INTERNATIONAL STANDARD

ISO 23460

Second edition
2023-06

Space projects — Programme management — Dependability assurance requirements

Projets spatiaux — Management de programme — Exigences d'assurance de sécurité de fonctionnement

Reference number
ISO 23460:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

This second edition cancels and replaces the first edition (ISO 23460:2011), which has been technically revised.

The main changes are as follows:

— updating of normative references and related terms and definitions;

— minor changes on tables.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The objective of dependability assurance is to ensure a successful mission by optimizing the system dependability within all competing technical, scheduling 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 ensuring conformity to reliability, availability and maintainability requirements.

Space projects — Programme management — Dependability assurance requirements

1 Scope

This document specifies the requirements for a dependability (reliability, availability and maintainability) assurance programme for space projects.

It defines the dependability requirements for space products as well as for system functions implemented in software, and the interaction between hardware and software.

This document is applicable to all programme phases.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 10795, *Space systems — Programme management and quality — Vocabulary*

ISO 15865, *Space systems — Qualification assessment*

ISO 16192, *Space systems — Experience gained in space projects (lessons learned) — Principles and guidelines*

ISO 17666, *Space systems — Risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 10795 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
criticality
classification of a function or of a software, hardware or operation according to the severity of the consequences of its potential failures

Note 1 to entry: This notion of criticality, applied to a function or a software, hardware or operation, considers only severity, differently from the criticality of a failure or failure mode (or a risk), which also considers the likelihood or probability of occurrence.

3.2
failure scenario
conditions and sequence of events leading from the initial root cause to an end failure

4 Policy and principles

4.1 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. The relationship between dependability activities and programme phases are provided in Annex A.

This process includes the following types of activities:

a) definition, organization and implementation of the dependability programme, as defined in Clause 5;

b) dependability risk identification, reduction and control, as defined in Clause 6;

c) dependability engineering, as defined in Clause 7;

d) dependability analyses, as defined in Clause 8;

e) dependability testing, demonstration and data collection, as defined in Clause 9.

4.2 Tailoring

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

5 Dependability programme management

5.1 Organization

The contractor shall implement the dependability (reliability, availability and maintainability) assurance as an integral part of the product assurance discipline.

5.2 Dependability programme planning

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

The content of document requirement list (DRL) used as dependability programme input to the overall project DR, is provided in Annex B.

For each product, the extent to which dependability assurance is applied shall be adapted to the severity (as defined in 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.

The contractor shall identify a failure as nonconformity and shall perform a series of control activities such as reporting, analyses, and prevention consistently with nonconforming item control system in quality management system.

5.3 Dependability critical items

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

Dependability critical items shall be subject to risk assessment and critical items control.

The control measures shall include:

a) 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;

b) dependability participation on nonconformity 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.

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

5.4 Design reviews

The contractor should establish and conduct a formal programme of scheduled and documented design reviews using ISO 21349 for guidance.

The contractor shall ensure that all dependability data for a design review is 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.

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

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.

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 shall include the dependability activities to verify conformity to the project dependability plan and requirements.

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

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

Nonconformity to dependability assurance requirements shall be identified and the rationale for retention of unresolved nonconformity shall be provided by a waiver request.

5.7 Subcontractor control

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.

5.9 Documentation

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.

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

6 Dependability risk reduction and control

6.1 General

As part of the risk management process implemented on the project in accordance with ISO 17666, the contractor shall analyse, reduce and control all dependability risks that lead to the nonconformity of dependability requirements, i.e. all risks of degradation or loss of technical performance required for the product.

Dependability risk analysis reduction and control 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 to 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.

6.2 Identification and classification of undesirable events

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

Preliminary identification and classification of undesirable events shall be determined from an 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 all be events whose occurrence can jeopardize, compromise, or degrade the success of the mission. At lower levels of the product tree (space segment, ground segment, sub-assemblies 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.

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

6.3 Assessment of failure scenarios

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

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 in the realization of the product mission) using functional failure modes effects analysis (FMEA), as defined in 8.2.2, which enables the determination of the effects (induced risks) for each function: loss, degradation and untimely occurrence. The functions shall be defined in advance (the functional analysis can be used for this purpose).

b) Analysis of the functional failure to 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 of identifying undesirable events induced by erroneous sequencing (e.g. loss of synchronism and untimely operations).

c) Analysis of the potential propagation of failures between different functions to be investigated.

d) Analysis of failure modes associated with the human factor 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.

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

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

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

6.4 Criticality classification of functions and products

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

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).

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

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 the context of risk reduction, the following measures shall be considered:

a) detailed risk assessment based on the 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 specifications on the design or operations as presented in 7.3.2 and 7.3.3.

6.6 Risk decisions

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

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

Decisions shall be taken, controlled and implemented within the risk management process applied to the project.

6.7 Verification of risk reduction

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

Verifications shall include:

a) monitoring and close out verification of actions and recommendations;

b) review of detailed risk assessment from dependability analyses;

c) reassessment of residual risks, verification of acceptability with reference to applicable criteria defined in the project risk policy;

d) identification of problem areas.

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

6.8 Documentation

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

a) visibility on results and progress of risk identification, assessment and reduction;

b) a definition of applicable requirements at the lower level of the product tree;

c) appropriate justifications of decisions on risk reduction and risk acceptance;

d) traceability, for each risk, to all pertinent analyses, results, data, decisions and close out status.

