INTERNATIONAL STANDARD

ISO 14620-1

First edition
2002-12-01

Space systems — Safety requirements —

Part 1: System safety

Systèmes spatiaux — Exigences de sécurité —

Partie 1: Sécurité système

Reference number
ISO 14620-1:2002(E)

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.

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*

— *Part 2: Launch site operations*

The following part is under preparation:

— *Part 3: Flight safety systems*

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.

3.2 Abbreviated terms

The following abbreviated terms are used within this European Standard.

Abbreviation	Meaning
CCB	configuration control board
ECSS	European Cooperation for Space Standardization
EEE	electronic, electrical, electromechanical
FMECA	failure modes, effects and criticality analysis
FTA	fault free analysis
GEO	geostationary orbit
GSE	ground support equipment
IEC	International Electrotechnical Commission
LEO	low Earth orbit
MIL STD	military standard (US Department of Defense)
MIP	mandatory inspection point
NRB	nonconformance review board
NUREG-CR	US Nuclear Regulatory Commission contractor report
TRB	test review board
VTL	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 European Standard commensurate with the programme requirements.

b) The system safety programme should be tailored by the customer in accordance with the type of project, safety criticality, complexity, and phase of development in accordance with the requirements of ISO 14300-1 and ISO 14300-2.

   1) The supplier shall establish and maintain a system safety programme.

   2) The supplier shall apply launch site and launch vehicle safety requirements regulations as defined in the project requirements to support efficient and effective achievement of system safety objectives.

   3) The appropriate system safety programme requirements of this European Standard shall be applied for the implementation of the applicable launch site and launch vehicle requirements and regulations.

c) Compliance with the safety requirements defined herein does not relieve the supplier from compliance with national or international safety regulations.

d) Tailoring shall not diminish the intent 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.

4.2 Safety organization

4.2.1 General

Each supplier is responsible for the safety of his product as detailed in next subclauses.

4.2.2 Safety representative

Each supplier shall appoint a safety representative in accordance with ISO 14300-2 who is qualified by training or experience to perform system safety functions.

4.2.3 Reporting lines

Safety representatives shall have reporting lines to the project manager and access to top management that are independent of the hierarchical reporting line within the project.

4.2.4 Safety integration

Safety shall be integrated in all project activities.

4.2.5 Coordination with others

The safety representatives should coordinate with all affected medical boards, radiation protection committees, industrial safety organizations and environmental protection agencies as appropriate.

4.3 Safety representative access and authority

4.3.1 Access

The safety representative of an organization shall have access to that organization's safety related data relevant to project safety, and shall be at liberty to report freely, and without organizational constraint on any aspect of project safety.

4.3.2 Delegated authority to reject - stop work

The safety representative of an organization shall have the delegated authority to reject any project document, or to stop any project activity of this organization that does not conform to approved safety requirements or procedures.

4.3.3 Delegated authority to interrupt operations

To properly control risk, the safety representative of an organization shall have the delegated authority to interrupt hazardous operations of this organization and make the system under consideration safe again when it becomes clear that the operation does not conform to the agreed measures.

4.3.4 Conformance

The supplier shall assure conformance of his own and his subsuppliers' project activities with project safety policy and requirements.

4.3.5 Approval of reports

The supplier should not permit project reports that address matters related to safety certification to be issued without signed approval of the safety representative.

4.3.6 Review

No project hazardous operation or system mission shall be permitted to proceed without prior review and approval by the safety representative.

4.3.7 Representation on boards

Safety should be represented at configuration control boards (CCBs), nonconformance review boards (NRBs), test review board (TRBs), and at qualification, and acceptance reviews, where safety requirements and safety critical functions are involved. Safety should be further represented at medical boards or equivalent where exposure or endurance limits are defined for flight and ground crews.

4.4 Safety risk management

4.4.1 Risks

Risk to human life, investments made, mission and environment shall be managed throughout the project by performing the following activities:

a) allocation of safety requirements;

b) hazard identification;

c) hazard evaluation;

d) hazard prevention, reduction, and control;

e) hazard close out, including residual risk acceptance.

4.4.2 Hazard assessment

All hazard assessments shall consider primarily the hazard potential and categorize all hazards according to the appropriate severity category. Corresponding controls shall be proposed. The initial design shall be chosen such that the hazard potential and its related consequence severity are minimized. The probability of a hazardous event shall consequently be taken into account whenever hazard consequence severity reduction methods alone are considered insufficient to adequately reduce the risk. The probability of occurrence shall be reduced by considering all areas of design for minimum risk, increasing the reliability of safety devices, providing warning devices, or using procedural controls and training.

4.4.3 Preferred measures

Hazard potential reducing measures that as a minimum do not reduce reliability shall be preferred. Probability and therefore risk-related reduction measures that do not lead to increased criticality shall be preferred.

4.5 Project phases and safety review cycle

4.5.1 Progress meetings

The supplier shall hold regular safety progress meetings to review the status of safety programme activities as required by this European Standard. The meetings may be attended by the relevant customer and supplier specialists.

4.5.2 Project reviews

4.5.2.1 General

a) The supplier shall support safety reviews by the customer and, as necessary, the safety approval authority of the project safety status as required.

b) Safety reviews shall be performed at all levels necessary to ensure satisfactory implementation of safety programme and technical safety requirements.

c) A safety data package shall be prepared for each review.

d) Safety reviews should be performed in conjunction with the following milestones as applicable and the objectives as described in the respective subclause.

4.5.2.2 Mission definition review

During the mission definition review, the supplier shall demonstrate that:

a) Safety requirements and lessons learned from previous projects were analysed and support was provided to design and operations concept trade-off.

b) Main system level safety requirements were identified.

4.5.2.3 Preliminary requirements review

During the preliminary requirements review, the supplier shall demonstrate that:

a) System level applicable hazards, hazardous conditions and events, together with safety critical aspects and safety risk of the concepts analysed, were identified and compared.

b) Project system level safety requirements were refined.

4.5.2.4 System requirements review

During the system requirements review, the supplier shall demonstrate that:

a) Safety requirements were specified in sufficient detail to allow the definition of the technical solutions for the system concept selected in phase A, the feasibility phase.

b) Results of the safety analysis were available in order to confirm that the recommended solution was in agreement with the project safety requirements.

4.5.2.5 Preliminary design review

During the preliminary design reviews, the supplier shall demonstrate that:

a) Hazard controls and safety requirements were sufficiently defined for detailed design to start.

b) The design as presented conforms to the safety requirements to the level of detail required by the review.

c) Verification methods for hazard controls were proposed.

d) Definition of safety requirements was finalized at system and at lower levels.

e) The required activities were included in the project verification programme.

f) Deviations from safety requirements were identified.

