ECSS-Q-30B
8 March 2002

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Dependability

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

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

ISSN: 1028‐396X

Price: € 10

Printed in 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.

The formulation of this Standard takes into account the existing ISO 9000 family of standards.

Significant changes between this version and the previous version are:

- addition of clause 6 “Dependability risk reduction and control”, and
- harmonization of other clauses resulting from new clause 6 and other published ECSS Standards since 1996.

This Standard has been prepared by the ECSS Product Assurance Working Group, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

This version B cancels and replaces ECSS-Q-30A.

(This page is intentionally left blank)

Contents

Figures

(This page is intentionally left blank)

1
Scope

This Standard defines the requirements for a dependability (reliability, availability and maintainability) assurance programme for space projects in order to comply with the ECSS policy as defined in ECSS-Q-00.

It defines the dependability requirements for space products. The requirements for the assurance of software products are defined in ECSS-Q-80. The dependability requirements for system functions implemented in software, and the interaction between hardware and software, are defined in this Standard.

The provisions of this document apply to all programme phases.

When viewed from the perspective of a specific project context, the requirements defined in this Standard should be tailored to match the genuine requirements of a particular profile and circumstances of a project.

NOTE Tailoring is a process by which individual requirements of specifications, standards and related documents are evaluated and made applicable to a specific project by selection, and in some exceptional cases, modification of existing or addition of new requirements.
[ECSS-M-00-02A, clause 3]

(This page is intentionally left blank)

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 revisions of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references the latest edition of the publication referred to applies.

ECSS-P-001	Glossary of terms
ECSS-Q-00	Space product assurance — Policy and principles
ECSS-Q-20	Space product assurance — Quality assurance
ECSS-Q-40B	Space product assurance — Safety
ECSS-Q-80	Space product assurance — Software product assurance
ECSS-M-40	Space project management — Configuration management

(This page is intentionally left blank)

3

Terms, definitions and abbreviated terms

3.1 Terms and definitions

The following terms and definitions are specific to this Standard in the sense that they are complementary or additional to those contained in ECSS‐P‐001.

3.1.1
failure scenario

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

3.1.2
risk

quantitative measure of the magnitude of a potential loss and the probability of incurring that loss

[ECSS‐P‐001]

NOTE 1 In clause 6 of this Standard, unless it is specifically addressed by the term "dependability risk", the term "risk" is as defined in ECSS‐P‐001.

NOTE 2 In the context of this Standard, risk is related to the potential loss or degradation of the required technical performances, that affects the attainment of dependability objectives.

3.1.3
undesirable event

an event whose consequences are detrimental for the success of the mission related to the technical performances

[ISO/IEC 12207:1995]

3.2 Abbreviated terms

The following abbreviated terms are defined and used within this Standard.

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

FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FTA	fault tree analysis
MMI	man-machine interface
NRB	nonconformance review board
PA	product assurance
QA	quality assurance
TRB	test review board
WCA	worst case analysis

4

Policy and principles

4.1 Objectives

The objective of dependability assurance is to ensure a successful mission by optimizing the system dependability within all competing technical and financial constraints.

Dependability assurance is a continuous and iterative process throughout the project life cycle, using quantitative and qualitative approaches, with the aim of

- identifying all technical risks to satisfy functional requirements which can lead to nonconformance with reliability, availability and maintainability requirements,
- providing related risk assessment,
- defining reduction and control measures, as part of the risk management process implemented on the project, and
- ensuring conformance to reliability, availability and maintainability requirements.

4.2 Basic approach

To achieve the objectives of dependability, dependability assurance is implemented according to a logical process.

This process starts in the conceptual design phase at the highest level of the functional tree with a top-down definition of tasks and requirements to be implemented. Results achieved at all levels of the functional tree are controlled and used in a bottom-up approach so as to consolidate dependability assurance of the product.

This process includes the following types of activities:

- definition, organization and implementation of the dependability programme, as defined in clause 5;
- dependability risk identification, reduction and control, as defined in clause 6;
- dependability engineering, as defined in clause 7;
- dependability analyses, as defined in clause 8;
- dependability testing, demonstration and data collection, as defined in clause 9.

(This page is intentionally left blank)

5 Dependability programme management

5.1 Organization

The contractor shall implement the dependability (reliability, availability and maintainability) assurance as an integral part of his product assurance discipline as defined in ECSS-Q-00.

