
Space systems — Safety requirements —

**Part 1:
System safety**

Systèmes spatiaux — Exigences de sécurité —

Partie 1: Sécurité système

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 14620-1:2002

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>



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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 14620-1:2002

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>

© ISO 2002

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.ch
Web www.iso.ch

Printed in Switzerland

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 3.

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 part of ISO 14620 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 14620-1 was prepared by the European Committee for Standardization (CEN) in collaboration with Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Throughout the text of this document, read “...this European Standard...” to mean “...this International Standard...”.

ISO 14620 consists of the following parts, under the general title *Space systems — Safety requirements*:

- *Part 1: System safety* <https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>
- *Part 2: Launch site operations*

The following part is under preparation:

- *Part 3: Flight safety systems*

Contents

	Page
Foreword.....	vii
Introduction	viii
1 Scope	1
1.1 General.....	1
1.2 Field of application	2
1.3 Tailoring.....	2
2 Normative references	2
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Abbreviated terms	7
4 System safety programme	7
4.1 Scope	7
4.2 Safety organization.....	8
4.2.1 General.....	8
4.2.2 Safety representative.....	8
4.2.3 Reporting lines.....	8
4.2.4 Safety integration.....	8
4.2.5 Coordination with others	8
4.3 Safety representative access and authority.....	8
4.3.1 Access.....	8
4.3.2 Delegated authority to reject - stop work.....	8
4.3.3 Delegated authority to interrupt operations.....	8
4.3.4 Conformance.....	8
4.3.5 Approval of reports.....	9
4.3.6 Review.....	9
4.3.7 Representation on boards	9
4.4 Safety risk management.....	9
4.4.1 Risks.....	9
4.4.2 Hazard assessment	9
4.4.3 Preferred measures	9
4.5 Project phases and safety review cycle	9
4.5.1 Progress meetings.....	9
4.5.2 Project reviews.....	10
4.5.3 Safety programme review	12
4.5.4 Safety data package	12
4.6 Safety programme plan	12
4.6.1 Implementation.....	12
4.6.2 Safety activities	12
4.6.3 Definition.....	12
4.6.4 Description	13
4.6.5 Safety and project engineering activities.....	13
4.6.6 Supplier and sub-supplier premises.....	13
4.6.7 Conformance	13
4.7 Safety certification.....	13
4.8 Safety training	13
4.8.1 Overall training.....	13
4.8.2 Participation	14
4.8.3 Detailed technical training	14
4.8.4 Product specific training.....	14

