International Standard

ISO 14620-1

Space systems — Safety requirements —

Part 1: System safety

Systèmes spatiaux — Exigences de sécurité —

Partie 1: Sécurité système

Third edition
2026-08

Reference number
ISO 14620-1:2026(en)

© ISO 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **vi**
Introduction ..... **vii**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 4
4 System safety programme **4**
4.1 Scope 4
4.2 Safety organization 5
4.2.1 General 5
4.2.2 Safety representative 5
4.2.3 Reporting lines 5
4.2.4 Safety integration 5
4.2.5 Coordination with others 5
4.3 Safety representative access and authority 5
4.3.1 Access 5
4.3.2 Delegated authority to reject — Stop work 5
4.3.3 Delegated authority to interrupt operations 6
4.3.4 Conformance 6
4.3.5 Approval of reports 6
4.3.6 Review 6
4.3.7 Representation on boards 6
4.4 Safety risk management 6
4.4.1 Safety risks 6
4.4.2 Hazard assessment 6
4.4.3 Preferred measures 7
4.5 Project phases and safety review cycle 7
4.5.1 Progress meetings 7
4.5.2 Project reviews 7
4.5.3 Safety programme review 9
4.5.4 Safety data package 9
4.6 Safety programme plan 10
4.6.1 Implementation 10
4.6.2 Safety activities 10
4.6.3 Definition 10
4.6.4 Description 10
4.6.5 Safety and project engineering activities 10
4.6.6 Supplier and sub-supplier premises 10
4.6.7 Conformance 11
4.7 Safety approval process 11
4.8 Safety training 11
4.8.1 Overall training 11
4.8.2 Participation 11
4.8.3 Detailed technical training 11
4.8.4 Product specific training 11
4.8.5 Records 11
4.8.6 Identification 12
4.9 Accident and incident reporting and investigation 12
4.10 Safety documentation 12
4.10.1 General 12
4.10.2 Customer access 12
4.10.3 Supplier review 12
4.10.4 Documentation 12

© ISO 2026 – All rights reserved

4.10.5 Safety data package 12
4.10.6 Safety deviations and waivers 13
4.10.7 Safety Verification tracking log 13
4.10.8 Lessons-learned file 13

5 Safety engineering 14
5.1 Safety engineering objectives 14
5.1.1 General 14
5.1.2 Elements 14
5.1.3 Lessons learned 14
5.2 Safety design principles 14
5.2.1 Human life consideration 14
5.2.2 Design selection 14
5.2.3 System safety order of precedence 14
5.2.4 Environmental compatibility 15
5.2.5 Safe without services 15
5.2.6 Fail safe design 16
5.2.7 Hazard detection — Signalling and safing 16
5.2.8 Access 16
5.2.9 Safety risk reduction and control 16
5.3 Failure tolerance requirements 19
5.3.1 Basic requirements 19
5.3.2 Software 19
5.3.3 Payload interface 19
5.3.4 Redundancy separation 19
5.3.5 Failure propagation 20
5.3.6 Design for minimum risk 20
5.3.7 Probabilistic safety targets 20
5.4 Identification and control of safety-critical functions 21
5.4.1 Identification 21
5.4.2 Flow-down of safety-critical functions 21
5.4.3 Inadvertent operation 21
5.4.4 Provisions 21
5.4.5 Shutdown and failure tolerance requirements 22
5.4.6 Electronic, electrical, electromechanical 22

6 Safety analysis requirements and techniques 22
6.1 General 22
6.2 Assessment and allocation of requirements 22
6.2.1 Safety requirements 22
6.2.2 Additional safety requirements 23
6.2.3 Define safety requirements — Functions 23
6.2.4 Define safety requirements — Subsystems 23
6.2.5 Justification 23
6.2.6 Functional and subsystem specification 23
6.3 Safety analysis 23
6.3.1 General 23
6.3.2 Mission analysis 23
6.3.3 Feasibility 23
6.3.4 Preliminary definition 23
6.3.5 Detailed definition, production and qualification 23
6.3.6 Utilization 24
6.3.7 Disposal 24
6.4 Specific safety analysis 24
6.4.1 General 24
6.4.2 Hazard analysis 24
6.4.3 Safety risk assessment 25
6.4.4 Safety analysis for hardware-software systems 25
6.5 Supporting assessment and analysis 26
6.5.1 General 26

© ISO 2026 – All rights reserved

6.5.2 Warning time analysis ... 26
6.5.3 Caution and warning analysis ... 26
6.5.4 Common cause and common mode failure analysis ... 27
6.5.5 Fault tree analysis ... 27
6.5.6 Human dependability analysis ... 27
6.5.7 Failure modes, effects and criticality analysis ... 27
6.5.8 Hardware-software interaction analysis (HSIA) ... 27
6.5.9 Sneak analysis ... 28
6.5.10 Zonal analysis ... 28
6.5.11 Energy trace analysis ... 29