5.2 Dependability programme planning

5.2.1

The contractor shall develop, maintain and implement a dependability plan for all programme phases that describes how compliance with the dependability programme requirements is demonstrated. The plan shall address the applicable requirements of this document.

5.2.2

For each product, the extent that dependability assurance is applied shall be adapted to the severity (as defined in subclause 7.3.1) of the consequences of failures at system level. For this purpose, products shall be classified into appropriate categories that are defined in accordance with the risk policy of the project.

5.3 Dependability critical items

5.3.1

Dependability critical items are identified by dependability analyses performed to support the risk reduction and control process performed on the project. The criteria for identifying dependability critical items are given in subclause 6.4.

5.3.2

Dependability critical items shall be subject to risk assessment and critical items control in accordance with ECSS-Q-00.

a. The control measures shall include:

1. a review of all design, manufacturing and test documentation related to critical functions, critical items and procedures to ensure that appropriate measures are taken to control the item having a bearing on its criticality;

2. dependability participation on nonconformance review boards (NRB), failure review boards, configuration control boards and test review boards (TRB), and the approval process for waivers and deviations, to ensure that dependability critical items are disposed with due regard to their criticality.

b. The dependability aspects shall be considered within the entire verification process for dependability critical items until close out.

5.4 Design reviews

5.4.1

The contractor shall ensure that all dependability data for a design review are complete to a level of detail consistent with the objectives of the review and are presented to the customer in accordance with the project review schedule.

5.4.2

The contractor shall ensure that dependability aspects are duly considered in all design reviews.

5.4.3

All dependability data submitted shall clearly indicate the design baseline upon which it is based and shall be coherent with all other supporting technical documentation.

5.4.4

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

5.5 Audits

The audits as specified in ECSS-Q-20 shall include the dependability activities to verify conformance to the project dependability plan and requirements.

5.6 Use of previously designed, fabricated, qualified or flown items

5.6.1

Where the contractor proposes to take advantage of previously designed, manufactured qualified or flown elements in his system, he shall demonstrate that the proposed elements do conform to the dependability assurance requirements of the design specification.

5.6.2

Nonconformances to dependability assurance requirements shall be identified and the rationale for retention of unresolved nonconformances shall be provided by a waiver request in accordance with requirements in ECSS-M-40.

5.7 Subcontractor control

General requirements for the control of subcontractors are defined in ECSS-Q-00. In particular, the contractor shall be responsible for ensuring that products obtained from subcontractors meet the dependability requirements specified for the overall system.

5.8 Progress reporting

The contractor shall report dependability progress to the customer as part of product assurance activities as required in ECSS-Q-00.

5.9 Documentation

5.9.1

The contractor shall maintain all data used for the dependability programme. The file shall contain the following as a minimum:

a. dependability analyses, lists, reports and input data;

b. dependability recommendation status log.

5.9.2

In accordance with the business agreement upon request the customer shall have access to project dependability data.

(This page is intentionally left blank)

6

Dependability risk reduction and control

6.1 General

As part of the risk management process implemented on the project (see ECSS-M-00-03), the contractor shall analyse, reduce and control all dependability risks that lead to the nonconformance to dependability requirements, i.e. all risks of degradation or loss of technical performances required for the product.

Dependability risk analysis reduction and control shall be implemented according to the process presented in Figure 1, and shall include the following steps:

a. identification and classification of undesirable events according to the severity of their consequences;

b. analysis of failure scenarios, determination of related failure modes, failure origins or causes;

c. classification of functions and associated products into criticality categories, allowing definition of appropriate tailoring of risk reduction efforts in relation with their criticality;

d. definition of actions and recommendations for detailed risk assessment, risk elimination, or risk reduction and control to an acceptable level;

e. implementation of risk reduction;

f. decisions on risk reduction and risk acceptance;

g. verification of risk reduction, assessment of residual risks.