4.5.2.6 Critical design review

During the critical design review the supplier shall demonstrate that:

a) The results of the safety analyses, performed on the solution obtained in the previous phase, were made available in order to permit verification that the detailed design is in agreement with the project safety requirements and can be used as a basis for manufacturing models to be used for qualification.

b) All changes made to technical requirements were assessed with respect to consequent changes to hazard controls.

c) Safety verification methods for all hazard controls were agreed upon and the necessary activities were entered into the verification programme.

4.5.2.7 Qualification review

During the qualification review, the supplier shall demonstrate that:

a) All design qualification activities related to critical items and safety critical functions, as appropriate to the level of the review, were completed and the applicable reports were approved.

b) All safety critical functions were qualified.

4.5.2.8 Acceptance review

During the acceptance review the supplier shall demonstrate that:

a) All late changes introduced into the design and technical requirements were assessed with respect to consequential changes to hazard controls and their verifications.

b) Verification for all defined hazard control measures was completed and accepted.

c) All open verifications were recorded in the verification tracking log (VTL) at this time. Verification procedures for verifications open at time of acceptance were qualified and mutually agreed upon as appropriate for later execution.

d) All safety related nonconformances, failures, waivers, and accident or incident reports were formally accepted and closed or documented on an open-items list with any constraints identified.

4.5.2.9 Flight readiness review

During the flight readiness review the supplier shall demonstrate that:

a) The VTL shows no further open verifications.

b) Verifications which shall be performed nominally at a later point in time (i.e. late access inspections), are closed on the basis of an existing, documented launch organization procedure and are executed by personnel who have been trained according to this procedure.

c) All open work related to safety critical functions was completed or scheduled as part of normal pre-launch activities.

d) All safety related nonconformances, failures, waivers, and accident or incident reports were formally accepted and closed.

e) All safety related flight anomalies on previously flown common designs or reflown hardware were resolved and closed.

4.5.2.10 Operational readiness review

During the operational readiness review, the results of the vehicle/ground compatibility tests and the operational qualification tests (during which the operational procedures shall have been verified) shall be assessed. This assessment shall verify that the combined operation of vehicle and ground facilities does not introduce new hazards or require additional controls.

4.5.2.11 Launch commitment meeting

During the launch commitment meeting, the current safety status shall be presented which documents any potential effects of countdown anomalies, weather and hardware or personnel conditions. It shall state whether the safety status is acceptable for launch to proceed and shall be subject to review and formal acceptance by the customer and the safety approval authority.

4.5.2.12 In orbit test review

During the in orbit test review, the validity of previous hazard and risk acceptance shall be reconfirmed considering any design or operational changes which have been introduced. This shall include assessment of the continued validity of previously accepted operational margins, and waivers against safety critical functions. Updated safety analyses shall be provided as necessary to support the decision to authorize continuous usage of the system.

4.5.2.13 End-of-life assessment

During the end-of-life assessment, a safety package shall be provided which documents the safety status of the system with respect to its capability to support the planned end-of-life and disposal operations and their conformance with the applicable requirements, including any relevant international safety regulations.

4.5.3 Safety programme review

The safety programme shall be reviewed, depending on project criticality, either:

a) as part of the scheduled project milestone reviews; or

b) as part of a dedicated safety review.

4.5.4 Safety data package

The supplier shall prepare and deliver the safety data package. The content of the safety data package shall be defined for each project or programme by the safety approval authority.

4.6 Safety programme plan

4.6.1 Implementation

The supplier shall show how the safety programme is implemented in the safety programme plan in accordance with ISO 14300-2. The plan may either be included as part of an overall project product assurance plan or as a separate safety programme sub-plan.

4.6.2 Safety activities

Safety planning shall cover the safety activities for the project phases as defined in ISO 14300-1.

4.6.3 Definition

The plan shall define:

a) the safety programme tasks to be implemented;

b) the personnel or supplier responsible for the execution of the tasks;

c) the schedule of safety programme tasks related to project milestones;

d) safety programme activity interface with project engineering and with other product assurance activities;

e) how the supplier accomplishes the tasks and verifies their satisfactory completion (by reference to internal procedures as appropriate).

4.6.4 Description

The plan shall include a description of the project safety organization, its responsibilities, and its working relationship with the reliability, maintainability, software product assurance, parts, materials and processes and quality assurance disciplines of product assurance, with configuration management, system engineering, design and other project functions and departments of organizations.

4.6.5 Safety and project engineering activities

The plan shall show how the project safety organization implements concurrent safety and project engineering activities in continuous support of the project design and development process.

4.6.6 Supplier and sub-supplier premises

The plan shall describe how safety related activities and requirements are defined for, and controlled at, suppliers' and sub-suppliers' premises. Only those requirements that are relevant to the sub-suppliers' and suppliers' activities and responsibilities shall be made applicable.

4.6.7 Conformance

The plan shall make provisions for assuring conformance to safety requirements and regulations that are applicable to any other facilities and service that are utilized during the course of the project.

4.7 Safety certification

a) All projects shall certify the safety of the flight and ground system products as having reached an acceptable level of risk in conformance to project specific safety requirements.

b) The certification process shall be completed before delivery to any party other than the purchaser.

c) The certification shall include a statement that open verifications shall be closed in accordance with the established verification tracking log and do not affect further safe processing at third party premises.

d) For any given project, the entity that defines, or makes applicable, detailed technical safety requirements constitutes the safety approval authority or part thereof.

e) It shall be the responsibility of the project organization to provide to the certification authority all safety related information that is required to enable the statement of safety compliance to be accepted and understood.

4.8 Safety training

4.8.1 Overall training

a) Safety training is a part of the overall training as required by ISO 14300-1 and ISO 14300-2.

b) All safety related training of any personnel working - permanently or occasionally - with products that can have hazardous properties has three major aspects:

1) general awareness briefings on safety measures to be taken at a given location or working environment;

2) basic technical training in the required safety techniques and skills (e.g. inspection, test, maintenance or integration), which are mandatory to fulfil the job function under consideration;

3) product specific training that focuses on the hazards related to the specific product.

4.8.2 Participation

Participation in the general awareness briefing shall be mandatory for all personnel who have access to the area where the product is processed.

4.8.3 Detailed technical training

Detailed technical training shall be provided to all project engineering and safety personnel working with hazardous products.

4.8.4 Product specific training

Product specific training shall be provided by specialists to all new project engineers as well as the flight and ground crews.

4.8.5 Records

Records of personnel having received training shall be maintained.

4.8.6 Identification

Where safety training is identified as required for the flight operations crew or for mission control personnel, this shall be identified to the customer together with a definition of the type of training required and its scope. The supplier shall support implementation of the training programme as defined by the customer.

4.9 Accident/incident reporting and investigation

a) The supplier shall report to the responsible entity all accidents and incidents that affect the product and occur during project activities under the control of the supplier or his sub-suppliers.

b) The supplier shall support project related accident and incident investigations that occur outside of the supplier's control or facility at the request of the responsible entity.