7 Safety verification ... 29
7.1 General ... 29
7.2 Tracking of hazards ... 29
7.2.1 Hazard reporting system ... 29
7.2.2 Status ... 29
7.2.3 Safety progress meeting ... 29
7.2.4 Review and disposition ... 29
7.2.5 Documentation ... 29
7.2.6 Mandatory inspection points (MIPs) ... 30
7.3 Safety verification methods ... 30
7.3.1 Verification engineering and planning ... 30
7.3.2 Methods and reports ... 30
7.3.3 Verification requirements ... 30
7.3.4 Analysis ... 30
7.3.5 Inspections ... 30
7.3.6 Tests ... 30
7.3.7 Verification and approval ... 31
7.4 Qualification of safety-critical functions ... 31
7.4.1 Verification ... 31
7.4.2 Qualification ... 31
7.4.3 Failure tests ... 31
7.4.4 Verification of design or operational characteristics ... 31
7.4.5 Safety verification testing ... 31
7.5 Hazard close-out ... 31
7.5.1 Safety assurance verification ... 31
7.5.2 Safety approval authority ... 32
7.6 Residual risk reduction ... 32

8 Operational safety ... 32
8.1 General ... 32
8.2 Basic requirements ... 32
8.3 Flight operations and mission control ... 32
8.3.1 Launcher operations ... 32
8.3.2 Contamination ... 33
8.3.3 Flight rules ... 33
8.3.4 Hazardous commanding control ... 33
8.3.5 Mission operation change control ... 33
8.3.6 Safety surveillance and anomaly control ... 33
8.4 Ground operations ... 33
8.4.1 Applicability ... 33
8.4.2 Initiation ... 34
8.4.3 Review and inspection ... 34
8.4.4 Hazardous operations ... 34
8.4.5 Launch and landing site requirements ... 34
8.4.6 GSE requirements ... 34

Bibliography ... 35

© ISO 2026 – All rights reserved

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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 third edition cancels and replaces the second edition (ISO 14620-1:2018), which has been technically revised.

The main change is as follows:

— definitions have been revised.

A list of all parts in the ISO 14620 series can be found on the ISO website.

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.

© ISO 2026 – All rights reserved

Introduction

The ISO 14620 series is intended to be applied together for the management, engineering and product assurance in space projects and applications.

The safety policy is implemented through a structured system safety programme supported by risk assessment. Hazardous system and environmental characteristics, as well as functions with potentially dangerous failure effects, are systematically identified and evaluated. Potential hazards are addressed through a reduction process in which they are first eliminated from design and operations, then minimized, and, if necessary, controlled and verified. Any residual risks are progressively assessed to ensure conformance to safety requirements, support design decisions, and in order to prioritise risk contributors, allocate resources, monitor progress in risk reduction, and inform safety-related decision-making. The effectiveness of hazard and risk control measures is formally verified to enable safety validation and risk acceptance. Finally, overall safety conformance is evaluated, and approval is obtained from the relevant authorities for both crewed and uncrewed projects.

The imposition of these requirements on the project suppliers' activities requires that the customer's project product assurance and safety organization also respond to these requirements in a manner which is commensurate with the project's safety criticality.

Launch site operations are described by ISO 14620-2 and flight safety systems in ISO 14620-3.

© ISO 2026 – All rights reserved

Space systems — Safety requirements —

Part 1:
System safety

1 Scope

This document specifies the safety programme and the technical safety requirements that are implemented in order to conform to the safety policy defined in ISO 14300-2. It is intended to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, and the environment from hazards associated with space systems.

This document is applicable to all space projects where during any project phase there exists the potential for hazards to personnel or the general public, space flight systems, ground support equipment, facilities, public or private property, or the environment.

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 14300-1, *Space systems — Programme management — Part 1: Structuring of a project*

ISO 14300-2, *Space systems — Programme management — Part 2: Product assurance*

ISO 14620-2, *Space systems — Safety requirements — Part 2: Launch site operations*

ISO 14620-3, *Space systems — Safety requirements — Part 3: Flight safety systems*

ISO 17666, *Space systems — Programme management — Risk management*

ISO 21347, *Space systems — Fracture and damage control*

ISO 24113, *Space systems — Space debris mitigation requirements*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions 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/

3.1.1
accident
mishap
undesired event arising from operation of any project-specific items which results in:

© ISO 2026 – All rights reserved

a) human death or injury;

b) loss of, or damage to, hardware, software or facilities which can then affect the accomplishment of the mission;

c) loss of, or damage to, public or private property; and

d) detrimental effects on the environment

[SOURCE: ISO 10795:2019, 3.8]

3.1.2
anomaly
gap between a current situation and an expected one

Note 1 to entry: An anomaly justifies an investigation that can lead to the discovery of a nonconformance, a defect.

