FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
23460**

ISO/TC **20**/SC **14**

Secretariat: **ANSI**

Voting begins on:
2023-03-03

Voting terminates on:
2023-04-28

Space projects — Programme management — Dependability assurance requirements

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

Reference number
ISO/FDIS 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;