4.10 Safety documentation

4.10.1 General

The supplier shall maintain safety-related data to support reviews and safety certification.

4.10.2 Customer access

The customer shall be given access to the data contained in the safety data file on request during audits, safety reviews and meetings held at the supplier's premises within the restrictions of the contract.

4.10.3 Supplier review

The supplier shall review project documentation including specifications, drawings, analyses, procedures and reports, nonconformance reports, failure reports, waivers, and documentation changes in order to verify or assess impact on:

a) the implementation of safety requirements and hazard and risk controls;

b) incorporation of hazard and risk controls into the design or the verification programme;

c) completion of verification activities;

d) the design and operational safety of the system;

e) the validity of safety analyses performed and documented.

4.10.4 Documentation

a) Records shall be maintained of the documents reviewed.

b) Safety documentation shall be updated where necessary to maintain currency.

c) The supplier shall certify that the safety documentation is accurate, valid, comprehensive and complete prior to launch site processing.

4.10.5 Safety data package

a) The supplier shall submit a safety data package for review - see 4.5.4. This may be a stand-alone package or may be integrated into the overall data package if the safety review is part of an overall project review.

b) The content of the data package shall be specified by the safety approval authority.

c) The design and operational baseline that is the subject of the safety data package shall be defined by reference to the relevant documentation.

d) Any data requested during previous safety reviews shall be incorporated into the safety data package.

e) The supplier shall integrate safety data related to the various subsystems or equipment that make up the system into the safety data package that is presented at the safety review.

f) All safety data shall be traceable from the safety data package and available for review as appropriate.

4.10.6 Safety deviations and waivers

4.10.6.1 Request for deviation

Safety requirements that cannot be met shall be identified and a request for deviation or waiver shall be generated.

4.10.6.2 Description, analysis and rationale

The deviation or waiver request shall describe why the requirement cannot be met and provide sufficient analysis and rationale to support an exception to the safety requirement.

4.10.6.3 Identification and review

The supplier shall identify all deviations and waivers that affect the applicable project safety requirements. The supplier's safety representative for the project shall review these deviations and waivers to ensure that possible impacts on safety are fully analysed. Adequate justification for any deviation considered acceptable by the supplier shall be provided.

4.10.6.4 Assessment of deviation

The accumulated deviations and waivers that affect safety shall be assessed to ensure that the effects of individual deviations do not invalidate the rationale used for the acceptance of other deviations. The supplier shall maintain a tracking list that identifies all safety-related deviations and waivers reviewed.

4.10.6.5 Review and disposition

Deviations and waivers that affect project safety requirements or safety critical functions which the supplier considers acceptable, shall be the subject of review and disposition by the customer's safety authority.

4.10.6.6 Certification authority approval

Safety deviations and waivers shall be subject to safety approval authority acceptance.

4.10.7 Verification tracking log

A verification tracking log shall be maintained in which the completion steps associated with hazard control verification items are clearly stated. Once the verification methods have been documented to mutual satisfaction of project and certification bodies, the verification tracking log establishes the validation record.

4.10.8 Lessons-learned file

a) The supplier shall collect the safety lessons learned during the project. The supplier shall make sure that the lessons learned are used during the project, as far as they are relevant.

b) Safety lessons learned should consider as a minimum:

1) the impact of newly imposed requirements;

2) assessment of all malfunctions, accidents, anomalies, deviations and waivers;

3) effectiveness of safety strategies of the project;

4) new safety tools and methods which have been developed or demonstrated;

5) effective versus ineffective verifications which have been performed;

6) changes proposed to safety policy, strategy or technical requirements with rationale.

5 Safety engineering

5.1 Safety engineering policy

5.1.1 General

Safety is an integral part of all project product assurance and engineering activities. It shall not be a stand-alone activity. The quality of all safety engineering related work shall be based on assurance that the system is designed, qualified, manufactured, and operated in accordance with product assurance requirements.

5.1.2 Elements

Safety engineering consists of management of hazard and risk reduction processes, hazard and risk potential assessment, design assurance, and hazard and risk control activities.

5.1.3 Lessons learned

Maximum use should be made of lessons learned in the design process.

5.2 Safety design principles

5.2.1 Human life consideration

The preservation of personnel safety shall be the most important priority in the development and operation of space systems.

5.2.2 Design selection

The major goal throughout the design phase shall be to ensure inherent safety through the selection of appropriate design features. Damage control, containment and isolation of potential hazards shall be included in the design considerations. The design shall allow for debris, fall-out and impact prevention.

5.2.3 System safety order of precedence

The following sequence of activities shall be applied to identified hazards, hazardous conditions, and functions whose failures have hazardous consequences:

a) Hazard elimination

Hazards and hazardous conditions shall, consistent with the project constraints and mission objectives, be eliminated from the design and operational concepts by the selection of design technology, architecture and operational characteristics.

b) Hazard minimization

Where hazards and hazardous conditions are not eliminated, the severity of the associated hazardous events and consequences shall, consistent with the project constraints and mission objectives, be minimized through selection of the least hazardous design architecture, technologies, and operational characteristics.

c) Hazard control - Safety devices

Hazards that are not eliminated through design selection shall be reduced and made controllable through the use of automatic safety devices as part of the system, subsystem or equipment. Safety inhibits shall be independent and verifiable.

d) Hazard control - Warning devices

When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safety devices, devices shall be employed for the timely detection of the condition and the generation of an appropriate warning signal. This shall be coupled with emergency controls of corrective action for operators to safe or shut down the affected subsystem.

e) Hazard control - Special procedures

1) When it is not possible to reduce the magnitude of a hazard through the design, the use of safety devices or the use of warning devices, special procedures shall be developed to counter the hazardous conditions for the enhancement of flight crew safety.

2) Special procedures can include emergency and contingency procedures, procedural constraints, or the application of a controlled maintenance programme.

3) Special procedures shall be qualified and appropriate training shall be provided for personnel.

4) Special procedures are the least effective of the hazard control and risk reduction measures available. Emphasis shall therefore be given to hazard control by the application of the alternative hazard control measures in the defined order of precedence.

5) The requirement for hazard detection, signalling and safing by the flight crew to control time-critical hazards shall be minimized and shall not be implemented if an alternative means of reduction or control of hazardous conditions is available.

6) To permit the use of real time monitoring, hazard detection and safing systems for hazard control, the availability of sufficient flight crew response time shall be verified. Acceptable safing procedures shall be developed and verified and the personnel trained.

7) Physical barriers, safe separation distances, minimal personnel allowance with access control, remote monitoring, tagout/lockout methods, and time-limited exposure shall be considered as means of hazard mitigation and risk reduction.