Documentation shall include:

a) identification and classification of undesirable events;

b) identification of failure scenarios, failure modes, causes and effects;

c) criticality classification of functions and products;

d) requirements at the lower level of the product tree;

e) definition of actions and recommendations;

f) dependability analyses, as needed for the purpose of risk assessment and reduction;

g) risk reduction status;

h) records of risk reduction and associated rationale.

7 Dependability engineering

7.1 Integration of dependability in the project

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.

Dependability issues shall be considered in all trades and 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.

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 a rationale has been provided for the acceptance of the remaining threats.

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 specifications

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 into 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 is 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) the definition of the maintenance concept;

i) maintenance tasks and requirements for special skills;

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

7.3 Dependability design criteria

7.3.1 Consequence category and severity

A severity classification shall be assigned in accordance with Table 1 to each identified failure mode analysed according to the failure effect (consequence).

Table 1 — Severity of consequences

Severity	Level	Dependability	Safety
Catastrophic	1	Failure propagation (only for lower than system level analysis)	Loss of life, life-threatening or permanently disabling injury or occupational illness Loss of system Loss of an interfacing manned flight system Loss of launch-site facilities Severe detrimental environmental effects
Critical	2	Complete loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness Major damage to interfacing flight system Major damage to ground facilities Major damage to public or private property Major detrimental environmental effects
Major	3	Major mission degradation	—
Minor or negligible	4	Minor mission degradation or any other effect	—

7.3.2 Failure tolerance

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.

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

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 are available.

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

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

a) 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 to 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.

b) 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 electrical, electronic, and electromechanical (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

In accordance with ISO 15865, 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. The qualification shall enable to verify the dependable requirements of parts, materials and processes.

The dependability discipline shall support:

a) definition of test characteristics and test objectives;

b) selection of measurement parameters;

c) statistical evaluation of test results.

8 Dependability analysis

8.1 Dependability analysis and the project life cycle

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

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.

Dependability analyses shall be implemented in order to:

a) ensure conformity to reliability, availability and maintainability requirements;

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

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

8.2 Dependability analytical methods

8.2.1 General

Dependability analyses shall be conducted on all appropriate levels of the space 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 conformity to the specified dependability requirement.

The methods identified in 8.2.2 to 8.2.4 shall be used and tailored to match the requirements of 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) Preliminary risk analysis shall be performed as soon as the design phases begin, in order to identify the possible causes of failure from feared events of the system. The following possible causes shall be taken into account: hardware, software and human.

b) Failure modes effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA).

   1) An FMEA and an 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 (FMECA process).

   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.

c) A 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.

d) A 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.

e) A fault-tree analysis (FTA) shall be used to verify that the design conforms to the failure tolerance requirements for combinations of failures.

   The prime contractor shall perform an FTA to identify possible event combinations leading to the undesirable end event “loss of mission”. The subsystem contractor shall support this activity by establishing an 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 (see 7.3.2). This analysis can be accomplished as part of the FMEA/FMECA or FTA.

g) Reliability requirements shall be apportioned to set reliability requirements for lower-level products.

h) 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 the FMEA/FMECA.

i) Worst-case analyses (WCA) 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. The WCA 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. Part-derating analyses shall be performed at equipment level.

k) A zonal analysis shall be used to ensure there is no failure propagation.

l) Failure detection isolation and recovery (FDIR) shall be performed at system level to ensure that autonomy and failure tolerance requirements are fulfilled.

8.2.3 Maintainability analyses

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.

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:

a) time required to diagnose (i.e. detect and isolate) item failures;

b) time required to remove and replace the defective item;

c) time required to return the system or subsystem to its nominal configuration and to perform the necessary checks;

d) item failure rates.

Scheduled maintenance analysis shall be performed at system level to determine the optimum scheduled maintenance plan that 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.

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

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

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

a) optimize the system concept with respect to design, operations and maintenance;

b) verify conformity to availability requirements;

c) provide inputs to estimate the overall cost of operating the system.

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.

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

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

The classification and ranking of design characteristics provide for:

a) 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;

b) defining appropriate integration, test and inspection methods, techniques and resources to be applied, and selection of the production facilities according to the design characteristics;

c) taking all precautions to conform to the requirements imposed by the design characteristics, e.g. environmental control;

d) achieving properly adapted and coherent classification and processing of nonconformities, changes and waivers.

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

8.4 Critical items list

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

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

Products that cannot be checked and tested after integration, the function or products where end-to-end test cannot be carried out, limited-life products, products that do not meet, or cannot be verified as meeting, applicable maintainability requirements, shall be listed as critical items.

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 for the project.

9 Dependability testing, demonstration and data collection

9.1 Dependability testing and demonstration

9.1.1 Reliability

Reliability testing and demonstration shall be performed according to the project requirement 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;

g) validate or justify databases used for theoretical demonstrations.

9.1.2 Maintainability

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

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.

9.1.3 Availability

Availability testing and demonstration shall be performed according to the project requirements and using the reliability and maintainability testing and demonstration.

9.2 Dependability data collection and dependability growth

Dependability data shall be collected during space system development from sources such as nonconformity and problem or failure reports, and maintenance reports. These data shall be based on an actual test or flight experience, and shall include the amount and mode of items used 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.

10 Lessons learned activity

A lesson-learned activity in accordance with ISO 16192 shall be organized to safeguard all dependability knowledge through recording, classifying and making available the proper information for the benefit of future space projects.