

---

---

**Space systems — Safety  
requirements —**

**Part 1:  
System safety**

*Systèmes spatiaux — Exigences de sécurité —*

*Partie 1: Sécurité système*

<https://standards.iteh.ai>  
**Document Preview**

[ISO 14620-1:2018](https://standards.iteh.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018)

<https://standards.iteh.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018>



iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO 14620-1:2018](https://standards.iteh.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018)

<https://standards.iteh.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2018

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  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>vii</b>
<b>Introduction</b> .....	<b>viii</b>
<b>1 Scope</b> .....	<b>1</b>
1.1 General.....	1
1.2 Field of application.....	2
1.3 Tailoring.....	2
<b>2 Normative references</b> .....	<b>2</b>
<b>3 Terms, definitions and abbreviated terms</b> .....	<b>2</b>
3.1 Terms and definitions.....	2
3.2 Abbreviated terms.....	5
<b>4 System safety programme</b> .....	<b>6</b>
4.1 Scope.....	6
4.2 Safety organization.....	6
4.2.1 General.....	6
4.2.2 Safety representative.....	6
4.2.3 Reporting lines.....	6
4.2.4 Safety integration.....	6
4.2.5 Coordination with others.....	6
4.3 Safety representative access and authority.....	6
4.3.1 Access.....	6
4.3.2 Delegated authority to reject — stop work.....	7
4.3.3 Delegated authority to interrupt operations.....	7
4.3.4 Conformance.....	7
4.3.5 Approval of reports.....	7
4.3.6 Review.....	7
4.3.7 Representation on boards.....	7
4.4 Safety risk management.....	7
4.4.1 Safety risks.....	7
4.4.2 Hazard assessment.....	7
4.4.3 Preferred measures.....	8
4.5 Project phases and safety review cycle.....	8
4.5.1 Progress meetings.....	8
4.5.2 Project reviews.....	8
4.5.3 Safety programme review.....	10
4.5.4 Safety data package.....	10
4.6 Safety programme plan.....	11
4.6.1 Implementation.....	11
4.6.2 Safety activities.....	11
4.6.3 Definition.....	11
4.6.4 Description.....	11
4.6.5 Safety and project engineering activities.....	11
4.6.6 Supplier and sub-supplier premises.....	11
4.6.7 Conformance.....	11
4.7 Safety certification.....	12
4.8 Safety training.....	12
4.8.1 Overall training.....	12
4.8.2 Participation.....	12
4.8.3 Detailed technical training.....	12
4.8.4 Product specific training.....	12
4.8.5 Records.....	12
4.8.6 Identification.....	12
4.9 Accident/incident reporting and investigation.....	13
4.10 Safety documentation.....	13

4.10.1	General.....	13
4.10.2	Customer access.....	13
4.10.3	Supplier review.....	13
4.10.4	Documentation.....	13
4.10.5	Safety data package.....	13
4.10.6	Safety deviations and waivers.....	14
4.10.7	Verification tracking log.....	14
4.10.8	Lessons-learned file.....	14
<b>5</b>	<b>Safety engineering.....</b>	<b>15</b>
5.1	Safety engineering objectives.....	15
5.1.1	General.....	15
5.1.2	Elements.....	15
5.1.3	Lessons learned.....	15
5.2	Safety design principles.....	15
5.2.1	Human life consideration.....	15
5.2.2	Design selection.....	15
5.2.3	System safety order of precedence.....	15
5.2.4	Environmental compatibility.....	16
5.2.5	Safe without services.....	16
5.2.6	Fail safe design.....	16
5.2.7	Hazard detection — Signalling and safing.....	17
5.2.8	Access.....	17
5.2.9	Safety risk reduction and control.....	17
5.3	Failure tolerance requirements.....	19
5.3.1	Basic requirements.....	19
5.3.2	Software.....	20
5.3.3	Payload interface.....	20
5.3.4	Redundancy separation.....	20
5.3.5	Failure propagation.....	20
5.3.6	Design for minimum risk.....	21
5.3.7	Probabilistic safety targets.....	21
5.4	Identification and control of safety critical functions.....	22
5.4.1	Identification.....	22
5.4.2	Inadvertent operation.....	22
5.4.3	Provisions.....	22
5.4.4	Shutdown and failure tolerance requirements.....	22
5.4.5	Electronic, electrical, electromechanical.....	22
<b>6</b>	<b>Safety analysis requirements and techniques.....</b>	<b>23</b>
6.1	General.....	23
6.2	Assessment and allocation of requirements.....	23
6.2.1	Safety requirements.....	23
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.....	24
6.3	Safety analysis.....	24
6.3.1	General.....	24
6.3.2	Mission analysis.....	24
6.3.3	Feasibility.....	24
6.3.4	Preliminary definition.....	24
6.3.5	Detailed definition, production and qualification.....	24
6.3.6	Utilization.....	24
6.3.7	Disposal.....	24
6.4	Specific safety analysis.....	25
6.4.1	General.....	25
6.4.2	Hazard analysis.....	25