5.2.4 Environmental compatibility

a) The system design shall meet the applicable safety requirements under the worst-case natural and induced environments defined for the project.

b) Design and performance margins shall be established and applied considering worst-case combinations of induced and natural environments and operating characteristics.

5.2.5 Safe without services

Whenever the safe operation of the system depends on externally provided services (e.g. power), the system design shall be such that critical or catastrophic consequences are not induced (at least for a certain interval of time that shall be defined for each project) after the loss or upon the sudden restoration of those services.

5.2.6 Fail safe design

The system, and its parts thereof, shall be designed in such a way that failures brings the system into a safe state.

5.2.7 Hazard detection - Signalling and safing

a) Safety monitoring, display, alarm and safing capabilities shall be incorporated for human space flight systems. These capabilities shall provide the information necessary to allow the flight crew and ground system operators to take actions which are necessary to protect personnel from the consequences of failures within safety critical functions and the failure of hazard control measures.

b) The system design shall provide the capability for detecting failures that result in degradation of failure tolerance with respect to the hazard detection, signalling and safing function. When implemented, the performance of these functions shall be verifiable during manned flight and ground operational phases.

c) The emergency, caution and warning function shall detect and notify the flight crew and ground system operators of emergency, warning and caution situations.

d) Safing functions and capabilities shall be included which provide for the containment or control of emergency, warning and caution situations.

e) Provisions shall be included for the monitoring of safing function execution.

f) Dedicated safing functions shall be provided for emergency situations. Control of warning and caution situations shall be acceptable by system re-configuration or by dedicated safing functions, as appropriate to each case.

g) No single failure shall cause loss of the emergency and warning function.

h) Where the operation of a safing system introduces a new hazard, as a minimum, inadvertent activation of the safing system shall be controlled in accordance with the failure tolerance requirements.

i) No single failure shall cause loss of the emergency and warning functions together with the monitored functions.

j) Emergency, warning and caution data, out of limit annunciation and safing commands shall be given priority over other data processing and command functions.

k) When systems or elements are integrated into, or docked with the other systems or elements, the emergency, warning, caution, and safing function shall enable the areas of control responsibility to monitor and display the applicable parameters, and to control the relevant safing functions.

l) Emergency, warning, and caution parameter status information shall be available and displayed at the launch control and mission control centres in “near-real-time” during the relevant operational phases. It shall be possible for the flight crew to ascertain and monitor in “real time” the status of emergency, warning and caution parameters of non-crewed systems or elements prior to docking with crewed systems.

5.2.8 Access

All project products shall be designed such that any required access to products during flight or ground operations can be accomplished with minimum risk to personnel.

5.3 Safety risk reduction and control

5.3.1 Severity

a) The severity of identified hazardous events shall be categorized as shown in Table 1:

Table 1 — Severity of identified hazards and consequences (1)

Severity		Consequence	
1)	Catastrophic hazards	i)	loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system;
		ii)	loss of launch site facilities or loss of system;
		iii)	severe detrimental environmental effects.
2)	Critical hazards	i)	temporarily disabling but not life-threatening injury, or temporary occupational illness;
		ii)	major damage to flight systems or loss or major damage to ground facilities;
		iii)	major damage to public or private property; or
		iv)	major detrimental environmental effects.

b) In addition to the above two categories, other categories may be used to complete assessment of the safety risk being assumed. Two sample categories are shown in Table 2:

Table 2 — Severity of identified hazards and consequences (2)

Severity		Consequence
3)	Marginal hazards	minor injury, minor disability, minor occupational illness, or minor system or environmental damage.
4)	Negligible hazards	less than minor injury, disability, occupational illness, or less than minor system or environmental damage.

c) The availability of:

1) design features which reduce the probability of a hazardous event occurring, but which do not affect its severity;

2) warning devices, flight crew safe haven, or flight crew escape capabilities

shall not be used as rationale for the reduction of the hazard severity level.

d) For international programmes, a coherent set of consequence severity shall be established for joint operational phases. These categories shall not violate the policy of prioritization for the protection of human life, nor the principles of categorization in accordance with the definition of consequence severity categories in Table 1.

e) Consequence severity classifies hazards according to their impact on human life. This impact can be immediate and personal. It also can be on a broader scale not limited to a single person only. The hazardous consequences can be short term or long term. Detrimental environmental effect, from the point of view of long term hazardous consequences to the global public, shall be considered.

f) In space flight, the environment concerned can be outer space, including the Moon and the planets, geostationary orbit (GEO), low Earth orbit (LEO) as well as the Earth's atmosphere. Careful system studies should be performed to assess the future consequences of current technology.

5.3.2 Failure tolerance requirements

5.3.2.1 Basic requirements

Failure tolerance is one of the basic safety requirements that is used to control hazards. The design of the system shall meet the following failure tolerance requirements:

a) No single failure or operator error shall have critical (or catastrophic) consequences.

b) No combination of:

   1) two failures; or

   2) two operator errors; or

   3) one failure and one operator error

   shall have catastrophic consequences.

c) All hazards not controlled by conformance to failure tolerance shall be controlled by conformance to design to minimum risk or by meeting probabilistic safety targets.

d) Technical requirements for areas of design for minimum risk shall be identified and approved by the relevant safety approval authorities.

5.3.2.2 Software

a) The required failure tolerance for software that supports a safety critical function shall be implemented utilizing dissimilar methods and algorithms (diversity). Alternatively, independent hardware back-up to the software function may be provided.

b) Anomaly detection for, and actuation of safety functions, such as emergency stops, should be independent of software and program logic controllers.

c) Acceptable software safety can be achieved through a formal software safety programme consisting of software hazard analysis, software design requirements analysis, test, and verification and validation.

5.3.2.3 Payload interface

Having taken into account any failure tolerance of the payload services provided by the carrier, the payload shall be designed so that loss or degradation of resources, supplied to the payload by the carrier, shall not result in catastrophic or critical hazardous consequences.

5.3.2.4 Redundancy separation

a) The system design should include the capability for on-board redundancy management of safety critical functions, and provide failure tolerance and redundancy status information to the flight and ground crews, including immediate flight crew notification in the case of failure detection, redundancy switch-over, or loss of operational redundancy.

b) Redundancy management shall include failure detection, failure isolation and switching of redundant items.

c) The flight crew and mission control shall be able to override automatic safing and redundancy switch-over.

d) Alternate or redundant safety critical functions shall be physically and functionally separated or protected in such a way that any event which causes the loss of one path shall not result in the loss of alternative, or redundant paths.

5.3.2.5 Failure propagation

Hardware or software failures shall not cause additional failures with hazardous effects or propagate to cause the hazardous operation of interfacing hardware.