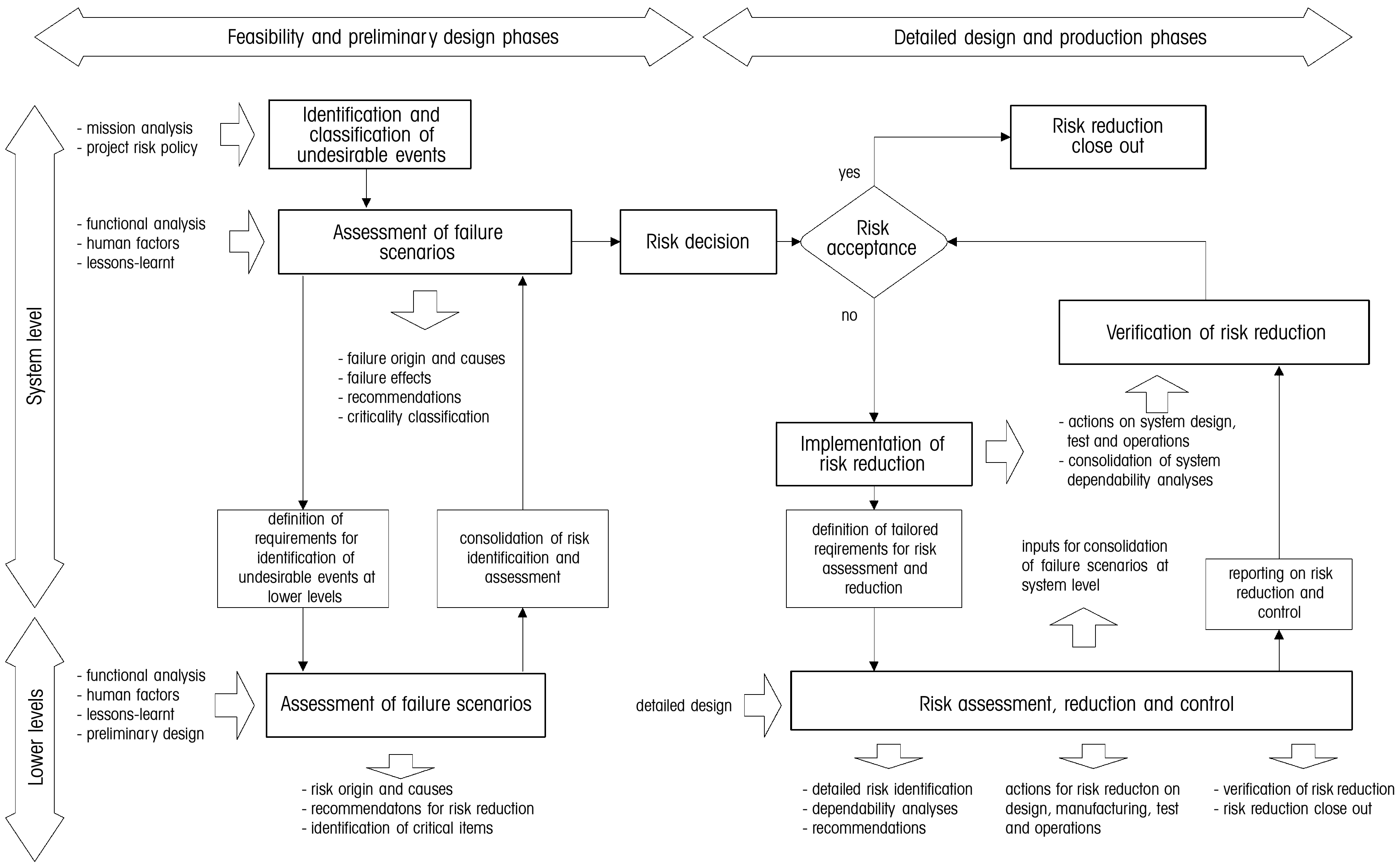
Feasibility and preliminary design phases
Detailed design and production phases
System level
Lower levels
- mission analysis
- project risk policy
Identification and classification of undesirable events
- functional analysis
- human factors
- lessons-learnt
Assessment of failure scenarios
Risk decision
Risk acceptance
yes
no
Risk reduction close out
Verification of risk reduction
- failure origin and causes
- failure effects
- recommendations
- criticality classification
Implementation of risk reduction
- actions on system design, test and operations
- consolidation of system dependability analyses
definition of requirements for identification of undesirable events at lower levels
consolidation of risk identification and assessment
definition of tailored reqirements for risk assessment and reduction
inputs for consolidation of failure scenarios at system level
reporting on risk reduction and control
- functional analysis
- human factors
- lessons-learnt
- preliminary design
Assessment of failure scenarios
detailed design
Risk assessment, reduction and control
- risk origin and causes
- recommendatons for risk reduction
- identification of critical items
- detailed risk identification
- dependability analyses
- recommendations
actions for risk reducton on design, manufacturing, test and operations
- verification of risk reduction
- risk reduction close out

Figure 1: Dependability risk reduction and control

6.2 Identification and classification of undesirable events

6.2.1

The contractor shall provide identification of undesirable events leading to the loss or degradation of product performances, together with their classification into categories related to the severity of their consequences (see subclause 7.3.1).

