ECSS–Q–40A

19 April 1996

Space Product Assurance

Safety

ECSS Secretariat
ESA–ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Published by: ESA Publications Division,
ESTEC, P.O. Box 299,
2200AG Noordwijk,
The Netherlands.

Price: 35 Dutch Guilders

Printed in the Netherlands

Foreword

This standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, National Space Agencies and European industry associations for the purpose of developing and maintaining common standards.

Requirements in this standard are defined in terms of what must be accomplished, rather than in terms of how to organise and perform the necessary work. This allows existing organisational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

The formulation of this standard takes into account the existing ISO 9000 family of documents.

This standard has been prepared by the ECSS Product Assurance Working Group, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Contents List

1

General

1.1 Scope

This standard defines the safety programme and the technical safety requirements that shall be implemented in order to comply with the ECSS Safety Policy as defined in ECSS–Q–00. 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 European space systems.

The ECSS safety policy is applied by implementing a deterministic safety programme, supported by probabilistic risk assessment, which may be summarised as follows:

- hazardous characteristics (system and environmental hazards) and functions with potentially hazardous failure effects are identified and progressively evaluated by iteratively performing systematic deterministic safety analyses.
- the potential hazardous consequences associated with the system hazardous characteristics and functional failures are subjected to a hazard reduction sequence whereby:
  - hazards are eliminated from the system design and operations
  - hazards are minimised and
  - hazard controls are applied and verified.
- The risks that remain after the application of a deterministic hazard elimination and reduction sequence are progressively assessed and subjected to probabilistic risk assessment, in order to:
  - show compliance with safety targets
  - support design trades;
  - identify and rank risk contributors;
  - support apportionment of project resources for risk reduction;
  - assess risk reduction progress;
  - support the safety and project decision making process (e.g. waiver approval, residual risk acceptance).
- the adequacy of the hazard and risk control measures applied are formally verified in order to support safety validation and risk acceptance.
- Safety compliance shall be assessed by the project, and safety certification shall be obtained from the relevant authorities.

1.2 Field of Application

This standard is applicable to all European 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 specific applicability of the safety programme and technical requirements defined in this standard and its supporting standards will be tailored by the customer in accordance with the project's safety criticality, and specific application. It is the supplier's responsibility to ensure that in any subcontracts placed by him the relevant requirements from this standard are applied.

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

1.3 Normative References

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

ECSS–P–001	Glossary of Terms
ECSS–M–00	Space Project Management: Policy and Principles
ECSS–M–20	Space Project Management: Project Organisation
ECSS–M–30	Space Project Management: Project Phasing and Planning
ECSS–M–40	Space Project Management: Configuration Management
ECSS–Q–00	Space Product Assurance: Policy and Principles
ECSS–Q–20	Space Product Assurance: Quality Assurance
ECSS–Q–30	Space Product Assurance: Dependability
ECSS–Q–60	Space Product Assurance: EEE Components Requirements
ECSS–Q–70	Space Product Assurance: Materials, Mechanical Parts and Processes Control
ECSS–E–10	Space Engineering: Systems

1.4 Definitions and Abbreviations

1.4.1 Definitions

For the purposes of this standard, the definitions given in ECSS–P–001 Issue 1 apply. In particular, it should be noted that the following terms have a specific definition for use in ECSS standards.

Accident

Caution Condition

Contingency Procedure

Criticality

Emergency procedure

Failure

Failure Tolerance

Hazard

Incident

Pressure Vessel

Residual Risk

Risk

Safety Assurance

The following terms and definitions are specific to this standard and shall be applied.

“Cause

When used in the context of hazard analysis, the action or condition by which a hazardous event is initiated (an initiating event). The cause may arise as the result of failure, human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).”

“Common Cause Failure

Failures of multiple items occurring from a single cause that is common to all of them.”

NUREG/CR–2300‘PRA procedures guides’, 1982

“Common Mode Failure

Failures of multiple identical items that fail in the same mode.”

NUREG/CR–2300‘PRA procedures guides’, 1982

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

“Emergency

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

“Hazardous Event

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

“Inhibit

A design feature that provides a physical interruption between an energy source and a function actuator (e.g. a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster). Two inhibits are independent if no single failure can eliminate more than one inhibit.”

“Operator Error

The failure of a operator to perform an action as required or trained.”

“Safety

ISO 8402:1994

i.e. system state where an acceptable level of risk is not exceeded with respect to fatality, injury or illness, damage to launcher hardware or launch site facilities, damage to an element of an interfacing manned flight system, the main functions of the flight system itself, pollution of the environment and damage to public or private property.”

“Safety Critical Function

A function that, if lost or degraded, or as a result of incorrect or inadvertent operation, would result in catastrophic (0_A) or critical (0_B) consequences.”

“Safety Critical Item

An item that does not comply with the applicable safety requirements for the project, or that cannot be verified as complying with those requirements.”

“Safing

The action of

- containment and/or control of emergency and warning situations;
- placing a system (or part thereof) in a predetermined safe condition.”

“Warning Condition:

A condition where potentially catastrophic and/or critical hazardous events are imminent and where pre-planned safing action is required within a limited time.”

1.4.2 Abbreviations

The following abbreviations are defined and used within this standard.

Abbreviation	Meaning
CCB	Configuration Control Board
CDR	Critical Design Review
ECSS	European Cooperation for Space Standardization
FMECA	Failure Modes Effects and Criticality Analysis
FTA	Fault Tree Analysis
GEO	Geostationary Orbit
GSE	Ground Support Equipment
LEO	Low Earth Orbit
MIP	Mandatory Inspection Point
MRB	Material Review Board
PDR	Preliminary Design Review
QR	Qualification Review
TRB	Test Review Board
VCD	Verification Control Document

2

Safety Programme

The scope and content of the safety programme is intended to 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 ECSS–M–20 and ECSS–Q–00.

a. The supplier shall apply launch site and launch vehicle safety requirements and regulations as defined in the project requirements.

b. The appropriate safety programme requirements of this standard shall be applied for the implementation of the applicable launch site and launch vehicle requirements and regulations.

