ECSS–Q–30A
19 April 1996

Space Product Assurance

Dependability

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

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

Price: 35 Dutch Guilders

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 must be accomplished, rather than in terms of how to organise and perform the necessary work. This allows existing organisational 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 documents.

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 page is intentionally left blank)

Contents List

Tables

1

General

1.1 Scope

This standard defines the requirements for a Dependability (Reliability, Availability and Maintainability) Assurance programme for European Space Projects in order to comply with the ECSS policy as defined in ECSS–Q–00.

It defines the Dependability requirements for the complete space product. The requirements for the assurance of software products are contained in ECSS–Q–80; the Dependability requirements for system functions implemented in software, and the interaction between hardware and software, are defined in this document.

1.2 Objectives

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

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

- ensuring that reliability, availability and maintainability targets are met,
- identifying all technical risks with respect to functional needs, which can lead to non–achievement of 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.

1.3 Basic Approach

System Dependability requirements will be defined by the customer and will appear in the appropriate specifications.

The contractor shall make a Dependability apportionment of system requirements and allocate these to lower levels, and impose Dependability requirements appropriate to that level in both qualitative and quantitative ways.

The contractor shall evaluate the Dependability characteristics of his products and their operation through a programme of analyses, reviews and demonstrations.

The contractor shall implement a Dependability risk management which supports the Project Risk Management Programme as defined by the requirements of ECSS–M–00. He shall conform to the requirements in sub–clause 3.3.5 of ECSS–Q–00. Dependability risk identification, reduction and control shall be an integral part of the overall risk management process.

1.4 Applicability

The provisions of this document also apply to all programme phases including concept, design, development, manufacturing, and operational phases.

The requirements of this document shall be tailored by the customer according to the type of programme and criticality of products. The tailored requirements shall be included in the Statement of Work (SOW) for each programme.

1.5 Normative Documents

This ECSS Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these apply to this ECSS Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

ECSS–P–001 ECSS Vocabulary

ECSS–Q–00 Product Assurance

ECSS–Q–20 Quality Assurance

ECSS–Q–40 Safety Assurance

ECSS–Q–80 Software Product Assurance

ECSS–M–00 Space Project Management

ECSS–M–30 Project Phases and Planning

1.6 Definitions and Abbreviations

1.6.1 Definitions

For the purposes of this standard, the definitions given in ECSS–P–001 Issue 1 apply. In particular, it should be noted that the following terms have a specific definition for use in ECSS standards.

Acceptance

Alert

Analysis

Anomaly

Approval

Audit

Availability

Business Agreement

Calibration

Configuration Management

Contingency Procedure

Contract

Contractor

Corrective Action

Critical Item

Criticality
Data
Demonstration
Dependability
Design
Development
Deviation
Document
Documentation
Equipment
Failure
Inspection
Maintainability
Maintenance
Mission
Nonconformance
Performance
Procedure
Process
Product
Product Assurance
Project
Qualification
Quality
Quality Assurance
Reliability
Repair
Requirement
Rework
Review
Risk
Safety
Service
Specification
Supplier
System
Tailoring
Test
Validation
Verification
Waiver

The following terms and definitions are specific to this standard and shall be applied.

"Overstress: a value of any parameter in excess of the specified design limits or in excess of a specified or rated value."

1.6.2 Abbreviations

The following abbreviations are defined and used within this standard.

Abbreviation	Meaning
EEE:	Electric, Electronic, Electromechanical
FMECA:	Failure Modes, Effects and Criticality Analysis
FTA:	Fault Tree Analysis
MRB:	Material Review Board
SOW:	Statement of Work
TRB:	Test Review Board

2

Dependability Programme Management

2.1 Organisation

2.1.1

The contractor shall organise Dependability assurance (Reliability, Availability and Maintainability) as an integral part of his Product Assurance discipline as defined in ECSS–Q–00.

2.2 Dependability Programme Planning

2.2.1

The contractor shall develop, maintain, and implement a Dependability programme plan as part of the overall Product Assurance Plan for each programme phase, which describes how compliance with the Dependability programme requirements will be assured. The plan shall address the applicable requirements of this document.

2.2.2

The programme shall lay down rules concerning the proper handling of the product throughout its life cycle so as to ensure that dependability aims are met.