6.2.2

Preliminary identification and classification of undesirable events shall be determined from analysis of criteria for mission success, during conceptual and preliminary design phases. The undesirable events to be considered at the highest product level (overall system including space and ground segments) shall be all events whose occurrence can jeopardize, compromise, or degrade the mission success. At lower levels of the product tree (space segment, ground segment, subassemblies and equipment), the undesirable events to be considered shall be the product failure effects which can induce the undesirable events identified for the highest product level.

6.2.3

Identification and classification of undesirable events shall be consolidated after assessment of failure scenarios (see subclause 6.3).

6.3 Assessment of failure scenarios

6.3.1

The contractor shall investigate the possible scenarios leading to the occurrence of undesirable events, and shall identify related failure modes, failure origins and causes, detailed failure effects.

6.3.2

In conceptual and preliminary design phases, the following analyses shall be performed for preliminary determination and assessment of the failure scenarios:

a. Analysis of functional failures (i.e. failures of the functions involved into realization of the product mission) using functional FMEA, as defined in subclause 8.2.2, which allows to determine the effects (induced risks) for each function: loss, degradation and untimely occurrence. The functions shall be previously defined (the functional analysis can be used for this purpose).

b. The analysis of functional failure shall be conducted for each phase of the product life cycle considering all modes of operations in their actual sequence of implementation throughout the mission with the purpose to identify undesirable events induced by erroneous sequencing (e.g. loss of synchronism and untimely operations).

c. Potential propagation of failures between different functions shall be investigated.

d. Analysis of failure modes associated to human factors in performance of operations.

e. Analysis of potential application to the product of typical failure modes already observed from past experience on similar products or missions.

6.3.3

In the detailed design phase the assessment of failure scenarios shall be consolidated by considering the following additional contributions:

a. analysis of specific failure modes and failure effects induced by the selected design which cannot be detected by analysis of functional failure;

b. zonal analysis for detection of potential failure propagation paths induced by proximity of elements.

6.4 Criticality classification of functions and products

a. During the preliminary design phase, the contractor shall classify functions, operations and products into criticality categories.

b. The criticality category of functions and operations shall be directly related to the severity of the consequences resulting from failure of the function or operation (e.g. a function whose failure induces a catastrophic consequence shall be classified with the highest criticality level).

c. The criticality category of products (hardware and software) shall be the highest criticality category of the functions associated to the product.

d. The criticality classification shall be used to focus efforts on the most critical areas.

6.5 Actions and recommendations for risk reduction

The contractor shall define actions and recommendations for risk reduction up to an acceptable level.

In definition of the risk reduction, the following measures shall be considered:

a. detailed risk assessment based on performance of dedicated dependability analyses, and in specific cases, performance of dependability tests. A selection and tailoring of the dependability analyses presented in clause 8 shall be defined according to the nature and the criticality category of the product;

b. elimination of failure causes, reduction of failure occurrence probability, reduction of failure effects, monitoring and control of the failure scenarios, by actions on the design or operations as presented in subclauses 7.3.2, 7.3.3 and 7.5.3.

6.6 Risk decisions

6.6.1

The contractor shall make and document decisions on risk acceptance and actions for risk reduction.

6.6.2

Decisions shall be based on established criteria defined within the project risk policy, considering technical and programmatic implications.

6.6.3

Decisions shall be taken, controlled and implemented within the risk management process applied on the project, in accordance with requirements defined in ECSS-M-00-03.

6.7 Verification of risk reduction

a. The contractor shall perform appropriate verifications in order to ensure that identified risks have been eliminated or reduced to an acceptable level.

b. Verifications shall include

1. monitoring and close out verification of actions and recommendations,
2. review of detailed risk assessment from dependability analyses,
3. reassessment of residual risks, verification of acceptability with reference to applicable criteria defined in the project risk policy, and
4. identification of problem areas.

c. Results shall be reported to the project risk management for acceptance or complementary decisions.