Compliance with the safety requirements defined herein in no way relieves the supplier from compliance with national or international safety regulations.

2.1 Safety Organisation

Each supplier is responsible for the safety of his product. Therefore,

2.1.1

Each supplier shall appoint a safety representative in accordance with ECSS–Q–00, 3.3.1.

2.1.2

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

2.1.3

Safety shall be integrated in all project activities.

2.1.4

The safety representatives shall have established links to all affected medical boards, radiation protection committees and industrial safety organisations, as appropriate.

2.2 Safety Representative Access and Authority

2.2.1

The Safety Representative shall have the right of access to all data relevant to project safety, and shall be at liberty to report freely, and without organisational constraint on any aspect of project safety.

2.2.2

The Safety Representative shall have the delegated authority to reject any project document, or to stop any project activity which does not comply with approved safety requirements or procedures.

2.2.3

To properly control risk the Safety Representative shall have the delegated authority to

– interrupt hazardous operations and make the system under consideration safe again when it becomes clear that the operation does not comply with the measures agreed upon in the corresponding hazard report and derived approved hazardous procedure,

2.2.4

To properly control risk the Launch Site Safety Authority Representative shall have the delegated authority to

– interrupt the launch sequence at any time when it does not comply with safety forecasts before the product becomes a hazard for ground populations.

2.2.5

The supplier shall perform safety audits of his own and his subsuppliers', project activities to verify compliance with project safety policy and requirements , as part of the project audits as specified in ECSS –M–20, requirements 4.2.6 – 4.2.9, in accordance with ECSS–Q–00 3.3.3.f.

The purpose of the audit is to identify safety problem areas and fields which are not covered by specific safety requirements.

2.2.6

The customer shall be informed of the audit schedule. Right of access (ECSS–M–20, 4.2.6) shall be provided for participation by the customer in these audits, and for the customer safety audits of the supplier and his project related activities.

2.2.7

The supplier shall not permit any project report which addresses matters related to safety certification to be issued without signed approval of safety representative.

2.2.8

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

2.2.9

Safety shall be represented at Configuration Control Boards, MRB's, TRB's, and at qualification, and acceptance reviews, where safety requirements and safety critical functions and/or items are involved. Safety shall be further represented

at all medical boards or equivalent where exposure/endurance limits are defined for flight and ground crews.

2.3 Safety Risk Management

2.3.1

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

– allocation of safety requirements,

– hazard identification,

– hazard evaluation,

– hazard prevention, reduction, and control

– hazard close–out, including residual risk acceptance.

2.3.2

All hazard assessments have to consider primarily the hazard potential and categorise 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 is minimised. The probability of a hazardous event shall consequently be taken into account whenever hazard consequence severity reduction methods alone are considered insufficient, i.e. all areas of design for minimum risk, or the reliability of safety devices.

2.3.3

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

2.4 Project Phases and Safety Review Cycle

2.4.1

The supplier shall hold regular safety progress meetings with the customer and his sub-suppliers as part of the project progress meetings as specified in ECSS–M–20, clause 4.2.2 –_4.2.5. The meetings shall be attended by the relevant customer and supplier specialists and shall review the status of safety programme activities as required by this standard and the contract.

2.4.2

a. The supplier shall support safety reviews by the customer, and as necessary the launcher authority, of the project safety status as required by this standard. The customer will perform safety reviews. Safety reviews shall be performed at all levels necessary to ensure satisfactory implementation of safety programme and technical safety requirements. The customer shall chair all safety reviews at prime supplier level. A safety data package shall normally be prepared for each review.

The customer is expected to perform safety reviews in conjunction with the following milestones as outlined in ECSS–M–30. The objective of each review will be:

Mission Definition Review

2.4.3

Safety requirements and lessons learned from previous projects shall be analysed. Support shall be provided to design and operations concept trade–off. Main system level safety requirements shall be identified.

Preliminary Requirements Review

2.4.4

System level applicable hazards, hazardous conditions and events, together with safety critical aspects and safety risk of the concepts analysed, shall be identified and compared. Project system level safety requirements shall be refined.

System Requirements Review

2.4.5

Safety requirements shall be specified in sufficient detail to allow the definition of the technical solutions for the system concept selected in phase A. Results of the safety analysis shall be available in order to confirm that the recommended solution is in agreement with the project safety requirements.

Preliminary Design Review

2.4.6

Hazard controls and safety requirements shall be sufficiently defined for detailed design to commence. The design as presented shall comply with the safety requirements to the level of detail required by the review.

2.4.7

Verification methods for hazard controls shall be proposed, definition of safety requirements shall be finalised at system and at lower levels, and the required activities included in the project verification programme.

2.4.8

Safety critical items shall be identified and listed. Deviations from safety requirements shall be identified.

Critical Design Review

2.4.9

The results of the safety analyses performed on the solution obtained in the previous phase shall be 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. All changes made to technical requirements shall be assessed with respect to consequent changes to hazard controls.

2.4.10

Safety verification methods for all hazard controls shall be agreed upon and the necessary activities entered into the verification programme.

Qualification Review.

2.4.11

All design qualification activities related to safety critical and fracture critical items, and safety critical functions, as appropriate to the level of the review, shall be completed, and the applicable reports approved.

2.4.12

All safety critical items and safety critical functions shall be qualified..

Acceptance Review

2.4.13

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

2.4.14

Verification for all defined hazard control measures shall be completed and accepted. All open verification shall be recorded in the VCD at this time. Verification procedures for verifications open at time of acceptance shall be qualified, and mutually agreed upon as appropriate for later execution.

2.4.15

All safety related nonconformances, failures, waivers, and accident/incident reports shall be formally accepted and closed, or documented on an open–items list with any constraints identified

Flight Readiness Review

2.4.16

The verification control document (VCD) shall show no further open verifications. Verifications which have to be performed nominally at a later point in time , i.e. late access inspections, etc., shall be closed on the basis of an existing, documented launch organisation procedure which is to be executed by personnel who have been trained according to this procedure.