5.3.3 Design for minimum risk

5.3.3.1 General

Hazards related to design for minimum risk areas of design (e.g. mechanisms, structures, pressure vessels, pressurized lines and fittings, pyrotechnic devices, material compatibility and material flammability) shall be controlled by the safety-related properties and characteristics of the design, such as margin or factors of safety. Failure tolerance requirements shall only to be applied to the design process as necessary to ensure that credible failures that can affect the design do not invalidate safety-related properties.

5.3.3.2 Fracture control

Where structural failure can have catastrophic or critical consequences, structures, pressure vessels, fasteners and load-bearing paths within mechanisms shall be designed in accordance with recognized fracture control standards.

5.3.3.3 Safety factors

a) Structural safety factors shall be defined and applied.

b) The worst credible combination of environmental conditions shall be considered for determined safety margins.

5.3.3.4 Materials

Materials shall be selected and controlled. Material selection shall assure that hazards associated with material characteristics (e.g. toxicity, flammability, resistance to stress corrosion, outgassing, offgassing, resistance to radiation, resistance to thermal cycling, arc tracking, thermal degradation and microbiological growth) are either eliminated or controlled. If this is not feasible, the system design shall include the necessary provisions (e.g. containment of hazardous substances) to control hazardous events associated with material characteristics in accordance with the requirements of this European Standard.

5.3.4 Probabilistic safety targets

a) Probabilistic safety targets should be established for hazardous consequences at system level for each project or programme. These probabilistic targets should assist in the acceptable risk decision for each identified hazard.

b) In establishing these safety targets, conformance should be ensured with the requirements set up by launch safety authorities and national and international regulations. Additionally, the following criteria should also be taken into account when setting up the targets:

   1) with respect to targets for the ground and flight personnel, the individual risk should be comparable to the one accepted for other professionally exposed personnel (e.g. risk for flight crew members could be compared to the one for test pilots, risk for ground personnel should be comparable to the one for similarly exposed industrial workers);

   2) with respect to targets for the civil population, the total risk for the exposed ground population should be compared with the one caused by other hazardous human activities (e.g. risk from overflight of commercial aircraft, chemical plants, as appropriate).

c) The assessment of conformance with the safety targets should also be used to:

   1) identify and rank major risk contributors;

2) support the decision-making process for those cases where nonconformances with the qualitative requirements are identified.

d) Safety targets shall not be used as the sole requirements imposed on a system, but they should be used in combination with the other qualitative requirements of this European Standard.

e) Additionally, note that the allocation of "targets" to the various functions and subsystems is addressed in 6.1. The conformance with the quantitative requirements shall be performed through risk analysis (see 6.4.3).

5.4 Identification and control of safety critical functions

5.4.1 Identification

A system function that, if lost or degraded, or through incorrect or inadvertent operation, would result in a catastrophic or critical hazardous consequence, shall be identified as safety critical function.

EXAMPLE A series of operational events that can result in a hazard if they occur inadvertently or are operated out of order.

5.4.2 Inadvertent operation

Inadvertent operation of a safety critical function shall be prevented by:

a) two independent inhibits, if it induces critical consequences;

b) three independent inhibits, if it induces catastrophic consequences.

5.4.3 Provisions

The system shall provide the following for manned space systems and the following should be a goal for ground operation of the system for unmanned space systems:

a) failure tolerance and redundancy status information of safety critical functions;

b) the status of at least two inhibits for manned flight and one inhibit for unmanned flight on functions that, if inadvertently operated, could lead to catastrophic consequences to the flight and ground crew, including:

1) notification in real time in case of failure detection;

2) announcement of any loss of operational redundancy;

3) notification of redundancy switch-over; or

4) changes of inhibit status.

5.4.4 Safe shutdown and failure tolerance requirements

The design shall either provide the capability for the safe shutdown of safety critical functions prior to in-flight maintenance operations or shall conform to the failure tolerance requirements during maintenance operations.

5.4.5 Electronic, electrical, electromechanical

Electronic, electrical, electromechanical (EEE) components used to support safety critical functions in flight standard hardware shall be selected and procured in accordance with the applicable programme requirements. [See also ISO 14621].

6 Safety analysis requirements and techniques

6.1 General

a) Safety analyses shall be performed in a systematic manner in order to ensure that sources of safety risk are identified and eliminated or are minimized and controlled.

b) Safety risks can be the result of the hazardous characteristics associated with the:

1) design, including the technology selected, the physical arrangement of elements, subsystems and equipment;

2) operating modes;

3) potential for operator error;

4) operating environment;

5) hazardous effects which can result from the failure of functions.

c) Safety analyses shall be initiated early in the design phase and shall provide concurrent support to project engineering in the selection of the least hazardous design and operational options that are compatible with the project mission and programme constraints.

d) The results of safety analyses shall also be used to support project management in the verification of risk reduction, ranking of risk sources, support to project resource allocation, monitoring of risk trends, and residual risk acceptance.

e) Analysis shall always be made with reference to a defined configuration baseline.

6.2 Assessment and allocation of requirements

6.2.1 Safety requirements

The supplier shall respond to the applicable safety requirements for the project.

6.2.2 Additional safety requirements

The supplier shall also identify additional safety requirements through the use of lessons learned from previous projects and the safety analyses performed during the project.

6.2.3 Define safety requirements - functions

The supplier, taking into account the results of functional failure analysis and the system level safety requirements, shall define the safety requirements for the various functions of the system.

6.2.4 Define safety requirements - subsystems

Subsequently the supplier, taking into account the results of the preliminary safety analysis and the architecture of the system, shall define the safety requirements associated with the various subsystems.

6.2.5 Justification

The supplier shall justify the proposed allocation of safety requirements at the latest at the end of the detailed definition phase.

6.2.6 Functional and subsystem specification

The supplier shall ensure that the function and subsystem-level safety requirements are included in the relevant functional and subsystem specification.

6.3 Safety analysis

6.3.1 General

Safety analysis shall be refined and updated in an iterative manner as the design process proceeds, to ensure that hazards and hazardous events are assessed, and that the relevant detailed design and operational requirements, hazard controls, and verification activities are defined and implemented.

6.3.2 Mission analysis

Safety analysis shall support the identification of major sources of safety risk as well as the performance of preliminary trade-offs between possible system concepts.

6.3.3 Feasibility

Safety analysis shall support trade-offs in arriving at the concept that has acceptable safety risk considering the project and mission constraints. The design technology selected and the operational concept to be implemented shall be selected based on the analysis data for the safest system architecture to eliminate or minimize hazards.

6.3.4 Preliminary definition

The safety analysis shall support a continued and more detailed safety optimization of the system design and operations and the identification of technical safety requirements and their applicability. The analysis shall also provide inputs to safety risk assessment in support of safety risk evaluation, the identification of significant risk contributors in the design and in the operational concept.

6.3.5 Detailed definition, production and qualification

Safety analysis shall support detailed design and operational safety optimization, safety requirements implementation evaluation, risk reduction verification, and hazard and risk acceptance. Analysis of operations shall also support the identification of emergency and contingency response planning and training requirements, and the development of procedures.

