SLOVENSKI STANDARD
SIST EN ISO 14620-1:2004

01-maj-2004

Space systems - Safety requirements - Part 1: System safety (ISO 14620-1:2002)

Space systems - Safety requirements - Part 1: System safety (ISO 14620-1:2002)

Raumfahrtsysteme - Sicherheitsanforderungen - Teil 1: Systemsicherheit (ISO 14620-1:2002)

Systemes spatiaux - Exigences de sécurité - Partie 1: Sécurité système (ISO 14620-1:2002)

Ta slovenski standard je istoveten z: **EN ISO 14620-1:2002**

ICS:

49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST EN ISO 14620-1:2004 **en**

Contents

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of an identical text or by endorsement, at the latest by June 2003, and conflicting national standards shall be withdrawn at the latest by June 2003.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.

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.

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*.

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]

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].

[EN 13701:2001]

3.1.13
hazard
existing or potential condition of an item that can result in a mishap

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 mirogravity programme.

NOTE 1 A programme can comprise several projects.

NOTE 2 A programme can last several years.

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]

3.1.24
safe state
state that does not lead to critical or catastrophic consequences

3.1.25
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

NOTE Adapted from EN 13701:2001.

3.1.26
safing
action of containment or control of emergency and warning situations or placing a system (or part thereof) in a predetermined safe condition

NOTE Adapted from EN 13701:2001.

3.1.27
supplier
organization or person that provides a product

EXAMPLE Producer, distributor, retailer or vendor of a product, or provider of a service or information.

NOTE 1 A supplier can be internal or external to the organization.

NOTE 2 In a contractual situation a supplier is sometimes called "contractor".

[EN ISO 9000:2000]

3.1.28
system
set of interdependent elements constituted to achieve a given objective by performing a specified function

NOTE The system is considered to be separated from the environment and other external systems by an imaginary surface which cuts the links between them and the considered system. Through these links, the system is affected by the environment, is acted upon by the external systems, or acts itself on the environment or the external systems.

[IEC 60050:1992]

3.1.29
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

3.1.30
warning condition
condition where potentially catastrophic or critical hazardous events are imminent and where pre-planned safing action is required within a limited time

NOTE Adapted from EN 13701:2001.

3.1.31
zonal analysis
systematic inspection of the geographical locations of the components and interactions of a system, evaluation of potential subsystem-to-subsystem interactions with and without failure, and assessment of the severity of potential hazards inherent in the system installation.