6.4.3	Safety risk assessment.....	25
6.4.4	Safety analysis for hardware-software systems.....	26
6.5	Supporting assessment and analysis.....	27
6.5.1	General.....	27
6.5.2	Warning time analysis.....	27
6.5.3	Caution and warning analysis.....	27
6.5.4	Common cause and common mode failure analysis.....	27
6.5.5	Fault tree analysis.....	28
6.5.6	Human dependability analysis.....	28
6.5.7	Failure modes, effects and criticality analysis.....	28
6.5.8	Sneak analysis.....	28
6.5.9	Zonal analysis.....	29
6.5.10	Energy trace analysis.....	29
<b>7</b>	<b>Safety verification.....</b>	<b>30</b>
7.1	General.....	30
7.2	Tracking of hazards.....	30
7.2.1	Hazard reporting system.....	30
7.2.2	Status.....	30
7.2.3	Safety progress meeting.....	30
7.2.4	Review and disposition.....	30
7.2.5	Documentation.....	30
7.2.6	Mandatory inspection points.....	30
7.3	Safety verification methods.....	31
7.3.1	Verification engineering and planning.....	31
7.3.2	Methods and reports.....	31
7.3.3	Verification requirements.....	31
7.3.4	Analysis.....	31
7.3.5	Inspections.....	31
7.3.6	Tests.....	31
7.3.7	Verification and approval.....	31
7.4	Qualification of safety critical functions.....	32
7.4.1	Verification.....	32
7.4.2	Qualification.....	32
7.4.3	Failure tests.....	32
7.4.4	Verification of design or operational characteristics.....	32
7.4.5	Safety verification testing.....	32
7.5	Hazard close-out.....	32
7.5.1	Safety assurance verification.....	32
7.5.2	Safety approval authority.....	32
7.6	Residual risk reduction.....	33
<b>8</b>	<b>Operational safety.....</b>	<b>33</b>
8.1	General.....	33
8.2	Basic requirements.....	33
8.3	Flight operations and mission control.....	33
8.3.1	Launcher operations.....	33
8.3.2	Contamination.....	33
8.3.3	Flight rules.....	33
8.3.4	Hazardous commanding control.....	34
8.3.5	Mission operation change control.....	34
8.3.6	Safety surveillance and anomaly control.....	34
8.4	Ground operations.....	34
8.4.1	Applicability.....	34
8.4.2	Initiation.....	35
8.4.3	Review and inspection.....	35
8.4.4	Hazardous operations.....	35
8.4.5	Launch and landing site requirements.....	35
8.4.6	GSE requirements.....	35

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[ISO 14620-1:2018](https://standards.itih.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018)

<https://standards.itih.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018>

## 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 on 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 the following URL: [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 14620-1:2002), which has been technically revised.

The main changes compared to the previous edition are as follows:

- definitions have been revised; and
- the document has been aligned with the ISO/IEC Directives Part 2, 2016 edition.

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](http://www.iso.org/members.html).

## Introduction

This document is one of the series of space standards intended to be applied together for the management, engineering and product assurance in space projects and applications.

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[ISO 14620-1:2018](https://standards.itih.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018)

<https://standards.itih.ai/catalog/standards/iso/a6ce0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018>



# Space systems — Safety requirements —

## Part 1: System safety

### 1 Scope

#### 1.1 General

This document defines the safety programme and the technical safety requirements that are implemented in order to comply with the safety policy as 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. Launch site operations are described by ISO 14620-2 and flight safety systems in ISO 14620-3.

The safety policy is applied by implementing a system safety programme, supported by risk assessment, which can be summarized as follows.

- a) Hazardous characteristics (system and environmental hazards) and functions with potentially hazardous failure effects are identified and progressively evaluated by iteratively performing systematic safety analyses.
- b) The potential hazardous consequences associated with the system characteristics and functional failures are subjected to a hazard reduction sequence whereby:
  - 1) hazards are eliminated from the system design and operations;
  - 2) hazards are minimized; and [ISO 14620-1:2018](https://standards.iteh.ai/catalog/standards/iso/a6cef0cfe-9bc3-4afc-8d6b-60276c178454/iso-14620-1-2018)
  - 3) hazard controls are applied and verified.
- c) The risks that remain after the application of a hazard elimination and reduction process are progressively assessed and subjected to risk assessment, in order to:
  - 1) show compliance with safety targets;
  - 2) support design trades;
  - 3) identify and rank risk contributors;
  - 4) support apportionment of project resources for risk reduction;
  - 5) assess risk reduction progress; and
  - 6) support the safety and project decision-making process (e.g. waiver approval, residual risk acceptance).
- d) The adequacy of the hazard and risk control measures applied are formally verified in order to support safety validation and risk acceptance.
- e) Safety compliance is assessed by the project and safety approval obtained from the relevant authorities.