6.3.6 Utilization

Safety analysis shall evaluate design and operational changes for impact on safety, verifying that safety margins are maintained and that operations are conducted within acceptable risk. The analysis shall also support the evaluation of operational anomalies for impact to safety, and the continued evaluation of risk trends.

6.3.7 Disposal

Safety analysis shall evaluate all disposal operations and the hazards posed to the ground population and environment by the disposal. Disposal solutions with minimal hazardous consequences shall be identified.

6.4 Specific safety analysis

6.4.1 General

The types of analyses to be selected for a given project shall be proposed by the product supplier on the bases of past experience and updated as necessary in the course of the safety analysis.

NOTE Safety analysis consists of a combination of all the analyses described in the following subclauses. Supporting analysis is described in 6.5.

6.4.2 Hazard analysis

a) Hazard analysis shall be performed in a systematic manner, beginning in the concept phase and continuing through the operational phase, including end-of-life and disposal.

b) Hazard analysis shall identify and evaluate:

   1) hazards associated with system design, its operation and the operation environment;

   2) the hazardous effects resulting from the physical and functional propagation of initiator events;

   3) the hazardous events resulting from the failure of system functions and functional components;

   4) time critical situations.

c) The following potential initiator events shall be considered:

   1) hardware failure (random or time dependent);

   2) latent software error;

   3) operator error;

   4) design inadequacies, including:

      i) inadequate margins;

      ii) unintended operating modes caused by sneak-circuits;

      iii) material inadequacies and incompatibilities;

      iv) hardware - software interactions;

   5) natural and induced environmental effects;

   6) procedural deficiencies.

d) This includes a systematic analysis of the “system” operations and operating procedures which shall be performed in the detailed design and operational stages of a project. This analysis evaluates the capability of the system to be operated safely, to determine the safest operating modes, and to evaluate the acceptability of the operating procedures. The analysis shall be repeated as the design and operational detail evolves, particular attention being paid to the system’s operational modes and man/machine interfaces.

6.4.3 Safety risk assessment

a) Safety risk assessment shall be performed in progressive steps during the implementation of the safety programme.

b) Risk assessment shall be used to:

   1) support design trades (risk comparison);

   2) rank risk contributors;

   3) identify major risk contributors;

4) support the safety decision-making process (e.g. for waivers, unresolved residual risks);

5) monitor the effectivity of the hazard control and risk-reducing process by assessing safety risk trends;

6) assess conformance to probabilistic safety targets.

c) The results of safety risk assessment shall not be used as the sole basis for acceptance or rejection of residual risks.

d) The supplier shall identify sources of data and rational used for safety risk assessment.

6.4.4 Safety analysis for hardware-software systems

6.4.4.1 Safety critical function

Software that implements or controls safety critical functions shall be subject to safety analysis. The software safety analysis may be performed as a stand-alone software safety analysis or as part of other safety analyses depending on the application. In any case, the scope and level of depth of the software safety analysis identified by means of the functional failure analysis and the preliminary system level safety analyses and its performance shall be coordinated with system FTA, hazard analysis, FMECA and sneak analysis, as appropriate.

6.4.4.2 Requirements definition phase

During the software requirements definition phase the supplier shall examine the system and the software requirements in order to identify unsafe modes (e.g. out of sequence, wrong event, inadvertent command, failure to command and deadlocking). The analysis should preferably be performed by means of (top level) FMECA and FTA. Appropriate software safety requirements shall be identified in the software requirements document to control the above mentioned unsafe modes.

6.4.4.3 Architectural and detailed design phase

During the software architectural design and the detailed design phases, the supplier shall determine where, and under what conditions, the system might trigger hazardous events. Input/output, timing and effects of hardware failures on the software should be included in the analysis at this stage. FTA and check list based design review methods may be used.

6.4.4.4 Software code

When the software code becomes available, the supplier shall:

a) analyse for correctness and completeness;

b) verify that the software safety requirements have been properly implemented;

c) verify that the software can handle the appropriate conditions with expected input overload conditions.

6.5 Supporting assessment and analysis

6.5.1 General

The application of the following supporting assessment and analysis tools is at the discretion of the programme or project authorities.

6.5.2 Warning time analysis

a) Warning time analysis shall be performed during the concept definition phase and the design and development phase in order to evaluate time-critical situations identified in the hazard analysis and to support the implementation of hazardous-situation detection and warning devices or contingency procedures.

b) The analysis shall determine:

1) the time during which the event shall be detected and the response action taken;

2) the detection capability of the proposed design with respect to detection sensitivity and detection time;

3) the resultant time available for response;

4) the adequacy of the proposed design or contingency procedures, including emergency evacuation, rescue, system re-configuration, redundancy switching, and maintenance.

c) The detection times to be determined shall be:

1) from the occurrence of the initiating event to the time when a hazardous consequence occurs (propagation time);

2) the time from the occurrence of the initiating event to the time of earliest detection or annunciation; and

3) the time taken for corrective action to be implemented.

6.5.3 Caution and warning analysis

a) Caution and warning analysis shall be performed during the concept definition phase and the design and development phase of human space flight programmes in order to identify:

1) emergency, warning, and caution parameters;

2) the required safing functions and capabilities;

3) limit sensing requirements;

4) the applicability of the individual “caution and warning” functions to the different mission phases.

b) The caution and warning analysis shall utilize the results of the warning time and hazards analyses as appropriate.

6.5.4 Common cause and common mode failure analysis

6.5.4.1 Multiple failures

Multiple failures, which result from common cause or common mode failure mechanisms, shall be considered as single failures for determining failure tolerance.

6.5.4.2 Identification of requirements and scope

The supplier shall identify the requirement for and the scope of dedicated common cause and common mode analyses by means of the review of the results of the other safety analyses, such as fault tree analysis (FTA) and hazard analysis, and of the characteristic of the system and of its environment.

6.5.4.3 Identification of common cause failures

The supplier shall identify potential common cause failures by assessment of the effects of common causes (e.g. radiation, thermal environment and fires). This analysis shall be performed in coordination with the FTA and the hazard analysis. The analysis of common cause failures can require that use be made of the result of dedicated engineering analyses (e.g. thermal analyses, meteorite or debris impact analysis).

6.5.4.4 Analysis of common mode failures

Common mode failures shall be analysed by means of the use of check lists (to be established by the supplier) that list potential common modes for system components during the manufacturing, integration, test, operation and maintenance phases. The common mode analysis should be coordinated with the failure modes, effects and criticality analysis (FMECA).

6.5.4.5 Integration of results

Results of common cause and common mode analysis should be integrated, at the appropriate level, together with the results of the system level safety analyses (fault tree analysis, hazard analysis).