4.8.5	Records.....	14
4.8.6	Identification.....	14
4.9	Accident/incident reporting and investigation	14
4.10	Safety documentation	14
4.10.1	General.....	14
4.10.2	Customer access	14
4.10.3	Supplier review	14
4.10.4	Documentation.....	15
4.10.5	Safety data package	15
4.10.6	Safety deviations and waivers.....	15
4.10.7	Verification tracking log.....	16
4.10.8	Lessons-learned file	16
5	Safety engineering.....	16
5.1	Safety engineering policy	16
5.1.1	General.....	16
5.1.2	Elements	16
5.1.3	Lessons learned.....	16
5.2	Safety design principles	17
5.2.1	Human life consideration	17
5.2.2	Design selection	17
5.2.3	System safety order of precedence	17
5.2.4	Environmental compatibility.....	18
5.2.5	Safe without services	18
5.2.6	Fail safe design	18
5.2.7	Hazard detection - Signalling and safing	18
5.2.8	Access	19
5.3	Safety risk reduction and control.....	19
5.3.1	Severity	19
5.3.2	Failure tolerance requirements	21
5.3.3	Design for minimum risk.....	22
5.3.4	Probabilistic safety targets	22
5.4	Identification and control of safety critical functions	23
5.4.1	Identification.....	23
5.4.2	Inadvertent operation	23
5.4.3	Provisions.....	23
5.4.4	Safe shutdown and failure tolerance requirements	23
5.4.5	Electronic, electrical, electromechanical	23
6	Safety analysis requirements and techniques	24
6.1	General.....	24
6.2	Assessment and allocation of requirements	24
6.2.1	Safety requirements	24
6.2.2	Additional safety requirements	24
6.2.3	Define safety requirements - functions	24
6.2.4	Define safety requirements - subsystems	24
6.2.5	Justification	24
6.2.6	Functional and subsystem specification	25
6.3	Safety analysis	25
6.3.1	General.....	25
6.3.2	Mission analysis	25
6.3.3	Feasibility	25
6.3.4	Preliminary definition	25
6.3.5	Detailed definition, production and qualification	25
6.3.6	Utilization	25
6.3.7	Disposal	25
6.4	Specific safety analysis	25
6.4.1	General.....	25
6.4.2	Hazard analysis.....	26
6.4.3	Safety risk assessment	26
6.4.4	Safety analysis for hardware-software systems	27
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	28
6.5.4	Common cause and common mode failure analysis	28
6.5.5	Fault tree analysis.....	29
6.5.6	Human dependability analysis	29
6.5.7	Failure modes, effects and criticality analysis	29
6.5.8	Sneak analysis	29
6.5.9	Zonal analysis	30
6.5.10	Energy trace analysis	30
7	Safety verification	30
7.1	General.....	30
7.2	Tracking of hazards	31
7.2.1	Hazard reporting system.....	31
7.2.2	Status	31
7.2.3	Safety progress meeting	31
7.2.4	Review and disposition	31
7.2.5	Documentation.....	31
7.2.6	Mandatory inspection points	31
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.....	32
7.3.4	Analysis	32
7.3.5	Inspections	32
7.3.6	Tests.....	32
7.3.7	Verification and approval.....	32
7.4	Qualification of safety critical functions	32
7.4.1	Validation	32
7.4.2	Qualification	32
7.4.3	Failure tests	33
7.4.4	Verification of design or operational characteristics.....	33
7.4.5	Safety verification testing	33
7.5	Hazard close-out.....	33
7.5.1	Safety assurance verification	33
7.5.2	Safety approval authority.....	33
7.6	Residual risk reduction	33
8	Operational safety.....	34
8.1	Basic requirements.....	34
8.2	Flight operations and mission control	34
8.2.1	Launcher operations	34
8.2.2	Contamination	34
8.2.3	Flight rules.....	34
8.2.4	Hazardous commanding control	34
8.2.5	Mission operation change control	35
8.2.6	Safety surveillance and anomaly control	35
8.3	Ground operations.....	35
8.3.1	Applicability.....	35
8.3.2	Initiation	35
8.3.3	Review and inspection	35
8.3.4	Hazardous operations	35
8.3.5	Launch and landing site requirements.....	36
8.3.6	GSE requirements.....	36
	Bibliography	37

iTech STANDARD PREVIEW
(standards.iteh.ai)

ISO 14620-1:2002
<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4cf/79a5066a1cd7/iso-14620-1-2002>

Foreword

This document EN ISO 14620-1:2002 has been prepared by Technical Committee CEN/SS T02 "Aerospace", the secretariat of which is held by CMC, in collaboration with Technical Committee ISO/TC 20 "Aircraft and space vehicles".

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2003, and conflicting national standards shall be withdrawn at the latest by June 2003.

The European Standard EN ISO 14620-1 was prepared by the European Cooperation for Space Standardization (ECSS) Product Assurance Working Group for CEN in close collaboration with ISO Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*, WG 5, *Program management*.

EN ISO 14620 consists of the following parts, under the general title *Space systems — Safety requirements*:

- *Part 1: System safety*
- *Part 2: Launch site operations*

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

[ISO 14620-1:2002](https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002)

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>

Introduction

This European Standard 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 STANDARD PREVIEW (standards.iteh.ai)

ISO 14620-1:2002

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>

1 Scope

1.1 General

This European Standard 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.