## 1.2 Field of application

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.

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.

## 1.3 Tailoring

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

NOTE Tailoring is the process by which individual requirements of specifications, standards and related documents are evaluated, and made applicable to a specific programme or project by selection, and in some exceptional cases, modification of existing or addition of new requirements.

## 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 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 terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

#### 3.1.1

##### **accident**

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

- a) human death or injury;
- b) loss of, or damage to, hardware, software or facilities which could then affect the accomplishment of the mission;
- c) loss of, or damage to, public or private property; and
- d) detrimental effects on the environment

Note 1 to entry: Accident and mishap are synonymous.

[SOURCE: EN 16601-00-01:2015, 2.3.3]

### 3.1.2

#### **cause**

action or condition by which a hazardous event is initiated (an initiating event)

Note 1 to entry: The cause can arise as the result of failure, human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).

Note 2 to entry: This definition is specific to this document, when used in the context of hazard analysis.

### 3.1.3

#### **caution condition**

condition which has the potential to degrade into a warning condition, and which might require specific action, including the implementation of special procedures or restrictions on the operation of the system

[SOURCE: EN 13701:2001]

### 3.1.4

#### **common cause failure**

failure of multiple items occurring from a single cause which is common to all of them

[SOURCE: Adapted from NUREG/CR-2300 PRA:1982]

### 3.1.5

#### **common mode failure**

failure 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.

[SOURCE: NUREG/CR-2300 PRA:1982]

### 3.1.6

#### **critical fault**

fault which is assessed as likely to result in injury to persons, significant material damage, or other unacceptable consequences

[SOURCE: IEC 60050:1992]

### 3.1.7

#### **emergency**

condition when potentially catastrophic or critical hazardous events have occurred, where immediate and pre-planned safing action is possible and is mandatory in order to protect personnel

[SOURCE: Adapted from EN 13701:2001]

### 3.1.8

#### **fail safe**

design property of an item which prevents its failures from resulting in critical faults

[SOURCE: IEC 60050:1992]

### 3.1.9

#### **failure**

termination of the ability of an item to perform a required function

[SOURCE: IEC 60050:1992]

## ISO 14620-1:2018(E)

### 3.1.10

#### **fault**, noun

<state> the state of an item characterized by inability to perform as required, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of a failure of the item itself, but can exist without prior failure.

[SOURCE: Adapted from IEC 60050:1992]

### 3.1.11

#### **fault**, noun

<event> an unplanned occurrence or defect in an item which may result in one or more failures of the item itself or of other associated equipment

Note 1 to entry: An item may contain a sub-element fault, which is a defect that can manifest itself only under certain circumstances. When those circumstances occur, the defect in the sub-element will cause the item to fail, resulting in an error. This error can propagate to other items causing them, in turn, to fail. After the failure occurs, the item as a whole is said to have a fault or to be in a faulty state ([3.1.10](#)).

[SOURCE: IEC 60050:1992, modified — Note 1 to entry from EN 13701:2001]

### 3.1.12

#### **hazard**

existing or potential condition of an item that can result in an accident

Note 1 to entry: This condition can be associated with the design, fabrication, operation or environment of the item, and has the potential for mishaps.

Note 2 to entry: "Items" can include human beings.

[SOURCE: ISO 14620-2:2011, 3.9, modified — "mishap" changed to "accident", Note 2 to entry added]

### 3.1.13

#### **hazardous event**

occurrence leading to undesired consequences and arising from the triggering by one (or more) initiator events of one (or more) hazards

[SOURCE: Adapted from EN 13701:2001]

### 3.1.14

#### **inhibit**

design feature that provides a physical interruption between an energy source and a function actuator

EXAMPLE A relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and thruster.

Note 1 to entry: Two inhibits are independent if no single failure can eliminate more than one inhibit.

[SOURCE: Adapted from EN 13701:2001]

### 3.1.15

#### **residual risk**

risk remaining in a system after completion of the hazard reduction and control process

[SOURCE: EN 13701:2001]

### 3.1.16

#### **safe state**

state that does not lead to critical or catastrophic consequences