6.5.5 Fault tree analysis

The fault tree analysis shall be used to establish the systematic link between the system-level hazard and the contributing hazardous events and subsystem, equipment or piece part failure. A fault tree analysis, or its equivalent, shall be performed to verify the failure tolerance of the product.

6.5.6 Human dependability analysis

a) Whenever safety analyses identify human errors as a cause of catastrophic or critical hazards, a dedicated human dependability analysis should be carried out.

b) The human dependability analysis shall be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human errors.

c) The human dependability analysis shall be developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.

6.5.7 Failure modes, effects and criticality analysis

The results of failure modes, effects and criticality analysis (FMECA) shall be used to support the hazard analysis in the evaluation of the effects of failures. FMECA and hazard analysis shall be considered complementary analyses.

6.5.8 Sneak analysis

6.5.8.1 Applicability

The aim of sneak analysis is to identify "sneak circuits", i.e. unexplained paths for a flow of mass, energy, data or logical sequence that under certain conditions can initiate an undesired function or inhibit a desired function. Sneak circuits are not the result of failure but are latent conditions inadvertently designed into the system. During design and development phases the following should be subject to sneak analysis:

a) functions whose failure would result in catastrophic consequences;

b) emergency, warning and dedicated safing sub-functions;

c) flight crew escape and rescue supporting sub-functions,.

6.5.8.2 Use of results

a) Sneak analysis results shall be used to support the hazard analysis and the FMECA in the identification of the possible causes of hazardous events or of failures, and to support design review.

b) Use shall be made of the results of functional failure analysis and hazard analysis to identify, within the applicable functions, the detailed scope of the sneak analysis by application of the following criteria:

1) sub-functions or items which do not conform to the applicable safety requirements, or which cannot be verified as conforming with those requirements, shall be analysed;

2) command and control sub-functions shall be included;

3) electrical power distribution sub-functions shall be included;

4) passive sub-functions (e.g. primary or secondary structures, passive thermal control) shall be excluded.

6.5.9 Zonal analysis

6.5.9.1 Definition

See 3.1.31.

6.5.9.2 Redundancy and objectives

Zonal analysis shall be performed where redundancy is used to reduce the probability of losing a function or of inadvertently actuating a safety critical function. The objectives of the zonal analysis are to ensure that equipment installation meets the adequate safety requirements regarding:

a) basic installation rules and space practices;

b) interaction between subsystems;

c) implication of human errors;

d) effects of external events.

6.5.10 Energy trace analysis

The basic elements of the energy trace are energy sources, targets and barriers. The energy sources associated with the system shall be identified and assessed for intensity. Then the analyst shall identifiy safety targets that can be adversely affected by each energy source. The final step shall be to identify barriers that can prevent the flow of energy to the targets. Barriers can be physical, time or space.

7 Safety verification

7.1 General

a) In order to be able to assure that safety has been built into the product, a system shall be in place which makes it possible to track all hazards and related risks, to relate all verifications of the corresponding hazard uniquely to unambiguous causes and controls.

b) Test, analysis, inspection and “review of design” are common techniques for verification of design features used to control hazards. The successful completion of the safety process requires positive feedback of completion results for all verification items associated with a given hazard.

7.2 Tracking of hazards

7.2.1 Hazard reporting system

The supplier shall establish a hazard reporting system for tracking the status of all identified hazards. The system shall be applied for all catastrophic and critical consequences.

7.2.2 Status

a) The status shall be either “open” or “closed”.

b) An “open” status shall, as a minimum, be indicated as:

1) controls defined and agreed within the supplier’s project organization;

2) verification methods defined and agreed within the supplier’s project safety, engineering and management organization;

3) verification completed and submitted for acceptance.

7.2.3 Safety progress meeting

Status of hazard control and risk reduction activities shall be reviewed at safety progress meetings and formally documented and submitted for customer review at project safety reviews - see 4.5.1.

7.2.4 Review and disposition

Hazards and safety risks with catastrophic and critical consequences shall be submitted for review and formal disposition by an appropriate approval authority.

7.2.5 Documentation

a) All hazard documentation shall be formally issued for each safety review and major project review.

b) When procedures or processes are critical steps in controlling a hazard, and subsequent test or inspection cannot independently verify the procedure or process results, then the procedure or process shall be independently verified in real time.

7.2.6 Mandatory inspection points

Critical procedure or process steps shall be identified as mandatory inspection points (MIPs) or as requiring independent observation.

7.3 Safety verification methods

7.3.1 Verification engineering and planning

a) Verification engineering shall select the best-suited, cost-effective verification methods consistent with verification requirements as documented.

b) Verification planning shall commence in an integrated fashion as soon as the control method has been selected.

7.3.2 Methods and reports

Safety verification methods can be review of design, analysis, inspection and test. For all safety verifications traceability shall be provided.

7.3.3 Verification requirements

With respect to the given design baseline, the requirement shall be verified by comparison of the review of design requirement with specification or drawing, as appropriate.

7.3.4 Analysis

a) All technical safety and engineering analysis performed or updated with analysis in respect to the as-built configuration can be used for verification.

b) Similarity is a special case of analysis since the basis for assessing that similarity is provided by analysis. For tracking purposes a similarity analysis shall contain a copy of (or a unique reference to) the referenced previous verification, verification procedure and requirement valid at the time of the first verification.

7.3.5 Inspections

a) All pre-flight safety inspections shall be assessed for inclusion in the MIP list. If included on the MIP list, close-out is feasible by MIP reporting or individual reporting as appropriate.

b) Launch preparation inspections shall be entered into the appropriate launch base procedure. The close-out shall be given by the approved launch authority procedure.

c) Late access procedures shall be the subject of training and shall be performed by qualified personnel.

d) Inflight inspections, including telescience inspections, shall be entered into flight procedures and operation manuals.

e) Training for flight crew and mission operation teams shall be performed. Training shall consist of product specific safety briefing, product training and mission simulation as appropriate.

f) Close-out shall be by safety-approved procedure, documented training session and a sufficient number of simulations.

7.3.6 Tests

Tests shall be performed for all safety critical functions. End-to-end testing should be used for safety critical functions.

7.3.7 Verification and approval

The choice of verification should be with the supplier; the approval should be with the relevant safety approval authority.

7.4 Qualification of safety critical functions

7.4.1 Validation

Safety critical functions shall be verified by testing - end-to-end testing should be used - which shall include application of the operating procedures, the “man-in-the-loop”, and the verification of the effectiveness of applicable failure tolerance requirements. The tests shall include the demonstration of nominal, contingency and emergency operational modes.

7.4.2 Qualification

The safety critical characteristics of all safety critical functions shall be fully qualified by test. Safety critical function qualification testing shall include the determination of performance margins considering worst case combinations of induced and natural environments and operating conditions. Qualification “by similarity” shall be applied only after customer approval on a case by case basis.