6.8 Documentation

a. Documentation on dependability risk analysis reduction and control shall be established, controlled and maintained throughout the project implementation, in order to provide

- visibility on results and progress of risk identification, assessment and reduction,
- definition of applicable requirements at lower level of the product tree,
- appropriate justifications of decisions on risk reduction and risk acceptance, and
- traceability, for each risk, to all pertinent analyses, results, data, decisions and close out status.

b. Documentation shall include

- identification and classification of undesirable events,
- identification of failure scenarios, failure modes, causes and effects,
- criticality classification of functions and products,
- requirements at lower level of the product tree,
- definition of actions and recommendations,
- dependability analyses, as needed for the purpose of risk assessment and reduction,
- risk reduction status, and
- records of risk reduction and associated rationale.

(This page is intentionally left blank)

7

Dependability engineering

7.1 Integration of dependability in the project

7.1.1

Dependability is an inherent characteristic of a system or product. Dependability shall be integrated with safety during the design process. The dependability characteristics shall be traded with other system attributes such as mass, size, cost and performance during the optimization of the design.

7.1.2

Dependability issues shall be considered in all trades, in all phases of the project beginning with the conceptual phase. Manufacture, assembly, integration, test and operations shall not degrade dependability attributes introduced into the design.

7.1.3

The results of dependability analyses, tests and demonstrations shall be reiterated in a timely manner through the design, testing, and all fabrication/integration processes until all threats to dependability objectives are eliminated, or rationale has been provided for the acceptance of those threats that remain.

7.1.4

Emphasis on dependability assurance shall be placed on either the design or manufacturing process depending on the project phase.

7.2 Dependability requirements in technical specification

Dependability requirements shall be taken into account during the preparation and review of design and test specifications. The main objective shall be to implement the findings of dependability analyses, and to verify that accepted dependability engineering recommendations have been incorporated in the relevant technical specifications. These specifications shall include

a. functional, operational and environmental requirements,

b. test requirements including stress levels, test parameters, and accept/reject criteria,

c. design performance margins, derating factors, quantitative dependability requirements, and qualitative dependability requirements (identification and classification of undesirable events), under specified environmental conditions,

d. human factors where human error is a consideration in mission success,

e. the degree to which the design shall be tolerant to failures of hardware or software,

f. the detection, isolation, diagnosis, and recovery of the system from failures and its restoration to an acceptable state,

g. the prevention of failures crossing interfaces with unacceptable consequences,

h. definition of the maintenance concept,

i. maintenance tasks and requirements for special skills, and

j. requirements for preventive maintenance, special tools, and special test equipment.

7.3 Dependability design criteria

7.3.1 Consequence category and severity

a. Consequence category

Mission success and safety can be jeopardized by system element failure or by hazardous events, of which the consequences shall be classified according to the following categories:

- loss of life, or injury to personnel;
- loss of mission, loss of the system, or damage to public or private property;
- detrimental environmental effects;
- degradation of mission objectives or performances;
- user dissatisfaction.

b. Consequence severity

The consequences shall be quantified by their severity, which is a measure of the magnitude of the consequence. The severity of a consequence shall be classified according to the following scale, in accordance with the criteria defined by each project in its risk policy:

- catastrophic
- critical
- major
- significant
- negligible

c. Severity of hazardous events shall be classified as defined in ECSS‐Q‐40B subclause 5.3.1.

7.3.2 Failure tolerance

a. The contractor shall verify the capability of the design to sustain single or multiple failures in accordance with failure tolerance requirements defined in the performance specifications.

b. This verification shall address all failure modes whose severity of consequence is classified as catastrophic, critical and major according to the project risk policy.

7.3.3 Design approach

a. The contractor shall develop and implement design criteria to improve reliability and to facilitate maintenance actions in predicted environments. In establishing reliability and maintainability design criteria the contractor shall use data obtained from previous programmes when appropriate data is available.

b. The contractor shall ensure that reliability is built into the design using fault tolerance and design margins. He shall assess the failure characteristics of systems to identify areas of design weakness and propose corrective solutions.

c. In implementation of availability and reliability into the design, the following methods shall preferably apply:

- functional design:
  - implementation of failure tolerance;
  - 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;
  - 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.
- physical design:
  - application of proven design rules;
  - preferred use of design that has performed successfully in the intended mission environment;
  - selection of parts having an appropriate quality level;
  - use of EEE parts derating and stress margins for mechanical parts;
  - optimum use of design techniques for redundancy (while keeping system design complexity as low as possible);
  - maximization of inspectability and testability of built-in equipment;
  - providing accessibility to equipment.