2.4.17

All open work related to safety critical items and safety critical functions shall be completed, or scheduled as part of normal pre-launch activities. All safety related nonconformances, failures, waivers, and accident/incident reports shall be formally accepted and closed.

2.4.18

All safety related flight anomalies on previously flown common designs or reflown hardware shall be resolved and closed.

Operational Readiness Review

2.4.19

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 in order to verify that the combined operation of vehicle and ground facilities does not introduce new hazards or require additional controls.

Launch Commitment meeting

2.4.20

A delta Safety Report shall be presented which documents the current safety status, including any potential effects of countdown anomalies, weather, and hardware or personnel conditions. The report shall state whether the safety status is acceptable for launch to proceed. The report shall be subject to review and formal acceptance by the customer , and the launch authority.

In Orbit Test Review

2.4.21

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

End Of Life Assessment

2.4.22

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 compliance with the applicable requirements, including any relevant international safety regulations.

2.4.23

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

– as part of the scheduled project milestone reviews

– as part of a dedicated safety review.

2.4.24

The supplier shall prepare and deliver the safety data package.

2.5 Safety Programme Plan

2.5.1

The supplier shall show how the safety programme is implemented in the safety programme plan in accordance with ECSS–Q–00 3.3.3.c and 3.3.3.d. The plan may either be included as part of an overall project product assurance plan, or as a separate safety programme subplan.

2.5.2

Safety planning shall cover the safety activities for the project phases as defined in ECSS–M–30.

The scope of safety programme activities that are typical of human space–flight programmes, and of space–flight programmes with no interface to human space–flight systems, are defined in annex A.

2.5.3

The plan shall define:

– the safety programme tasks to be implemented;

– the personnel/supplier responsible for the execution of the tasks;

– the schedule of safety programme tasks related to project milestones;
safety programme activity interfaces with project engineering and with other product assurance activities;

– (by reference to internal procedures as appropriate) how the supplier will accomplish the tasks and verify their satisfactory completion.

2.5.4

The plan shall include a description of the project safety organisation, 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 according to ECSS–M–40, and with system engineering according to ECSS–E–10 and design and other project functions and company departments.

2.5.5

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

2.5.6

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

2.5.7

The plan shall make provisions for assuring conformance to safety requirements and regulations which are applicable to any other facilities and services which are to be utilised during the course of the project.

2.6 Safety Certification

2.6.1

All projects shall certify that the flight and ground system products are safe and in compliance with the requirements of this standard as well as any applicable project specific safety requirements.

2.6.2

The certification process shall be completed prior to delivery to any party other than the purchaser.

2.6.3

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

For any given project, the customer who defines, or makes applicable, detailed technical safety requirements constitutes the safety certification authority or part thereof. It is the responsibility of the project organisation to provide to the certification authority all safety related information required to enable the statement of safety compliance to be accepted and understood.

2.7 Safety Training

Safety Training is a part of the overall training as required by ECSS–M–00 and ECSS–Q–00,3.3.2.c and 3.3.2.d.

All safety related training of any personnel working – permanently or occasionally – with products which may have hazardous properties has three major aspects:

- **general awareness briefings** on safety measures to be taken at a given location or working environment,
- **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,
- **product specific training** which focuses on the hazards related to the specific product.

2.7.1

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

2.7.2

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

2.7.3

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

2.7.4

Records of personnel having received training shall be maintained.

2.7.5

Where safety training is identified as being 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.

2.8 Accident/Incident Reporting and Investigation.

2.8.1

The supplier shall report to the customer all accidents and incidents which occur during project activities under the control of the supplier, or his subsuppliers.

The reporting format shall be standardized across the project.

2.8.2

The supplier's safety representative shall be responsible for the investigation of any reportable Incident and for supporting the customer in the investigation of accidents as directed. The supplier's safety organisation shall co-ordinate the investigation activities in co-operation with other supplier functional departments and subsuppliers as necessary.

2.8.3

The accident/incident shall remain open until closure is approved by the customer.

2.9 Safety Documentation

2.9.1

As part of the project documentation, the supplier shall maintain a safety documentation file. The file shall be kept current and shall include as a minimum:

- hazards analysis input data (e.g. design and operational data either by document reference and issue, or the document copy);
- project hazards analyses;
- supporting analyses (e.g. functional analysis, FMECA's, warning time analysis, caution and warning analysis, sneak analysis, engineering analyses, software failure analysis, human dependability analysis, procedure analyses, contingency analyses, safety studies, etc.) which are performed in support of hazard identification, and evaluation;
- technical safety requirements file;
- hazard and risk acceptance support documentation (analyses, qualification test procedures, drawings, etc.), either by document reference and issue, or the document copy);
- safety data packages (as appropriate to the project);
- risk assessment data;
- risk assessment reports;

– safety review and safety audit results;
– safety related nonconformances (including waivers) and failure documentation;
– document review tracking data;
– accident and incident data;
– safety requirements compliance data;
– verification tracking log ;
– safety problem data;
– safety lessons–learned file.

2.9.2

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.

2.9.3

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:

– the implementation of safety requirements and hazard and risk controls;
– incorporation of hazard and risk controls into the design, or the verification programme;
– completion of verification activities;
– the design and operational safety of the system;
– the validity of safety analyses performed and documented.

2.9.4

Records shall be maintained of the documents reviewed. Safety documentation shall be updated where necessary to maintain currency.

2.9.5 Safety Data Package

a. The supplier shall submit a safety data package to the reviews.

This may be a standalone 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.

Annex B can be used as a guideline for defining the contents of the safety data package.

c. The design and operational baseline which is the subject of the safety data package shall be defined by reference to the relevant documentation as defined in ECSS–M–40.

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 and/or equipment that make up the system into the safety data package that is to be presented at the safety review.

