliability prediction outputs.

E.7 Content

a. The reliability prediction document shall include:

   — a clear identification of the design being analysed,

   — reliability block diagrams,

   — the methodology used with rationales,

   — an analysis of the results,

   — recommendations for project decision.

Annex F (normative)
Failure Detection Identification and Recovery - DRD

F.1 Introduction

The main purpose of FDIR is to protect mission integrity i.e. to prevent a loss of all or part of the mission in cases where mission's continuity could have been preserved by adequate measures.

F.2 Scope and applicability

This DRD establishes the data content requirements for FDIR.

F.3 Normative references

ECSS-Q-ST-30	Space product assurance — Dependability

F.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

F.5 Description and purpose

The purposes of failure detection identification and recovery analysis are:

- to demonstrate conformance with the failure tolerance requirements of the project,
- to provide the list of actions and recommendations for project decision.

F.6 Application and interrelationships

The FDIR is linked with other dependability analyses such as:

- FMEA/FMECA,
- Hardware and software interaction analysis,
- Availability analysis.

F.7 Content

a. The FDIR analysis document shall include:

- a description of the system,
- a description of the method to perform FDIR (e.g. FMEA/FMECA synthesis, FDIR reviews),
- details of considered failures,
- symptoms of failures (e.g. TM, observables),
- detailed failure impact on the system,
- the recovery actions (e.g. TC, automatic on board mechanism),
- actions and recommendations for project team.

Annex G (normative) Zonal analysis - DRD

G.1 Introduction

The goal of zonal analysis is to evaluate the consequences due to potential subsystem–to–subsystem interactions inherent in the system installation.

G.2 Scope and applicability

This DRD establishes the data content requirements for zonal Analysis.

G.3 Normative references

ECSS-Q-ST-30	Space product assurance — Dependability

G.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

G.5 Description and purpose

The purpose of the zonal analysis is to:

- identify the possible interaction between subsystems,
- provide an assessment of these potential interactions,
- produce recommendations for mitigation.

G.6 Application and interrelationships

The zonal analysis is linked with other dependability analyses such as:

- FMEA/FMECA,
- Common-cause.

G.7 Content

a. The zonal analysis document shall include:

- an identification of the perimeter under investigation,
- a detailed definition of the interface(s),
- the description of the potential interaction(s),
- the list of actions and recommendations for project decision.

Annex H (normative) Maintainability analysis - DRD

H.1 Introduction

The purpose of the maintainability analysis is to show demonstrate conformance or identify non–conformance with the maintainability requirements.

The preliminary maintainability analysis will provide an indication of the maintainability apportionment result used in the analysis.

H.2 Scope and applicability

This DRD establishes the data content requirements for the maintainability analysis.

H.3 Normative references

ECSS-Q-ST-30	Space product assurance — Dependability

H.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

H.5 Description and purpose

The purpose of the maintainability analysis is to:

- identify the possible corrective and preventive maintenance tasks,
- provide MTBF and MTTR for availability analysis,
- provide recommendations for improvement.

H.6 Application and interrelationships

The maintainability analysis is linked with other dependability analyses such as:

- Reliability analysis,
- Availability analysis,
- Fault tree,
- FDIR,
- FMEA/FMECA.

H.7 Content

a. The document shall contain, as a minimum:

   — maintenance levels: for corrective and preventive actions,

   — identification of FDIR policy,

   — mathematical model description,

   — the maintenance indicators (e.g. MTTR, maintenance time per year, maintenance frequency),

   — the sparing recommendations (e.g. number of spares, weight and volume of up and downloading spares),

   — identification of Maintainability Critical Items.

Annex I (normative) Common-cause analysis - DRD

I.1 Introduction

The purpose of the common-cause analysis is to identify the root cause of failures that have a potential to negate failure tolerance levels.

I.2 Scope and applicability

This DRD establishes the data content requirements for common-cause analysis.

I.3 Normative references

ECSS-Q-ST-30	Space product assurance - Dependability

I.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

I.5 Description and purpose

The purpose of the common–cause analysis is to identify and analyse the effects of common parameters (such as radiation, temperature, physical location, vibration) on the particular design under investigation.

I.6 Application and interrelationships

The common-cause analysis is linked with other dependability analyses such as:

- Fault tree analysis,
- Availability analysis,
- Safety analysis,
- FMEA/FMECA.

I.7 Content

a. The common-cause analysis document shall include:

— a description of the perimeter of the design being analysed,

— the list of the ‘common-cause’ parameters and their effects,

— actions and recommendations for project team.

NOTE See check lists parameters examples in Annex L.

