
**Space projects — Programme
management — Dependability assurance
requirements**

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



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions	1
4 Policy and principles.....	2
4.1 Basic approach.....	2
4.2 Tailoring	2
5 Dependability programme management.....	2
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
6 Dependability risk reduction and control.....	4
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
7 Dependability engineering	7
7.1 Integration of dependability in the project.....	7
7.2 Dependability requirements in technical specification	7
7.3 Dependability design criteria	7
7.4 Involvement in test definition.....	9
8 Dependability analysis.....	9
8.1 Dependability analysis and the project life cycle	9
8.2 Dependability analytical methods	10
8.3 Classification of design characteristics in production documents	12
8.4 Critical items list.....	13
9 Dependability testing, demonstration and data collection	13
9.1 Dependability testing and demonstration.....	13
9.2 Dependability data collection and dependability growth.....	14
10 Lessons learned activity.....	14
Annex A (informative) Relationship between dependability activities and programme phases	15
Annex B (informative) Document requirement list (DRL)	17
Bibliography.....	18

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 23460 was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

This document is a preview generated by EVS

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 conformance to reliability, availability and maintainability requirements.

This document is a preview generated by EVS

This document is a preview generated by EVS

Space projects — Programme management — Dependability assurance requirements

1 Scope

This International Standard presents 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.

The provisions of this International Standard apply to all programme phases.

2 Normative references

The following referenced documents are indispensable for the application 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 17666, *Space systems — Risk management*

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

ISO 15865, *Space systems — Qualification assessment*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

failure scenario

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

3.2

risk

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

NOTE 1 In Clause 6, the term “risk” is as defined in ISO 17666.

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

3.3

undesirable event

event whose consequences are detrimental to the success of the mission

[ISO 10795:2011, definition 1.211]