2.9.6 Safety Deviations and Waivers

a. Safety requirements which cannot be met shall be identified and a safety deviation is to be generated.

b. The deviation shall describe why the requirement cannot be met and provide sufficient analysis and rationale to support an exception to the requirement. It needs to be shown why the deviating design or operation is nevertheless safe.

c. For safety critical items where it is impossible to verify whether the requirements have been met, a deviation or waiver shall be established which outlines the intended verification programme.

d. The supplier shall identify all deviations and waivers which affect: the applicable project safety requirements. These deviations and waivers shall be reviewed by the project safety representative to ensure that possible impacts on safety are fully analysed and that adequate justification for any deviation, which is considered to be acceptable by the supplier, is provided.

e. The accumulated deviations and waivers which 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 which identifies all safety related deviations and waivers reviewed.

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

Safety deviations and waivers are subject to safety certification authority approval, including launcher authority, as appropriate.

2.9.7 Verification Control Document

a. A verification control document (VCD) shall be maintained in which the completion steps associated with hazard report verification items are clearly stated.

Once the hazard reports have documented the verification methods to mutual satisfaction of project and certification bodies, the verification tracking log establishes the validation record.

2.9.8 Lessons–Learned File

a. The supplier shall collect the safety lessons learned during the project as called for by ECSS–Q–00 and ECSS–M–20, clause 5.1.2. The supplier shall make sure that the lessons learned are used during the project, as far as they are relevant.

b. Safety Lessons Learned shall address as a minimum

- the impact of newly imposed requirements,
- assessment of all malfunctions, accidents, anomalies, deviations and waivers,
- effectiveness of safety strategies of the project,
- new safety tools and methods which have been developed and/or demonstrated,
- effective versus ineffective verifications which have been performed,
- changes proposed to safety policy, strategy or technical requirements with rationale.

c. The lessons–learned file shall be made available to the customer upon request, as a minimum at the end of a project.

3

Safety Engineering

Safety is an integral part of all project product assurance and engineering activities. As such it is not a standalone activity. The quality of all safety engineering related work is based on assurance that the system is designed, qualified, manufactured, and operated in accordance with ECSS product assurance requirements as given in ECSS–Q–00, ECSS–Q–20, and ECSS–Q–30.

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

3.1 Safety Design Principles

3.1.1

The safety of human life shall be the overriding consideration during the design and operation of European space projects.

3.1.2

The major goal throughout the design phase shall be to insure inherent safety through the selection of appropriate design features. Damage control, containment and isolation of potential hazards shall be included in the design considerations.

3.1.3

The design of all products shall be such that

– the least hazardous design is chosen,
– environment compatibility in assured,
– the product is safe without relying on external services,
– failures which have been considered bring the system into a defined, operational safe mode,
– hazard detection, signalling and safing is duly considered,
– it allows for debris, fallout and impact prevention,
– it permits access to the product.

3.1.4 Hazard Elimination and Control Measures

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

Hazard Elimination.

a. 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.

Hazard Minimisation.

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

Hazard Control. Safety Devices

c. Hazards which cannot be 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.

Hazard Control. Warning Devices

d. 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, coupled with emergency controls of corrective action for operators to safe or shut down the affected subsystem.

Hazard Control. Special Procedures

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

f. Special Procedures may include emergency and contingency procedures, procedural constraints, or the application of a controlled maintenance programme. Special Procedures shall be qualified by testing, and appropriate training shall be provided for personnel.

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

h. The need for hazard detection, signalling and safing by the crew to control time–critical hazards shall be minimised and shall not be implemented if an alternative means of reduction or control of hazardous conditions is available.

i. To be allowed to use real time monitoring, hazard detection and safing systems for hazard control, the availability of sufficient crew response time shall be verified. Acceptable safing procedures are to be developed and verified and the personnel is to be trained.

3.1.5 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.

3.1.6 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 is to be defined for each project) after the loss of those services.

3.1.7 Fail Safe Design

The system, and its parts thereof, shall be designed in a such a way that failures brings the system into a 'safe state' (i.e. a state that does not lead to critical or catastrophic consequences), if this is compatible with the mission objectives.

3.1.8 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 crew and system operators to take action which may be 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 which 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 flight and ground operational phases.

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

d. Safing functions and capabilities shall be included which provide for the containment and/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 is acceptable by system re-configuration and/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 and 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 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.

3.1.9 Debris, Fallout and Impact Prevention

Space debris comprises any man-made Earth–orbiting object which is non-functional with no reasonable expectation of assuming its intended function. It thus includes non-operational spacecraft, spent rocket stages, material released during operations, and fragments generated by space system breakup due to explosions and collisions.

a. Means shall be provided to prevent the hazardous descent of debris as the result of launch vehicle stage descent, a launch abort, or the uncontrolled de-orbiting or orbital decay of spacecraft, or space system elements, which are likely to survive re-entry.

b. The creation of space debris in orbits which repeatedly intersect orbital paths used by space systems shall be avoided.

c. Normal operations shall not result in the creation of orbital space debris through the jettison or release of items, or the ejection of fragments.

d. Propellant, pressurised fluids, and stored electrical and mechanical energy which remains in orbital systems and elements at the end of mission shall be safely dissipated.

It should be ensured that released liquids do not form droplets.

e. Space systems and space system elements, including launch vehicle stages, in orbits with a perigee altitude below 2000 km shall remain in orbit for no longer than 25 years after completion of the operational mission. The post-operational orbital lifetime of space systems and space system elements, including launch vehicle stages, in orbits with a perigee altitude below 2000 km shall be limited to 25 years. This can be achieved by deorbiting immediately after mission completion, or transfer to an orbit with a maximum orbital lifetime of 25 years. The end-of-life manoeuvrability shall be established in accordance with launch and mission operations authority rules and regulations.

f. At the end of operational life, geostationary spacecraft shall be placed in a disposal orbit which has a perigee at least 300 km above the geostationary orbit.

g. If separation of the ABM from a geostationary satellite is necessary, separation shall occur in a super-synchronous orbit with a perigee at least 300 km above the geostationary orbit.

h. Upper stages used to transfer geostationary spacecraft from geostationary transfer orbit to geostationary orbit shall, on completion of the mission, be inserted into a disposal orbit which has a perigee at least 300 km above the geostationary orbit.

i. Launch vehicle sub-orbital stages shall be equipped with tracking aids to permit monitoring of trajectories and prediction of impact points.

j. Launch vehicle stages shall be equipped with a remotely commandable engine shut-off and/or stage destruction capability, as appropriate, in order to prevent the descent of stages and/or stage debris outside pre-defined safety limits.

k. The design of orbital stages shall support the capability of being safely de-orbited or moved to a disposal orbit, as appropriate.

l. Launch vehicles shall be designed to be insensitive to lightning strike when on the launch pad and during atmospheric flight.

m. The design shall prevent re-contact or impact of separated spacecraft or launch vehicle stages due to cold thrusting, tumbling, or attitude changes.