Annex J (normative) Worst Case Analysis - DRD

J.1 Introduction

The purpose of the WCA is to demonstrate that the item being analysed performs within specification despite particular variations in its constituent part parameters and the imposed environment.

J.2 Scope and applicability

This DRD establishes the data content requirements for the WCA.

J.3 References

J.3.1 Normative references

ECSS-Q-ST-30	Space product assurance - Dependability

J.3.2 Handbooks references

ECSS-Q-HB-30-01	Space product assurance – worst case analysis

J.4 Terms, definitions and abbreviated terms

The terms and definitions shall be in conformance with ECSS-S-ST-00-01 and clause 3 of ECSS-Q-ST-30.

J.5 Description and purpose

The WCA report describes the execution of the test and the results of the analysis.

It contains the method of analysis and the assumptions used. It describes the model, presents the results of the analysis and the conclusions.

Its principal use is to prove that the equipment is able to meet the specified performance requirements under worst case conditions of operation and to demonstrate sufficient operating margins for all operating conditions.

J.6 Application and interrelationships

The WCA is linked to other analyses such as:

- Radiation analysis,
- Thermal analysis.

J.7 Content

a. The WCA document shall include:

— assumptions applicable to the environmental condition,

— a list of the selected parts database with the worst case parameters,

— a description of the general methodology,

— an explanation of the numerical analysis technique,

— results and conclusion of the WCA.

Annex K (informative) Analyses applicability matrix

Scope of the Table K-1 is to present relation of documents associated to dependability activities to support project review objectives as specified in ECSS-M-ST-10.

NOTE This table constitutes a first indication for the data package content at various reviews. The full content of such data package is established as part of the business agreement, which also defines the delivery of the document between reviews.

The table lists the documents necessary for the project reviews (identified by "X").

The various crosses in a row indicate the increased levels of maturity progressively expected versus reviews. The last cross in a row indicates that at that review the document is expected to be completed and finalized.

NOTE All documents, even when not marked as deliverables in Table K-1, are expected to be available and maintained under configuration management as per ECSS-M-ST-40 (e.g. to allow for backtracking in case of changes).

Documents listed in Table K-1 are either ECSS-Q-ST-30 DRDs, or DRDs to other ECSS-Q-30-XX standards, or defined within the referenced DRDs.

Table K-1: Analyses applicability matrix

Document or DRD title	Phase												Applicable level	Remarks
	A	B		C	D		E					F		
	PRR	SRR	PDR	CDR	QR	AR	ORR	FRR	LRR	CRR	ELR	MCR		
Failure modes, effects and analysis/ failure modes, effects and criticality analysis	X	X	X	X	X	X							SS, SE, LL	ECSS-Q-ST-30-02 FMEA is generally requested for all projects. Typically FMECA is not performed for telecommunication, earth observation and scientific spacecrafts and for ground segments. Process FMECA is normally not required.
Hardware/software interaction analysis (HSIA)				X	X	X							SS, SE	ECSS-Q-ST-30-02 - Can be included in the FMECA. - Performed on specific project request.
Contingency analysis				X	X	X							SS, GS, SE	Annex D Can be included as part of the operations manual using inputs from FMECA and FDIR.
Fault tree analysis (FTA)	X	X	X	X	X	X							All	ECSS-Q-ST-40-12 Performed on specific project request
Common-cause analysis				X	X	X							SS, SE	Annex I Can be accomplished as part of FMECA / FTA.

Document or DRD title	Phase												Applicable level	Remarks
	A	B		C	D		E					F		
	PRR	SRR	PDR	CDR	QR	AR	ORR	FRR	LRR	CRR	ELR	MCR		
Reliability prediction	X	X	X	X	X	X							All	Annex E See also ECSS-Q-HB-30-08
Worst case analysis (WCA)				X	X	X							LL (electrical equipment)	Annex J See also ECSS-Q-HB-30-01
Part stress analysis				X	X	X							LL (electrical equipment)	ECSS-Q-ST-30-11
Zonal analysis		X	X	X	X	X							SS, GS	Annex G Performed on specific project request (usually required on launchers)
Failure detection, isolation and recovery (FDIR)		X	X	X	X	X							SS, GS	Annex F
Maintainability analysis		X	X	X	X	X							GS	Annex H Only when maintenance activities are required
Availability analysis		X	X	X	X	X							All (outage inputs, only, from LL)	ECSS-Q-ST-30-09