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;
 - 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;
 - 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 European Standard 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 European Standard should be 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

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

ISO 14300-1, *Space systems – Programme management – Part 1: Structuring of a programme.*

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef>

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

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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; or
- d) detrimental effects on the environment

[EN 13701:2001]

NOTE Accident and mishap are synonymous.

3.1.2**cause**

that which produces an effect; that which gives rise to any action, phenomenon or condition

NOTE 1 Cause and effect are correlative terms (Oxford English Dictionary).

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

NOTE 3 Adapted from EN 13701:2001.

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

[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

[NUREG/CR-2300 PRA:1982]

3.1.5**common mode failure**

failure of multiple identical items that fail in the same mode

NOTE 1 Common mode failures are a particular case of common cause failures.

NOTE 2 Adapted from NUREG/CR-2300 PRA:1982

3.1.6**contingency procedure**

pre-planned procedure to be executed in response to a departure from specified behaviour

[EN 13701:2001]

3.1.7**critical fault**

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

[IEC 60050:1992]

3.1.8**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

NOTE Adapted from EN 13701:2001.

3.1.9**fail safe**

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

[IEC 60050:1992]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 14620-1:2002](#)

[http://www.iso.org/standards/sist/86048528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002](#)

3.1.10

failure

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

[IEC 60050:1992]

3.1.11

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 A fault is often the result of a failure of the item itself, but can exist without prior failure.

NOTE 2 Adapted from IEC 60050:1992.

3.1.12

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

[IEC 60050:1992]

NOTE 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 [definition 3.1.11 above].

iteh STANDARD PREVIEW
(standards.iteh.ai)

[EN 13701:2001]

3.1.13

hazard

existing or potential condition of an item that can result in a mishap

ISO 14620-1:2002
<https://standards.iteh.ai/catalog/standards/sist/6c478528-6631-4282-a4ef-79a5060a1ed4/iso-14620-1-2002>

NOTE This condition can be associated with the design, fabrication, operation or environment of the item, and has the potential for mishaps.

[ISO 14620-2]

3.1.14

hazardous event

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

NOTE Adapted from EN 13701:2001.

3.1.15

incident

unplanned event that could have been an accident but was not

[EN 13701:2001]

3.1.16

inhibit

a 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 Two inhibits are independent if no single failure can eliminate more than one inhibit.

NOTE 2 Adapted from EN 13701:2001.

3.1.17**operator error**

failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator

3.1.18**organization**

group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLE Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

NOTE 3 This definition is valid for the purposes of quality management system standards. The term "organization" is defined differently in ISO/IEC Guide 2.

[EN ISO 9000:2000]

3.1.19**programme**

coordinated set of activities, not necessarily interdependent, that continue over a period of time and are designed to accomplish broad scientific or technical goals or increased knowledge in a specific subject

EXAMPLE The defence programme; The Apollo programme; Earth observation programme; Manned space and microgravity programme.

NOTE 1 A programme can comprise several projects.

NOTE 2 A programme can last several years. [ISO 14620-1:2002](https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-14620-1-2002)

<https://standards.iteh.ai/catalog/standards/sist/86048528-6631-4282-a4ef-14620-1-2002>

NOTE 3 "program" is American Standard English spelling for "programme".

NOTE 4 "program" is British Standard English for 'a series of coded instructions to control the operation of a computer or other machine' – Oxford English Dictionary.

3.1.20**project**

unique set of coordinated activities, with definite starting and finishing points, undertaken by an individual or organization to meet specific objectives within defined schedule, cost and performance parameters

[BS 6079:1996]

3.1.21**purchaser**

customer in a contractual situation

NOTE The purchaser is sometimes referred to as the "business second party".

3.1.22**residual risk**

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

[EN 13701:2001]

3.1.23**risk**

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

[EN 13701:2001]