3.1.10 Access

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

3.2 Safety Risk Reduction and Control

3.2.1 Severity

The severity of identified hazardous events shall be categorised as follows as lined out in ECSS–M–00, clause 6.3.

Severity	Consequence
Catastrophic Hazards:	–loss of life, life threatening or permanently disabling injury or occupational illness loss of an element of an interfacing manned flight system –loss of launch site facilities –long term detrimental environmental effects.
Critical Hazards:	–temporarily disabling but not life threatening injury, or temporary occupational illness; –loss of, or major damage to flight systems, major flight system elements, or ground facilities; –loss of, or major damage to public or private property; or –short term detrimental environmental effects.

The availability of:

- design features which reduce the probability of a hazardous event occurring, but which do not affect its severity;
- warning devices, crew safe haven, or crew escape capabilities, cannot be used as rationale for the reduction of the hazard level.

a. For projects which are launched by other agencies or launch authorities, the severity categories defined by those agencies or launch authorities shall apply during the applicable operational phases.

b. For co-operative programmes a coherent set of consequence severity shall be established for joint operational phases. These categories shall not violate the ECSS policy of prioritisation for the protection of human life, nor the principles of categorisation in accordance with the definition of consequence severity categories in ECSS–M–00.

Consequence severities classify hazards according to their impact on human life. This impact may 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. It is considered to be especially important to consider detrimental environmental effects form the point of view of long term hazardous consequences to the global public.

In space flight, the environment concerned may be outer space, including the Moon and the planets, the GEO/LEO orbits as well as the Earth's atmosphere. Careful system analysis studies are recommended as preventive means of technology consequence assessments with respect to all human environments.

c. The expert assessment on where to draw the line between exposures which do not create a hazard, and those which create critical hazards and those which create catastrophic hazards shall be performed by the responsible authority (e.g. medical board, radiation protection committee, etc.) early in the design phase.

Safety engineering is responsible for relating allowed exposure levels (e.g. maximum allowable concentrations, maximum emission concentrations, radiation doses, etc.) into detailed safety requirements and measures.

3.2.2 Failure Tolerance Requirements

Failure tolerance is one of the basic safety requirements that is used to control hazards.

a. The product shall tolerate a minimum number of credible failures determined by the hazard level. This criterion applies when the loss of a function or the inadvertent occurrence of a function results in a hazardous event.

b. Failure tolerance shall be incorporated whenever failure effects can lead to catastrophic or critical hazards.

In accordance with ECSS–Q–30, the design of the system shall meet the following failure tolerance requirements;

c. No single failure or operator error shall have critical or catastrophic consequences.

d. No combination of
   two failures,
   two operator errors
   one failure and one operator error
   shall have catastrophic consequences.

e. All hazards which are not controlled by compliance to failure tolerance shall be controlled by compliance to “design to minimum risk”.

f. Technical requirements for areas of design for minimum risk have to be identified and approved by the customer and agreed by the relevant safety certification authorities.

Software

g. The required failure tolerance for software which supports a safety critical function shall be implemented utilising dissimilar methods and algorithms (diversity), unless the software is capable of being modified and validated within the time from the occurrence of the software failure to the hazardous consequence. Alternatively, independent hardware back-up to the software function may be provided.

Payload Interface

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

Redundancy Separation

i. The system design shall 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 crew notification in the case of failure detection, redundancy switch-over, or loss of operational redundancy.

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

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

l. 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 will not result in the loss of alternative, or redundant paths.

Failure Propagation

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

3.2.3 Design to Minimum Risk

a. Hazards related to “Design for minimum risk” areas of design (e.g. mechanisms, structures, pressure vessels, pressurised lines and fittings, pyrotechnic devices, material compatibility, material flammability, etc.) shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety. The failure tolerance requirements are only to be applied to these designs as necessary to ensure that credible failures that may affect the design do not invalidate their safety related properties.

Fracture Control

b. 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 fracture control principles.

Safety Factors

c. Structural safety factors shall be defined and applied to limit loads.

d. When margins of safety are determined the worst expected combination of environmental conditions shall be considered.

Materials

e. Materials shall be selected and controlled in accordance with ECSS–Q–70. 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, 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 standard.

3.2.4 Probabilistic Safety Targets

Probabilistic safety targets should be established by the customer for hazardous consequences at system level that are catastrophic.

In establishing the above–mentioned targets, compliance 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:

- 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 crew members could be compared to the one for test pilots, risk for ground personnel should be compared to the one for industrial workers);
- 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 nuclear power plants, chemical plants, as appropriate).

The assessment of compliance with the safety targets should also be used to:

- identify and rank major risk contributors;
- support the decision making process for those cases where noncompliances with the qualitative requirements are identified.

a. 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 standard.

Additionally, note that the allocation of 'targets' to the various functions and subsystems is addressed in clause 4.1. The compliance with the quantitative requirements is performed through risk analysis (see sub–clause 4.2.12).

3.3 Identification and Control of Safety Critical Functions

3.3.1

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

This includes, but is not limited to, series of operational events which may result in a hazard if they occur inadvertently or are operated out of order.

3.3.2

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

– two independent inhibits, if it induces level 0B (critical) consequences;

– three independent inhibits, if it induces level 0A (catastrophic) consequences.

3.3.3

The system shall provide;

– failure tolerance and redundancy status information of safety critical functions;

– the status of, at least, two inhibits on functions that if inadvertently operated could lead to catastrophic consequences to the flight and ground crew, including notification in real time in case of failure detection, announcement of any loss of operational redundancy, notification of redundancy switch-over, or change of inhibit status.