Annex L (informative) Common-cause check lists

item	Common-cause Design check list
1	Prime and redundant items have independent power supplies.
2	Thermal decoupling between power supplies is maximised.
3	Independent data buses.
4	Bus I/F circuits designed to ensure faults do not lock out the bus.
5	Ideally, separate connectors serve prime and redundant functions (i.e. power, data, etc).
5.1	When item 5 is not possible, as occasionally, space considerations can make it difficult to achieve, wires to prime and redundant functions should be separated within the connector by unused pins.
6	Prime and redundant functions are in separate boxes / housings where possible.
6.1	When item 6 is not possible, is isolation between prime and redundant areas / components incorporated to reduce the likelihood of failure propagation, i.e. thermal effects, capacitance effects, etc, impacting on both prime and redundant functions.
7	In equipments with internal redundancy, the prime and redundant circuits use separate integrated circuits, and there is minimal use of common/shared printed circuit boards.
	<u>Where item 7 is not possible then:</u>
7.1	Is isolation between prime and redundant areas / components been incorporated to reduce the likelihood of failure propagation, i.e. thermal effects, propagation of stray capacitance effects, impacting on both prime and redundant functions.
7.2	Has isolation between high dissipation elements / heat sensitive elements been considered

item	Common-cause Design check list
7.3	Has placement of vias through nominal and redundant circuit planes in the multilayered circuit board been considered to eliminate Common-cause effects
7.4	Item 5 or 5.1 is satisfied
7.5	Has the design of the wiring layout for solder joints and PCD conductive tracks been considered to eliminate Common-cause effects (sufficient separation of solder joints, wires and tracks).
7.6	Has individual components with multi-application only been used by one nominal or redundant path.
8	Control and monitoring functions use separate integrated circuits, (e.g. those ICs which feature quadruple functionality). (A potential common mode failure case).
9	Protection and protected functions use separate integrated circuits, (e.g. those ICs which feature quadruple functionality). (A potential common mode failure case).
10	Pins / connections with shared / multiple wires do not cause Common-cause effects
11	All vent hole sizing is adequate
12	There is no contact between metals with electrochemical potentials > 0,5 V (metallic contamination does not cause short / open failures).
13	Software errors do not cause Common-cause effects
14	EEE Parts Procurement (parts quality, failure alerts, common parts with known weakness etc.) are respected.
15	All grounding or shielding is adequate between nominal and redundant paths
16	Pin, wire sizing and PCB tracks are compatible with the over current protection
17	Equipment level requirements are not erroneous, inconsistent or contradictory
18	Material selection does not introduce Common-cause affects (surface degradation, weakening, fracture, etc)

item	Common-cause Environment check list
1	The total dose levels of solar radiation (protons, alpha and beta particles, EM) do not exceed component tolerance thresholds.
2	Heavy ion radiation does not cause Bit-flip events in digital signals. Sufficient shielding is provided
3	Heavy ion radiation does not cause Single event burn-out (SEB) of power MOSFET junctions. Sufficient shielding is provided
4	Relays (or other sensitive components) do not change state due to vibration (in particular during launch, which is the most severe operating case). Location of components considered to minimise this effect
5	Magnetic field interaction, e.g. from unit power transformers or motors, do not cause Common-cause effects
6	Micrometeoroid impact and penetration does not cause damage
7	Contamination due to foreign bodies / debris
8	Thermal control failures do not affect prime and redundant equipments

item	Common-cause Unexpected operations check list
1	No incorrect commands are sent from ground control segment (GSC) to Payload
2	Incorrect TC sent within Payload
3	Heavy ion radiation does not cause Single event burn-out (SEB) of power MOSFET junctions
4	Relays (or other sensitive components) do not change state due to vibration (in particular during launch, which is the most severe operating case). Location of components considered to minimise this effect.
5	Magnetic field interaction, e.g. from unit power transformers or motors, do not cause Common-cause effects
6	Space debris or micrometeoroid impact and penetration does not cause damage

Bibliography

ECSS-S-ST-00	ECSS system – Description, implementation and general requirements
ECSS-Q-ST-30-09	Space product assurance — Availability analysis
ECSS-Q-ST-40	Space product assurance – Safety
ECSS-Q-ST-40-12	Space product assurance — Fault tree analysis - Adoption notice ECSS/IEC 61025
ECSS-Q-ST-80	Space product assurance — Software product assurance
ECSS-Q-HB-30-01	Space product assurance — Worst case analysis
ECSS-Q-HB-30-08	Space product assurance — Component reliability data sources and their use
ECSS-Q-HB-80-03	Space product assurance - Software dependability and safety methods and techniques
ECSS-Q-TM-30-12	Space product assurance — End of life parameter drifts
ECSS-E-ST-70-11	Space engineering — Space segment operability
ECSS-M-ST-10	Space project management – Project planning and implementation
ECSS-M-ST-40	Space project management – Configuration and information management
ECSS-M-ST-80	Space project management – Risk management