7.4 Involvement in test definition

7.4.1

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

7.4.2

The dependability discipline shall support

a. definition of test characteristics and test objectives,

b. selection of measurement parameters, and

c. statistical evaluation of test results.

7.5 Involvement in operational aspects

7.5.1

The contractor shall ensure that dependability cognizant and qualified staff

a. contribute to definition of operations manual and procedures, and

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

7.5.2

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

7.5.3

These analyses shall take into account the technical and human environment, and shall verify that the procedures

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

b. do not compromise equipment reliability;

c. are in accordance with established maintenance dispositions; and

d. include dispositions proper to minimize failures due to human errors.

7.6 Dependability recommendations

7.6.1

The contractor shall establish and maintain a system to track the dependability recommendations, in order to support the risk reduction process. These recommendations shall be derived from the reliability and safety analyses, the maintainability analyses or dependability and safety trade-off studies.

7.6.2

All recommendations shall be justified and formal evidence of acceptance or rejection of the recommendation by the contractor's management shall be documented and tracked.

7.6.3

An accepted dependability recommendation shall be included as a requirement in the relevant applicable documentation.

8

Dependability analysis

8.1 Dependability analysis and the project life cycle

8.1.1

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

8.1.2

Dependability analyses shall be performed initially to establish the conceptual design, and the system requirements. Thereafter, 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.

8.1.3

Dependability analyses shall be implemented in order to

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

b. identify all potential failure modes and technical risks with respect to functional requirements that can lead to nonconformance of dependability requirements, provide risk assessment and risk reduction and control measures in line with the risk management process implemented on the project.

8.1.4

The results of dependability analyses shall be incorporated into the design justification file.

8.2 Dependability analytical methods

8.2.1 General

a. Dependability analyses shall be conducted on all appropriate levels of the space system.

b. The main purpose of all dependability analyses shall be 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.

c. The methods identified in subclauses 8.2.2 to 8.2.4 shall be used, tailored to match the generic requirements on each project, to address the hardware, software and human functions comprising the system. A consistent set of analyses selected from these subclauses shall be defined early in the project, the justification being based on added value and cost impact.

8.2.2 Reliability analyses

These analyses can also be used for the purpose of determining maintainability and availability objectives and tasks. The following analyses used for reliability analysis are also used for determining maintainability and availability requirements and tasks:

a.

1. Failure modes effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA) shall be performed on the functional and physical design (functional FMEA/FMECA and hardware FMEA/FMECA respectively), and the processes used to realize the final product (Process FMECA).
2. All potential failure modes shall be identified and classified according to the severity (FMEA) or criticality (FMECA) of their consequences. 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.
3. 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.
4. Provisions for failure detection and recovery actions shall be provided as part of the FMEA/FMECA.
5. The FMEA/FMECA shall be used to support the reliability modelling and the Reliability and Safety Analyses.
6. Principles, requirements and procedures to apply FMEA/FMECA are described in ECSS-Q-30-02.

b. Hardware-software interaction analysis shall be performed to ensure that the software is designed to react in an acceptable way to hardware failure. This shall be performed at the level of the technical specification of the software. The hardware-software interaction analysis can be included in the FMEA/FMECA.

c. Contingency analysis shall be performed to identify all contingencies arising from failures of the system. The analysis shall identify the means to prevent, contain and limit each contingency, and detect and diagnose it to recover the system to a nominal or degraded state.

NOTE The contingency analysis is a system level task.

d. A fault tree analysis (FTA) shall be used to verify that the design conforms to the failure tolerance requirements for combinations of failures. Principles, requirements and procedures to apply FTA are described in ECSS-Q-40-12.

The prime contractor shall perform FTA to identify possible event combinations leading to the undesirable end event “loss of mission”. Subsystem contractor shall support 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.

e. Common-mode and common-cause analyses shall be performed on reliability and safety critical items to identify the root cause of failures that have a potential to negate failure tolerance levels (see subclause 7.3.2). This analysis can be accomplished as part of FMEA/FMECA or FTA. Principles, requirements and procedures to perform the analysis are described in ECSS-Q-40-10.

f. Reliability requirements shall be apportioned to set reliability requirements for lower level products.

g. Reliability prediction techniques shall be used to optimize the reliability of a design against competing constraints such as cost and mass, to predict the in-service reliability of a product and to provide failure probability data for purposes such as risk assessment.