3.3.4

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

3.3.5

EEE components used to support safety critical functions in flight standard hardware shall be selected and procured in accordance with the applicable requirements of ECSS–Q–60.

4

Safety Analysis Requirements and Techniques

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

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

- the design, including the technology selected, the physical arrangement of elements, subsystems and equipment;
- the operating modes;
- the operating environment; and
- the hazardous effects which may result from the failure of functions.

b. Safety analyses shall be initiated early in the design phase and shall also provide concurrent support to project engineering in the selection of the least hazardous design and operational options which are compatible with the project mission and programmatic constraints.

c. 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.

d. Analysis shall always be made with reference to a defined configuration baseline as defined by ECSS–M–40.

4.1 Assessment and Allocation of Requirements

4.1.1

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

4.1.2

The supplier shall also identify additional safety requirements through:

– use of lessons learned from previous projects;

– safety analyses performed during the project.

4.1.3

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.

4.1.4

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.

4.1.5

The supplier shall submit a justification of the proposed allocation of safety requirements to the customer at the latest at the end of the phase B 'detailed definition phase'.

4.1.6

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

4.2 Safety Analysis

4.2.1

Safety analyses 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.

Mission Analysis Phase

4.2.2

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.

Feasibility Phase

4.2.3

Safety analysis shall support trade–off's in arriving at the concept which intrinsically has the lowest safety risk considering the project and mission constraints. The analysis shall concentrate on eliminating or minimising the hazards by supporting the selection of the design technology and operational concept to be implemented, and by supporting the selection of the safest system architecture.

Preliminary Definition Phase

4.2.4

The Safety analysis shall support a continued and more detailed safety optimisation 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, and the identification of significant risk contributors in the design and in the operational concept.

Detailed definition, Production and Qualification Phase

4.2.5

Safety analysis shall support detailed design and operational safety optimisation, safety requirements implementation evaluation, risk reduction verification, and – hazard and risk acceptance. Analysis of operational safety shall also support the

identification of emergency and contingency response planning and training requirements, and the development of procedures.

Utilisation Phase.

4.2.6

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

Disposal Phase

4.2.7

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.

Safety analysis consists of a combination of all the analyses described in the rest of this clause.

4.2.8

The types of analyses which have 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.

Supporting analysis is described in clause 4.3.

4.2.9 Deterministic Hazard Analysis

a. Deterministic 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:
   - hazards associated with system design, its operation and the operation environment;
   - the hazardous effects resulting from the physical and functional propagation of initiator events;
   - the hazardous events resulting from the failure of system functions, and functional components;
   - time critical situations.

c. The following potential initiator events shall be considered:
   - hardware failure (random or time dependent);
   - latent software error
   - operator error;
   - design inadequacies, including:
     * inadequate margins;
     * unintended operating modes caused by sneak-circuits;
     * material inadequacies and incompatibilities;
     * hardware/software interactions;
   - natural and induced environmental effects;
   - procedural deficiencies.

This includes a systematic analysis of the “system” operations and operating procedures which is performed in the detailed design and operational stages of a project in order to evaluate the capability of the system to be operated safely, to deter-

mine the safest operating modes, and to evaluate the acceptability of the operating procedures. The analysis is repeated as the design and operational detail evolves, particular attention being paid to the system's operational modes and man/machine interfaces.

4.2.10 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 which have been identified in the hazard analysis, and to support the implementation of hazardous–situation detection and warning devices and/or contingency procedures.

b. The analysis shall determine:

- the time during which the event shall be detected and the response action taken;
- the detection capability of the proposed design with respect to detection sensitivity and detection time;
- the resultant time available for response,
- the adequacy of the proposed design and/or contingency procedures, including emergency evacuation, rescue, system re-configuration, redundancy switching, and maintenance.

c. The detection times to be determined shall be:

- from the occurrence of the initiating event to the time when a hazardous consequence occurs (propagation time);
- the time from the occurrence of the initiating event to the time of earliest detection and/or annunciation; and
- the time taken for corrective action to be implemented.

4.2.11 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: emergency, warning, and caution parameters; the required safing functions and capabilities; limit sensing requirements; and the applicability of the individual 'caution and warning' functions to the different mission phases.

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

4.2.12 Probabilistic Safety Risk Assessment

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

b. Risk assessment shall be used to:

- support design trades (risk comparison);
- rank risk contributors;
- identify major risk contributors;
- support the safety decision making process (e.g. for waivers,unresolved residual risks, etc.);
- monitor the effectivity of the hazard control and risk–reducing process by assessing safety risk trends;
- assess compliance with probabilistic safety targets.

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

d. Sources of data used for risk assessment shall be identified and rational shall be provided by the supplier.

4.2.13 Common Cause and Common Failure Mode Analysis.

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

b. The supplier shall identify the need 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 (e.g. FTA; Hazard Analysis) and of the characteristic of the system and of its environment.

c. The supplier shall identify potential 'common cause failures' by assessment of the effects of 'common causes' (e.g. radiation, thermal environment, fire). This analysis shall be performed in co-ordination with the FTA and the Hazard Analysis. The analysis of common cause failures may require that use be made of the result of dedicated engineering analyses (e.g. thermal analyses, meteorite/debris impact analysis, etc.).

d. Common mode failures shall be analysed by means of use of checklists (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 FMECA.

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 (FTA, hazard analysis)

4.2.14 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. It is necessary to perform a fault–tree analysis or its equivalent in order to verify the failure tolerance of the product.

4.3 Supporting Assessment and Analysis

The assessment tools and analysis methods introduced in this clause are not specifically safety oriented. Refer also to ECSS–Q–30. It is the purpose of this clause to address which analyses can contribute to safety assessment, and how.

4.3.1 Human Dependability Analysis

a. Whenever safety analyses identify human errors as a cause of catastrophic or critical hazards, a dedicated human dependability analysis shall 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.

4.3.2 FMECA.

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 to be complementary analyses.