7.4.3 Failure tests

Induced failure tests shall be performed when required by safety analysis for evaluating failure effects, and for demonstrating failure tolerance conformance in safety critical functions.

7.4.4 Verification of design or operational characteristics

Verification of unique safety required design or operational characteristics shall form part of the development, qualification or acceptance testing programmes as appropriate.

7.4.5 Safety verification testing

Where full-scale testing cannot be performed owing to cost or technical constraints, separate equivalent safety verification testing shall be performed using technically representative hardware or models.

7.5 Hazard close-out

7.5.1 Safety assurance verification

In time for acceptance by the customer, and in preparation of transfer to the launch site, safety assurance shall verify that:

a) hazard close-outs performed so far by the responsible engineer are still valid;

b) there have been no oversights;

c) the verifications reflect the as-built/as-modified status of the hardware;

d) all open verifications at this time are acceptable for transfer to the launch site;

e) all open verifications have been entered into the verification tracking log, which now becomes a living document.

7.5.2 Safety approval authority

Close out of each hazard requires approval by the safety approval authority. Hazards shall be considered for closure only when:

a) the hazard has been eliminated, or

b) the hazard has been minimized and controlled in accordance with the applicable requirement and the associated verification activities have been successfully completed, or

c) the safety approval authority has granted a deviation or waiver.

7.6 Residual risk reduction

Safety risks associated with catastrophic and critical consequences, which have been subject to the application of the hazard reduction precedence, shall be designated as residual risks. Residual risk shall be compared to the acceptable risk. Where the residual risk exceeds the acceptable risk additional risk reduction action shall be taken.

8 Operational safety

8.1 Basic requirements

During the operational phase, the safety issues assume even greater importance since all problems shall be dealt with in real time, under fixed resource constraints:

a) Safety involvement in the operational phase shall be planned.

b) Responsibilities, rules and contingency procedures shall be established prior to operation for hazardous “limit” conditions that can occur during ground and inflight operations.

c) Operating ranges and performance limits for safe operation shall be established for the design, and shall be specified.

d) The design should not require continuous active control by personnel in order to stay within the established operating ranges and performance limits.

e) Man/machine interfaces shall be designed and the personnel tasks shall be scoped to minimize the potential for hazardous events resulting from human error.

f) Limits for flight crew exposure to natural and system-induced environments shall be established and maintained by design features or operational constraints which cover nominal, contingency, and emergency operational modes, in order to preclude crew injury or inability to perform safety critical functions.

8.2 Flight operations and mission control

8.2.1 Launcher operations

Hazards to the public, public and private property and the environment, resulting from launcher system operation or malfunction shall be precluded by constraints applied to nominal and abort trajectories, staging, and the descent of spent stages.

8.2.2 Contamination

Normal or abort operations shall not result in contamination of the Earth’s environment that endangers human health, crops or natural resources or that exceed limits set by national or international regulations.

8.2.3 Flight rules

Flight rules shall be prepared for each mission that outline preplanned decisions designed to minimize the amount of real time rationalization required when anomalous situations occur. These flight rules do not constitute additional safety requirements but do define actions for spacecraft mission completion consistent with safety requirements.

8.2.4 Hazardous commanding control

Hazardous commanding control shall ensure that:

a) All hazardous commands shall be identified.

b) Hazardous commands are those that can remove an inhibit to a safety-critical function or activate an unpowered hazardous subsystem.

c) Failure modes associated with flight operation - including hardware, software and procedures - used in commanding from control centres or other ground equipment shall be considered in the safety assessment.

d) The system design shall provide protection to avoid the erroneous acceptance of commands that can affect personnel safety, or cause hardware or software damage.

e) Payload commands, which can result in catastrophic or critical hazardous consequences, shall be authorized and verified.

8.2.5 Mission operation change control

Mission operation change control shall ensure that:

a) All changes, which are desired or become necessary during mission, shall be reviewed for safety impact.

b) The responsible safety approval authority shall approve all operational change requests with safety impact.

8.2.6 Safety surveillance and anomaly control

a) During mission operations, appropriate attention shall be given to all product parameters that have been identified in the safety review process as safety status parameters.

b) Safety status parameters are all those parameters that make it possible to assess the status of the implemented hazard controls.

8.3 Ground operations

8.3.1 Applicability

The following requirements shall be applicable to:

a) development, qualification and acceptance testing;

b) assembly, integration and test operations;

c) launch site operations;

d) servicing and turn-around operations; and

e) transportation and handling operations

where those locations:

1) are potentially hazardous to personnel or project hardware; or

2) have high risks in terms of programme importance; or

3) involve particularly valuable or critical test hardware, facilities or effort.

8.3.2 Initiation

The supplier should institute procedures to perform safety readiness reviews and inspections prior to the performance of any applicable operation.

8.3.3 Review and inspection

Readiness reviews and inspections should include safety review and assessment of facilities, equipment, test articles, operating, test and contingency procedures, access controls, and personnel capabilities for compliance with safety requirements.

8.3.4 Hazardous operations

Hazardous operations shall be monitored for compliance with safety requirements and procedures, and for the possible development of unforeseen hazardous situations. Where necessary, contingency and emergency plans or

procedures shall be established and verified prior to the commencement of the operation. The safety representative shall have the authority to stop any operation that does not conform to safety requirements.

8.3.5 Launch and landing site requirements

a) Launch site operations shall be subject to hazard analysis.

b) For ground operations, the analysis shall address:

1) the potential hazardous consequences of human error and procedural deficiencies;

2) the adequacy and maintenance of operational margins;

3) the potential for human exposure to hazards and hazardous effects;

4) the requirements for operator and flight crew training;

5) the adequacy of information and data provided by the flight hardware, ground support equipment (GSE), or test equipment, as appropriate, to support the performance of the operations in accordance with the applicable safety requirements.

8.3.6 GSE requirements

Ground support equipment shall be subject to hazard analysis.

Bibliography

[1] EN 13701:2001, *Space systems — Glossary of terms.*

[2] *The Oxford English Dictionary (Second edition).*

[3] NUREG-CR-2300-Volumn 1 1983, *A guide to the performance of probabilistic risk assessments for nuclear power plants.*

[4] IEC 60050:1992, *International electrotechnical vocabulary.*

[5] ISO/IEC Guide 2:1996, *Standardization and related activities. General vocabulary.*

[6] EN ISO 9000:2000, *Quality management systems — Fundamentals and vocabulary (ISO 9000:2000).*

[7] ISO/CD 14621-1, *Space systems — Electrical, electronic and electromechanical (EEE) parts -- Part 1: Part management.* 1)

[8] ISO/CD 14621-2, *Space systems — Electrical, electronic and electromechanical (EEE) parts – Part 2: Requirements.* 1)

1) To be published

ICS 49.140

Price based on 37 pages