The failure rates and methods used in reliability predictions shall be as specified by the customer. Reliability models shall be prepared to support predictions and FMEA/FMECA.

h. Worst case circuit performance analysis (WCCPA) (see ECSS-Q-30-01) shall be performed on electronic/electrical equipment to demonstrate that it performs within specification despite particular variations in its constituent part parameters and the imposed environment. WCA shall be accomplished at equipment level.

i. Part derating shall be performed to assure that the stress levels applied to all EEE parts are within the limits specified by the project. Databases for derating factors of EEE parts are presented in ECSS-Q-60-11. Part derating analyses shall be performed at equipment level.

j. Zonal analysis (see subclause 8.2.3 d.) should be used to insure there is no failure propagation.

8.2.3 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 predictions shall be performed at system level and used as a design tool to assess and compare design alternatives with respect to specified maintainability quantitative requirements.

These analyses shall be performed considering the

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

c. Scheduled maintenance analysis shall be performed at system level to determine the optimum scheduled maintenance plan that which minimizes the amount of support resources necessary to sustain the required safety level and mission capabilities and minimizes down time.

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

d. Zonal analysis shall be undertaken at system level to determine the optimal location for each product as regards accessibility, testability and repairability.

e. The maintainability analyses shall identify maintainability critical items which, as a minimum, shall include products that cannot be checked and tested after integration, limited-life products, products that do not meet, or cannot be validated as meeting, applicable maintainability requirements.

8.2.4 Availability analyses

a. The contractor shall perform availability analyses or simulations in order to assess the availability of the system. The results are used to

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

b. The contractor shall perform the outage analyses in order to supply input data for availability analyses. The analysis output includes a list of all potential outages identified (as defined in the project), their causes, probabilities of occurrence and duration. Instead of outage probabilities, failure rates associated with outages can be provided. Furthermore, the means of outage detection and the recovery methods shall be identified in the analysis.

c. The availability predictions/assessments shall be carried out at system level using the system reliability and maintainability models as well as the data from the outage analyses.

8.3 Classification of design characteristics in production documents

a. In support of the risk reduction and control process that shall be implemented for dependability critical items, the contractor shall classify the design characteristics of his product in order to highlight those areas of his product to which specific attention, control or verification shall be applied. This is an integrated effort of the dependability and QA disciplines (see ECSS-Q-00).

b. The classification and ranking of design characteristics provide for:

- drawing the attention of the engineering, production and test personnel to those characteristics of the product that are essential for the correct functioning of the product;
- defining appropriate integration, test and inspection methods, techniques, resources to be applied, and selection of the production facilities according to the design characteristics;
- taking all precautions to conform to the requirements imposed by the design characteristics, e.g. environmental control;
- achieving properly adapted and coherent classification and processing of nonconformances, changes and waivers.

c. The customer shall define the classification criteria in the project requirements documents. Alternatively, by agreement, the contractor may propose the classification criteria in his product assurance plan.

8.4 Critical items list

8.4.1

All critical items identified through the various dependability analyses shall be documented in a critical items list and subjected to management and control as defined in ECSS-Q-00. The documentation for each critical item shall include a justification for retention of that item that shall be subject to approval by the customer.

8.4.2

As a minimum items with single-point failure and at least a failure consequence severity classified as catastrophic, critical or major, shall be listed as a critical item.

8.4.3

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 listed as critical items.

8.4.4

Further classifications shall be determined by the customer (e.g. parts not meeting the derating requirements, wear-out times, limited-life items, or items with an extremely high failure probability) in line with the risk management policy defined on the project.

(This page is intentionally left blank)

9

Dependability testing, demonstration and data collection

9.1 Dependability testing and demonstration

9.1.1

Reliability testing and demonstration shall be performed according to the project requirements documents in order to

a. validate failure modes and effects,

b. check failure tolerance, failure detection and recovery,

c. obtain statistical failure data to support predictions and risk assessment,

d. consolidate reliability assessments,

e. validate the capability of the hardware to operate with software or to be operated by a human being in accordance with the specifications,

f. demonstrate the reliability of critical items, and

g. validate or justify data bases used for theoretical demonstrations.