Note 2 to entry: A deviation may be declared, foreseen or requested.

Note 3 to entry: An anomaly is often detected in comparison with what seems to be standard or with the expected use.

[SOURCE: ISO 10795:2019, 3.13]

3.1.3
cause
circumstance, condition, event or action that produces an effect or gives rise to any action, phenomenon or condition

Note 1 to entry: Cause and effect are correlative terms.

Note 2 to entry: Specific to this document, cause, when used in the context of hazard analysis, is the action or condition by which a *hazardous event* (3.1.11) is initiated (an initiating event). The cause can arise as the result of *failure* (3.1.9), human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).

[SOURCE: ISO 10795:2019, 3.35]

3.1.4
common cause failure
failure (3.1.9) of multiple items occurring from a single *cause* (3.1.3) which is common to all of them

[SOURCE: Adapted from NUREG/CR-2300 PRA:1982, ISO 10795:2019, 3.4]

3.1.5
common mode failure
failure (3.1.9) of multiple identical items that fail in the same mode

Note 1 to entry: Common mode failures are a particular case of *common cause failures* (3.1.5).

[SOURCE: NUREG/CR-2300 PRA:1982, ISO 10795:2019, 3.46]

3.1.6
emergency
situation where *hazardous events* (3.1.11) have occurred with potentially catastrophic or critical consequences requiring an immediate action

[SOURCE: Adapted from EN 16601-00-01:2015, 2.3.73]

3.1.7
fail safe
design property of a system, or subsystem (or part of it), which prevents its *failures* (3.1.9) from resulting in critical or catastrophic consequences (i.e. remain safe after one failure)

Note 1 to entry: Maintaining safety following two independent failures is referred to “fail safe – fail safe”.

© ISO 2026 – All rights reserved

[SOURCE: ISO 26871:2020, 3.1.32]

3.1.8
failure
event resulting in an item being no longer able to perform its required function

Note 1 to entry: "Failure" is an event, as distinguished from "fault" which is a state.

[SOURCE: EN 16601-00-01:2015, 2.3.81]

3.1.9
fault
state of an item characterized by inability to perform as required

Note 1 to entry: A fault can be the result of a failure of the item itself or can exist without prior failure.

Note 2 to entry: A fault can generate a failure.

[SOURCE: EN 16601-00-01:2015, 2.3.84]

3.1.10
hazard
existing or potential condition of an item that can result in an *accident* (3.1.1)

Note 1 to entry: This condition can be associated with the design, manufacturing, operation or environment.

Note 2 to entry: Hazards are not events but potential threats to safety.

[SOURCE: EN 16601-00-01:2015, 2.3.102]

3.1.11
hazardous event
accident (3.1.1) resulting from a *hazard* (3.1.10)

[SOURCE: EN 16601-00-01:2015, 2.3.103]

3.1.12
inhibit
<noun> design feature that prevents a function from undesirable execution

Note 1 to entry: An inhibit can be software or hardware.

[SOURCE: EN 16601-00-01:2015, 2.3.109]

3.1.13
residual risk
risk remaining after implementation of risk reduction measures

[SOURCE: ISO 17666:2025, 3.10]

3.1.14
safe state
state that does not lead to critical or catastrophic consequences

3.1.15
safety authority
body defining and making applicable (project specific) safety requirements and providing confirmation of conformance to project specific safety requirements

© ISO 2026 – All rights reserved

3.1.16
safety-critical function
function that, if lost or degraded, or as a result of incorrect or inadvertent operation, would result in catastrophic or critical consequences

[SOURCE: ISO 10795:2019, 3.212]

3.1.17
safing
action of containment or control of emergency and warning situations or placing a system (or part thereof) in a predetermined safe condition

[SOURCE: EN 16601-00-01:2015, 2.3.180]

3.1.18
system safety
application of engineering and management principles, criteria and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle

3.2 Abbreviated terms

CCB	configuration control board
CDR	critical design review
EEE	electronic, electrical, electromechanical
FAR	flight acceptance review
FMECA	failure modes, effects and criticality analysis
FSR	flight safety review
FTA	fault free analysis
GSE	ground support equipment
HSIA	hardware-software interaction analysis
MIP	mandatory inspection point
NRB	nonconformance review board
PDR	preliminary design review
TRB	test review board
SVTL	safety verification tracking log

4 System safety programme

4.1 Scope

a) The scope and content of the safety programme is to establish a safety management system to implement provisions of this document commensurate with the programme requirements.

© ISO 2026 – All rights reserved