2.2.3

For each product, the degree of dependability assurance shall be adapted to the severity of the consequences of product failures at system level. For this purpose, products shall be classified into appropriate categories which are defined in accordance with the risk policy of the project.

2.3 Dependability Critical Items

2.3.1

Dependability Critical Items shall be defined as a result of Dependability analyses performed with the aim of supporting the risk reduction and control process to be performed on the project. The criteria for identifying Dependability Critical Items are given in clause 4.4.

2.3.2

Dependability Critical Items shall be subject to Risk Assessment and Critical Items Control as required in clause 3.3.5 of ECSS–Q–00. The control measures shall include:

– 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 characteristics of the item having a bearing on its criticality;

– Dependability participation on Material Review Boards (MRB), 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;

– The Dependability function shall be included in the entire verification process for Dependability Critical Items until formal close-out.

2.4 Design Reviews

2.4.1

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 reviewing authority in accordance with the project review schedule.

2.4.2

The contractor shall ensure the participation of the Dependability disciplines in all design reviews

2.4.3

All Dependability data submitted shall clearly indicate the design baseline.

2.4.4

All changes shall be assessed for their impact on Dependability and a reassessment performed where necessary.

2.5 Audits

2.5.1

The contractor shall perform audits of his own and of his subcontractor‘s project activities as specified ECSS–Q–20 clause 2.6. These audits shall include the Dependability activities to verify compliance with the project Dependability policy and requirements, and to identify Dependability problem areas.

2.6 Use of Previously Designed, Fabricated or Flown Items

2.6.1

Where the contractor proposes to use previously designed, manufactured or flown elements in his system, he shall demonstrate that the proposed elements will comply with the Dependability assurance requirements of the design specification.

2.6.2

Nonconformances to requirements shall be identified and the rationale for retention shall be provided.

2.7 Subcontractor Control

2.7.1

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.

2.8 Progress Reporting

2.8.1

Dependability progress shall be reported by the contractor to the customer within normal Product Assurance and project progress reporting in accordance with the general requirements of ECSS–Q–00 sub–clause 3.3.3.e.

2.9 Documentation

2.9.1

The contractor shall maintain a project Dependability data file as part of his overall product assurance documentation system. The file shall contain the following as a minimum:

– Dependability analyses, lists, reports and input data;

– Dependability recommendation status log;

– Supporting analyses and documentation for any of the Dependability analyses.

2.9.2

The customer shall be allowed access, on request, to the data contained in the Dependability file.

(This page is intentionally left blank)

3

Dependability Engineering

3.1 Integration of Dependability in the Project

3.1.1

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 against other system attributes such as mass, size, cost and performance during the optimisation of the design.

3.1.2

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

3.1.3

Risks (Dependability) shall be assessed, and the processes for their reduction and control determined, jointly by Product Assurance, Engineering and Project Management.

3.1.4

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 have been eliminated, or rationale has been provided for the acceptance of those threats that remain.

3.1.5

Emphasis shall be placed on the appropriate aspects (design/manufacturing), depending on the project phase.

3.2 Dependability Requirements in Technical Specifications

3.2.1

Dependability requirements shall be taken fully into account during the preparation and review of design and test specifications. A principal goal shall be to implement the findings of Dependability analyses, and to verify that accepted Depend-

ability engineering recommendations have been incorporated in the relevant specifications. The specifications shall include:

– functional, operational and environmental requirements;
– test requirements including stress levels, test parameters and strategies, and accept/reject criteria;
– design performance margins, derating factors, quantitative Dependability requirements, and qualitative Dependability requirements (feared events), under specified environmental conditions;
– human factors where human error could be a consideration in mission success;
– the degree to which the design shall be tolerant to failures of hardware or software;
– the detection, isolation, diagnosis, and recovery of the system from failures and its restoration to an acceptable state;
– the prevention of failures crossing interfaces with unacceptable consequences;
– definition of the maintenance concept;
– maintenance tasks and the need for special skills;
– the need for preventive maintenance, special tools, and special test equipment.

3.3 Dependability Design Criteria

3.3.1 Consequence Category and Severity

a. Consequence category
Mission success (and safety) may be jeopardised 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
- pollution of the environment
- 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

3.3.2 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.