4.3.3 Sneak Analysis

a. During design and development phases, functions the failure of which would result in catastrophic consequences, emergency, warning and dedicated safing sub-functions, and crew escape and rescue supporting sub-functions, shall be subject to Sneak Analysis.

b. 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.

c. 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. subfunctions or items which do not comply with the applicable safety requirements, or which cannot be verified as complying with those requirements, shall be analysed;
   2. command and control subfunctions shall be included;
   3. electrical power distribution subfunctions shall be included;
   4. passive subfunctions (e.g. primary or secondary structures, passive thermal control) are excluded.

4.3.4 Safety Analysis for Hardware–Software Systems

a. 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 FTA, hazard analysis, FMECA, and sneak analysis, as appropriate.

b. 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, 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.

c. 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.

d. When the software code becomes available the supplier shall:

   - analyse for correctness and completeness;
   - verify that the software safety requirements have been properly implemented;
   - verify that the software can handle the appropriate
   - code with expected input overload conditions.

FTA, software sneak analysis, check-list based design, review methods may be used for this purpose in combination with static and dynamic analysis.

4.3.5 Zonal Analysis

Zonal analysis is a 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.

a. 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:
   - basic installation rules and space practices
   - interaction between subsystems
   - implication of human errors
   - effects of external events

(This page is intentionally left blank)

5

Safety Verification

In order to be able to assure that safety has been built into the product, a system needs to 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.

As laid out in ECSS–E–10, 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.

5.1 Tracking of Hazards

5.1.1

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.

5.1.2

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

Corresponding to the project phase, an “open” status shall, as a minimum, be indicated as:

– controls defined and agreed within the supplier’s project organisation;

– verification methods defined and agreed within the supplier’s project safety, engineering and management organisation;

– verification completed and submitted to the customer for acceptance.

5.1.3

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

5.1.4

Hazards and safety risks with catastrophic and critical consequences shall be submitted for review and formal disposition by the customer and as appropriate by the launch authority.

5.1.5

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

When procedures or processes are critical steps in controlling a hazard and the procedure and/or process results will not be independently verified by subsequent test or inspection, it is necessary to insure that the procedure/process be independently verified in real time.

5.1.6

Critical procedure/ process steps shall be identified in a hazard report as a mandatory inspection point (MIP) or as requiring independent observation.

5.2 Safety Verification Methods

Verification engineering shall select the best suited, cost effective verification methods consistent with verification requirements as documented in the hazard report. Verification planning shall commence in an integrated fashion as soon as the control method has been selected.

5.2.1

Safety verification methods are review of design, analysis, inspection and test. For all verifications, dated and signed verification reports have to be generated for tracking purposes.

5.2.2

With respect to the given design baseline the requirement is verified by comparison of the Review Of Design requirement with specification or drawing, as appropriate.

NOTE Reference to design reviews (e.g. PDR, CDR) is misleading and not acceptable in general.

5.2.3

All technical safety and engineering analysis which are performed or updated with analysis: respect to the as built configuration can be used for verification. Similarity is a special case of analysis since the basis for assessing that similarity is given 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 time of first verification.

5.2.4

Inspection: All pre-flight safety inspections shall be assessed for inclusion in the MIP list. In this case, close–out is feasible by MIP reporting or individual reporting as appropriate. Launch preparation inspections shall be entered into the appropriate launch base procedure. Then the close–out is given by the approved launch authority procedure. Late access procedures shall be the subject of training and shall be performed by qualified personnel. In-flight inspections, including tele-science inspections, shall be entered into flight procedures and operation manuals. Training for flight crew and mission operation teams is mandatory. Training consists of product specific safety briefing, product training and mission simulation, where necessary. Close–out is by safety approved procedure, documented training session and a sufficient number of simulations.

5.2.5

Tests are mandatory for all hazardous functions (end to end) and for safety critical items as identified on the corresponding safety deviation or waiver.

5.2.6

In general, the choice of verification shall be with the supplier, the approval is with the relevant safety certification authority.

5.3 Qualification of Safety Critical Functions

5.3.1

Safety critical functions shall be validated by “end-to-end” testing 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.

5.3.2

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.

5.3.3

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

5.3.4

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

5.3.5

Where full–scale testing is not possible owing to cost or technical constraints, separate equivalent safety verification testing shall be performed using technically representative hardware or models on customer approval.

5.4 Hazard Close–out Validation

5.4.1

In time for acceptance by the customer and in preparation of transfer to the launch site

– safety assurance shall validate that
– hazard close–outs performed so far by the responsible engineer are still valid,
– there have been no oversights,
– the verifications reflect the as–built/as–modified status of the hardware and
– all open verifications at this time are acceptable for transfer to the launch site and
– all open verifications have been entered into the verification tracking log, which now becomes a living document.

5.4.2

Hazards shall be considered for closure only when either:

– the hazard has been eliminated,

– the hazard has been minimised and controlled in accordance with the applicable requirement and the associated verification activities have been successfully completed,
– a deviation/waiver has been granted by the safety certification authority and a safety critical items control programme has been approved (see clause 5.6).
– Closeout of each hazard requires approval by the safety certification authority.

5.5 Residual Risk Reduction

Safety risks associated with catastrophic and critical consequences, which have been subject to the application of the hazard reduction precedence, are designated as residual risks.

5.5.1

Risk reduction shall be applied – either in parallel with or in sequence to hazard reduction – to reduce the residual risk to a level that is compliant with the quantitative safety target.

5.6 Safety Critical Items Control

5.6.1

Items or procedures that do not comply with the applicable safety requirements, or which cannot be verified as complying with those requirements, shall be identified as safety critical items.

5.6.2

The safety critical items list shall identify each safety critical item, an associated safety critical function, if applicable, and the item's critical performance characteristics.

5.6.3

Safety critical Items shall be ranked for criticality using criteria which shall be defined by the supplier and approved by the customer. The programme shall be subject to approval.

