

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 2023



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

# Contents

	Page
Foreword.....	v
Introduction.....	vi
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Policy and principles.....</b>	<b>2</b>
4.1 Basic approach.....	2
4.2 Tailoring.....	2
<b>5 Dependability programme management.....</b>	<b>2</b>
5.1 Organization.....	2
5.2 Dependability programme planning.....	2
5.3 Dependability critical items.....	3
5.4 Design reviews.....	3
5.5 Audits.....	3
5.6 Use of previously designed, fabricated, qualified or flown items.....	3
5.7 Subcontractor control.....	3
5.8 Progress reporting.....	4
5.9 Documentation.....	4
<b>6 Dependability risk reduction and control.....</b>	<b>4</b>
6.1 General.....	4
6.2 Identification and classification of undesirable events.....	4
6.3 Assessment of failure scenarios.....	5
6.4 Criticality classification of functions and products.....	5
6.5 Actions and recommendations for risk reduction.....	5
6.6 Risk decisions.....	6
6.7 Verification of risk reduction.....	6
6.8 Documentation.....	6
<b>7 Dependability engineering.....</b>	<b>7</b>
7.1 Integration of dependability in the project.....	7
7.2 Dependability requirements in technical specifications.....	7
7.3 Dependability design criteria.....	7
7.3.1 Consequence category and severity.....	7
7.3.2 Failure tolerance.....	8
7.3.3 Design approach.....	8
7.4 Involvement in test definition.....	9
<b>8 Dependability analysis.....</b>	<b>9</b>
8.1 Dependability analysis and the project life cycle.....	9
8.2 Dependability analytical methods.....	9
8.2.1 General.....	9
8.2.2 Reliability analyses.....	10
8.2.3 Maintainability analyses.....	11
8.2.4 Availability analyses.....	12
8.3 Classification of design characteristics in production documents.....	12
8.4 Critical items list.....	12
<b>9 Dependability testing, demonstration and data collection.....</b>	<b>13</b>
9.1 Dependability testing and demonstration.....	13
9.1.1 Reliability.....	13
9.1.2 Maintainability.....	13
9.1.3 Availability.....	13
9.2 Dependability data collection and dependability growth.....	13

<b>10</b>	<b>Lessons learned activity</b> .....	<b>14</b>
<b>Annex A</b> (informative)	<b>Relationship between dependability activities and programme phases</b> .....	<b>15</b>
<b>Annex B</b> (informative)	<b>Document requirement list (DRL)</b> .....	<b>17</b>
<b>Bibliography</b>	.....	<b>18</b>

## 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](http://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](http://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](http://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](http://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