3.3.3 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.

b. The contractor shall ensure that reliability is built into the design through the use of 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 high availability/reliability into the design, the following dispositions shall be considered:

- 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/reconfiguration times in relation with propagation times of worst case events;
  * implementation of monitoring of the parameters which are essential for mission performance and safety, considering the failure modes of the system in relation with the actual capability of the detection devices, and considering the acceptable environmental conditions to be maintained on the product.
- physical design:
  * observance of design rules
  * giving preference to a system design that has performed successfully in the intended mission environment;
  * validating nonproven design by analysis and test;
  * using most suitable parts
  * using EEE parts derating and stress margins for mechanical parts;
  * making optimum use of design techniques for redundancy (while keeping system design complexity as low as possible);
  * maximising inspectability and testability of built-in equipment;
  * providing accessibility to equipment.

3.4 Involvement in Test Definition

3.4.1

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

3.4.2

The Dependability discipline shall support:

– definition of test characteristics and test objectives;

– selection of measurement parameters;

– statistical evaluation of test results.

3.5 Involvement in Operational Aspects

3.5.1

The contractor shall ensure that Dependability specialists

– contribute to definition of operations manual and procedures, and

– assess operations manual and procedures for consistency with Dependability analyses.

3.5.2

Procedures for operations shall be analysed with the aim of identifying and assessing the risks associated with operations, sequences and situations which may affect dependability performance.

3.5.3

Those analyses shall consider the technical and human environment, and shall verify that the procedures:

– provide for anomalous situations and supply the necessary safeguard measures,

– do not compromise equipment reliability

– are in accordance with established maintenance dispositions

– include dispositions proper to minimise failures due to human errors

3.6 Dependability Recommendations

3.6.1

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

3.6.2

All recommendations shall be fully justified and formal evidence of acceptance or rejection of the recommendation by the contractor‘s management shall be provided and documented in the Dependability Recommendation Status Log.

3.6.3

An accepted Dependability recommendation becomes a requirement to be implemented into the relevant applicable documentation.

4

Dependability Analyses

4.1 Dependability Analysis and the Project Life Cycle

4.1.1

Dependability analyses shall be performed on all space projects throughout the project life-cycle to support the tasks and goals specified in clause 3.

4.1.2

Dependability analyses shall be performed initially to establish the conceptual design, and the system requirements. Thereafter, the analyses shall be continued to support the conceptual, preliminary and detailed development and optimisation of the design, including the testing programme, leading to its qualification.

4.1.3

Dependability analyses shall be implemented in order to:

– ensure that reliability, availability and maintainability targets are met

– identify all potential failure modes and technical risks with respect to functional needs which can lead to nonachievement of dependability targets, provide risk assessment and risk reduction and control measures in line with the risk management process implemented on the project.

4.1.4

The results of Dependability analyses shall be incorporated into the Justification File which is defined by ECSS–M–30.

4.2 Dependability Analytical Methods

4.2.1

Dependability analyses shall be conducted on all appropriate levels of the space system. The methods identified below shall be used, tailored as necessary on each project, to address the hardware, software and human functions comprising the system. 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 compliance with the specified Dependability requirement. A consistent set of analyses taken from the list below

shall be defined early in the project, the justification being based on added value/ cost impact.

4.2.2 Reliability Analyses

These analyses can also be used for the purpose of determining Maintainability and Availability objectives and tasks.

a. Functional Analysis (FA) shall be performed to establish the relative criticality of each function and/or functional path in the concept under study in order to establish the reliability requirements, including those for failure tolerance and the software criticality classes, and to guide management controls (see ECSS–Q–30x). The FA shall be used to support the reliability modelling and the Reliability and Safety Analyses. From FA, function, products and procedures can be classified in functional categories, depending of the effect of the loss of function or failure of the product article, or procedure.

b. Failure Modes, Effects and Criticality Analysis (FMECA) shall be performed on the functional and physical design (functional FMECA and product design FMECA respectively), and the processes used to realize the final product (Process FMECA). In all cases the FMECA shall identify how each failure mode is detected.

   All potential failure modes shall be identified and classified according to the severity of their consequences. Measures shall be recommended in the analysis and introduced in the product design and in the control of processes to render all such consequences acceptable to the project.

   Provisions for failure detection and recovery actions shall be provided as part of the FMECA.