9.1.2

Maintainability shall be demonstrated as performing the verification of the applicable maintainability requirements and to ensure that preventive and corrective maintenance activities is successfully performed within the scope of the maintenance concept.

9.1.3

“The maintainability demonstration” shall verify the ability to:

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

b. remove and replace each line replaceable unit or orbit replaceable unit;

c. perform mission-essential repairs that are not intended to be accomplished by replacements;

d. check that the product is fully functional after maintenance actions have been completed;

e. demonstrate that no safety hazard is introduced as a result of maintenance actions;

f. demonstrate that the maintenance operations can be performed within the applicable constraints (e.g. time and volume or accessibility). This shall include the operations necessary to prepare a system during the launch campaign, e.g. “remove-before-flight” items or replacement of batteries.

9.2 Dependability data collection and dependability growth

Dependability data shall be collected during space system development from sources such as nonconformance and problem or failure reports, and maintenance reports. These data shall be based on actual test or flight experience, and shall include the amount and mode of items use including their stresses and operational profile. Dependability data shall also be used for dependability performances monitoring and dependability growth monitoring through agreed or specified models.

Annex A (informative)

Relationship between dependability activities and programme phases

A.1 Feasibility phase (phase A)

In this phase the dependability assurance tasks shall be 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.2 Preliminary definition phase (phase B)

In this phase the dependability assurance tasks shall be to:

a. continue 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 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.3 Detailed definition and production/ground qualification testing phases (phase C/D)

In this phase the dependability assurance tasks shall be 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. supervise the collection of dependability data.

A.4 Utilization phase (phase E)

In this phase the dependability assurance tasks shall be to:

a. support flight readiness reviews;

b. support ground and flight operations;

c. monitor the design change traffic and its impact on dependability resulting from design evolution;

d. investigate dependability related flight anomalies;

e. supervise collection of dependability data during operations.

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 contractor-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 contract documentation requirements established by this Standard:

- dependability plan;
- failure modes, effects (and criticality) analysis - FMEA/FMECA;
- hardware-software interaction analysis;
- common mode and common cause analysis;
- fault tree analysis;
- contingency analysis;
- scheduled maintenance analysis;
- zonal analysis;
- dependability apportionment;
- dependability assessment;
- outage analysis;
- worst case analysis;
- part derating analysis;
- dependability critical items list;
- report on risk identification, assessment, reduction and control.

(This page is intentionally left blank)

Bibliography

The following documents, referenced in this Standard, define principles, requirements and procedures that may be applied to facilitate the implementation of this Standard:

ECSS-M-00-02A	Space project management — Tailoring of space standards
ECSS-M-00-03	Space project management — Risk management
ECSS-M-30	Space project management — Project phasing and planning
ECSS-Q-30-01 [1]	Space product assurance — Worst case analysis
ECSS-Q-30-02	Space product assurance — Failure modes, effects and criticality analysis (FMECA)
ECSS-Q-40-10 [1]	Space product assurance — Common cause and common failure mode analysis
ECSS-Q-40-12	Space product assurance — Fault tree analysis - Adoption notice ECSS/IEC 61025
ECSS-Q-60-11 [1]	Space product assurance — EEE components — Derating and end of life parameter drifts
ISO/IEC 12207:1995	Information technology — Software life cycle processes

[1] To be published.

(This page is intentionally left blank)

ECSS Document Improvement Proposal

1. Document I.D. ECSS-Q-30B	**2. Document date** 8 March 2002	**3. Document title** Dependability
4. Recommended improvement (identify clauses, subclauses and include modified text or graphic, attach pages as necessary)		
5. Reason for recommendation		
6. Originator of recommendation		
Name:	Organization:	
Address:	Phone: Fax: e-mail:	**7. Date of submission:**
8. Send to ECSS Secretariat		
Name: W. Kriedte ESA-TOS/QR	Address: ESTEC, P.O. Box 299 2200 AG Noordwijk The Netherlands	Phone: +31-71-565-3952 Fax: +31-71-565-6839 e-mail: Werner.Kriedte@esa.int

Note: The originator of the submission should complete items 4, 5, 6 and 7.

This form is available as a Word and Wordperfect-file on internet under
http://www.ecss.nl

(This page is intentionally left blank)