   The FMECA procedure and its application for the different purposes is described in ECSS–Q–30x.

c. 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 Software Requirements Document. The Hardware/Software Interaction Analysis may be included in the FMECA.

d. 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 acceptably degraded state (see ECSS–Q–30). The Contingency Analysis is a system level task.

e. A Fault Tree Analysis (FTA) shall be used to verify that the design complies with the failure tolerance requirements for combinations of failures.

   The Prime Contractor shall perform FTA to identify possible event combinations leading to the undesirable top 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
   - inadvertent activation of the subsystem function

f. 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 (ref. sub–clause 3.3.2). This analysis may be accomplished as part of FMECA or FTA.

g. Reliability Targets shall be apportioned to set reliability targets for lower level products.

h. Reliability Prediction techniques shall be used to optimise 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 (see ECSS–Q–30x). Reliability models shall be prepared to support predictions and FMECA.

i. Worst-case Analyses shall be performed on equipment to demonstrate that it will perform within specification despite particular variations in its constituent part parameters and the imposed environment. Worst–case Analyses shall be accomplished at equipment level.

j. Part Derating Analyses shall be performed to assure that the stress levels applied to all EEE parts are within the limits specified by the project (see ECSS-Q–30x). Part Derating Analyses shall be accomplished at equipment level.

k. Zonal Analysis (see sub–clause 4.2.3.d) shall be used as necessary to insure there is no failure propagation.

4.2.3 Maintainability Analyses

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

b. Maintainability Predictions shall be performed at system level and employed 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,
   - the time required to remove and replace the defective item,
   - the time required to return the system/subsystem to its original configuration and to perform the necessary checks,
   - the item failure rates.

   Maintainability predictions shall be used as a basis for estimating human resource requirements.

c. Scheduled Maintenance Analysis shall be performed at system level to determine the optimum scheduled maintenance plan that will minimise the amount of support resources needed to sustain the required safety level and mission capabilities and will also minimise down time.

   Each preventive maintenance action shall be based on the results of the application of a systematic decision logic to be approved by the customer (see ECSS–Q–30x).

d. Zonal Analysis shall be undertaken at system level to determine the optimal location for each product as regards accessibility, testability and repairability (see ECSS–Q–30x).

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 verified as meeting, applicable maintainability requirements.

4.2.4 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 optimise the system concept with respect to design, operations and maintenance.
   - to verify that the availability requirements are met,
   - to 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 programme), their causes, probabilities of occurrence and duration. Instead of outage probabilities, failure rates associated with outages may 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.

4.3 Classification of Design Characteristics in Production Documents

4.3.1

a. In support of the risk reduction and control process to 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 clause 3.3.5 and ECSS–Q–20 clause 2.8).

b. The classification and ranking of design characteristics shall make it possible:
   - to draw 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;
   - to define appropriate integration, test and inspection methods, techniques, resources to be applied, and selection of the production facilities according to the design characteristics;
   - to take all precautions making it possible to comply with the requirements imposed by the design characteristics, e.g. environmental control, etc.;
   - to achieve properly adapted and coherent classification and processing of non–conformances, changes and waivers.

c. The classification criteria shall either be imposed by the customer in the Statement of Work or be proposed by the contractor in his Product Assurance Plan.

4.4 Critical Items List

4.4.1

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 clause 3.3.5. Each Critical Item shall be supported with a Justification for Retention which shall be subject to approval by the customer.

4.4.2

Reliability Critical Items shall include at least single–point failures with a failure consequence severity classified as catastrophic, critical or major.

4.4.3

Maintainability Critical Items shall include 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.

4.4.4

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

(This page is intentionally left blank)

5

Dependability Testing, Demonstration and Data Collection

5.1 Dependability Testing and Demonstration

5.1.1

Reliability testing and demonstration shall be performed according to the customer's SOW in order to:

– validate failure modes and effects
– check failure tolerance, failure detection and recovery
– obtain statistical failure data to support predictions and risk assessment
– monitor reliability growth
– validate the capability of the hardware to operate with software or to be operated by a human being in accordance with the specifications
– demonstrate the reliability of reliability– and safety–Critical Items
– validate or justify data bases used for theoretical demonstrations

5.1.2

Maintainability demonstration shall be performed to verify the applicable maintainability requirements and to ensure that preventive and corrective maintenance activities can be successfully performed within the scope of the maintenance concept.

5.1.3

They shall verify the ability to:

– detect, diagnose and isolate each faulty Line Replaceable Unit/Orbit Replaceable Unit,
– remove and replace each Line Replaceable Unit/Orbit Replaceable Unit
– perform mission-essential repairs that are not intended to be accomplished by replacements
– check that the product is fully functional after maintenance actions have been completed

– demonstrate that no safety hazard is directly or indirectly introduced as a result of maintenance actions
– demonstrate that the maintenance operations can be performed within the applicable constraints (e.g. time, volume, accessibility, etc.). This shall include the operations necessary to prepare a system during the launch campaign, e.g. “remove before flight” items, replacement of batteries, etc.

5.2 Dependability Data Collection and Dependability Growth

5.2.1

Dependability data shall be collected during space system development from sources such as nonconformance and problem/failure reports, and maintenance actions. 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 reliability 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 concept trades and perform preliminary Dependability analyses to identify and compare the Dependability critical aspects of each design option; perform initial availability assessments where required;

c. 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 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 functional failure analysis, identify Dependability critical functional paths and establish the applicable failure-tolerance requirements;

d. Perform the Dependability analyses and common mode/common cause failure analyses; produce preliminary Dependability Critical Items list and the rationale(for retention;

e. Support the definition of the maintenance concept and the maintenance plan;

f. 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 Phases (Phase C/D)

In this phase the Dependability assurance tasks shall be to:

a. Update the functional failure analysis and perform detailed Dependability analyses; update all analyses in line with design maturity and test results; provide inputs to perform risk assessment.

b. Update and refine the Dependability Critical Items list and the rationale(for retention.

c. Define reliability and maintainability design criteria.

d. 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.

e. Perform contingency analyses in conjunction with design and operations engineering.

f. Support Design Reviews and monitor changes for impact on Dependability.

g. Define tool requirement and perform maintainability training and maintainability demonstration.

h. Support quality assurance during manufacture, integration and test; support MRB's and Failure Review Boards.

i. Review design and test specifications and procedures.

j. Review operational procedures to evaluate human reliability problems related to human/machine interface, check compatibility with the assumptions made in preparing the Dependability analysis, determine the impact of incompatibilities etc.

k. Supervise the collection of Dependability data.

A.4 Utilisation 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 operational data.

Annex B (informative)

Document Requirement List

The following list covers the contract documentation requirements established by ECSS–Q–30.

The list is intended to be used as Dependability programme input to the overall contract Document Requirement List. A tailoring for the specific programme needs shall be performed by the customer.

An assessment shall be made to ensure that there is no duplication of contractor–generated documentation within the Dependability and the Safety Programmes. The customer may specify, or agree, that two or more documentation items be combined into a single report.

- Dependability Programme Plan as part of PA-Programme Plan
- Functional Analysis
- Failure Modes, Effects and Criticality Analysis

FMECA may be supported by:

- Hardware/Software Interaction Analysis
- Common mode/Common cause Analysis
  - Fault Tree Analysis
  - Contingency Analysis
  - Scheduled Maintenance Analysis
  - Zonal Analysis
  - Dependability Apportionment
  - Dependability Prediction/Assessment
  - Outage Analysis
  - Worst-case Analysis
  - Part Derating Analysis
  - Dependability Critical Items List

Table B–1: PA Level 3 Standards – Annotated List ECSS–Q–30

PROPOSED LEVEL 3 STANDARDS		SUITABLE EXISTING STANDARD		REUSEABILITY CATEGORY	COMMENTS
Discipline	Title (proposed)	Identification (N°; Issue)	Title		MAJOR CHANGES
Dependability	Dependability analyses[1]: . Functional Analysis . FMECA . Contingency Analysis . Scheduled Maintenance Analysis . Zonal Analysis . Outage analysis . Availability analysis . Worst case analysis	PSS–01–303 Issue 1 dr. 9	FMECA (new)	4)	Complete revision of draft 7
Dependability	Derating and application rules	PSS–01–301	Same	1)	
Dependability	Failure rates			4)	Complete document and software browser available (mid 95)

NOTE 1 To be included in one or in seperate Level 3 Standards is TBD.

NOTE 2 FMECA = Failure Modes Effects and Criticality Analysis