5.6.4

The critical items control programme shall ensure that:

– All design, manufacturing, and testing documentation which is related to safety critical items is identified and marked, and that document traceability is maintained by document number and issue;
– Safety is represented on material review boards (MRB), configuration control boards), and test review boards (TRB) which involve safety critical items;
– The qualification status of all safety critical items, together with the safety critical functions which they support, is tracked;
– safety critical functions, items and procedures are qualified
– Assembly, maintenance, servicing, testing and operation of safety critical items and procedures are monitored for problems which may affect critical characteristics.

5.6.5

The safety critical items list and control programme shall be coordinated and integrated with the project critical items list and control programme in accordance with ECSS–Q–20. The safety critical items control programme shall be implemented during the design and development, and operational phases of the project. The safety critical items list shall be issued to support design and safety reviews.

6

Operational Safety

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

a. Safety involvement in the operational phase shall therefore be planned in advance.

b. Responsibilities, rules and contingency procedures shall be established prior to operation for hazardous ”limit” conditions which may occur during ground and in-flight operations.

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

d. The design shall 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 scoped, to minimise the potential for hazardous events resulting from human error.

f. Limits for 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.

6.1 Flight Operations and Mission Control

6.1.1

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.

6.1.2

Normal or abort operations shall not result in contamination of the Earth’s atmosphere which endangers human health, crops, natural resources, or the environment.

6.1.3 Hazardous Operations Control

Flight rules shall be prepared for each mission that outline preplanned decisions designed to minimise the amount of real-time rationalisation 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.

6.1.4 Hazardous Commanding Control

a. All hazardous commands shall be identified.

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

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

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

d. Payload commands which can result in catastrophic or critical hazardous consequences shall be authorised and verified by the mission control centre.

e. Mission control equipment shall be designed to accepted ergonomic principles, including consideration of operator stress reduction factors, and lessons learned from operator experience.

f. Mission control shall have personnel who provide real–time mission technical support such as: anomaly investigation, data evaluation, data searches, contingency support and procedure development, etc.

6.1.5 Mission Operation Change Control

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

b. Changes shall be grouped and processed according to the timeframe in which implementation is foreseen and the complexity of the change itself.

c. Ad-hoc real-time changes – change notes – shall be limited to a small number of individual procedural steps. No change notes with safety impact shall be allowed.

d. All changes – operational change requests – with new or extensively modified procedures, unverified and procedures for which personnel have not been trained shall be reviewed for safety impact – new hazards, impact to existing hazards, causes, controls and verifications.

e. All operational change requests with safety impact have to be negotiated by mission operations with the responsible safety certification authorities.

f. All long term replanning of the operational timeline shall be reviewed against safety constraints before replan request approval.

6.1.6 Safety Surveillance and Anomaly Control

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

Safety status parameters are all those parameters that make it possible to assess the status of the implemented safety inhibits and hazard controls.

b. These safety parameters, if any, shall be monitored at appropriate intervals. If the mission operations safety representative concludes that the product is operating in a hazardous state, the appropriate safing procedure shall be executed.

c. All mission anomalies shall be assessed for safety impact. Anomalies shall be continuously monitored.

6.1.7 Hazardous Debris, Fallout and Impact Control

a. In the case of a deviation from the planned launch trajectory during ascent, launch–vehicle stages shall be remotely destroyed and/or have their propulsion engines shut off, as appropriate, to prevent stages and/or debris from falling outside pre-defined safe areas.

b. The launch vehicle and spent stage trajectories shall be continuously monitored to determine vehicle, stage or debris impact points.

c. Residual propellants contained in spent or aborted suborbital stages shall be safely dispersed.

6.2 Ground Operations

The following requirements are applicable to: development, qualification and acceptance testing; assembly, integration and test operations; launch site operations; servicing and turn–around operations; and transportation and handling operations that:

- are potentially hazardous to personnel or project hardware, or
- have high risks in terms of programme importance, or
- involve particularly valuable or critical test hardware, facilities or effort.

6.2.1

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

6.2.2

Readiness reviews and inspections shall 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. These reviews and inspections shall be included in the supplier's mandatory inspection programme and shall be part of the test readiness review.

6.2.3

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 procedures shall be established and verified prior to the commencement of the operation. Safety personnel shall have the authority to stop any operation which does not comply with safety requirements.

6.2.4 Launch and Landing Site Requirements

a. Launch site and launch vehicle safety requirements shall apply during the applicable operational phases.

b. Project and carrier exposure to increased risk as a result of ground or flight operations which place the flight system in a configuration of increased hazard potential shall be accomplished as late as practical in the processing flow.

Launch, landing, turn-around, and mission operations shall be subject to hazards analysis.

c. For ground operations, the analysis shall address:

- the potential hazardous consequences of human error and procedural deficiencies;
- the adequacy and maintenance of operational margins;
- the potential for human exposure to hazards and hazardous effects;
- the needs for operator and flight crew training;

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

6.2.5 GSE requirements (Servicing GSE, Check–out and Test GSE, Handling and Transportation GSE, Umbilicals, Auxiliary)

a. Ground support equipment shall include design features to prevent hazardous events occurring as a result of facility failure or malfunction.

b. Ground support equipment used during checkout and pre-launch operations of human space flight systems shall be equipped to interface with the flight system emergency, warning and caution function and shall be capable of displaying and announcing the relevant signals, and initiating appropriate saf-ing commands.

Annex A (normative)

Safety Programme Tasks

A.1 Mission Analysis/ Needs Identification Phase 0

The following tasks apply to human space flight space programmes:

a. Analyse safety requirements and lessons learned associated with similar previous missions

b. Perform preliminary hazard analysis of the proposed system and operations concept to support concept trades

c. Perform comparative safety risk assessment of the concept options

d. Identify the main project safety requirements

e. Plan safety activities for the feasibility phase

f. Support the Mission Definitions Review

For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the Mission analysis phase:

Tasks a, b, d, e and f are only applicable for design and operational aspects related to launch site and launch vehicle safety, loss of the system, and for the prevention of debris creation during the mission.

Task c is not applicable.

A.2 Feasibility Phase – Phase A

The following tasks apply to human space flight space programmes:

a. Commence hazard analyses of the design and operations concepts in order to identify applicable system level hazards, hazardous conditions, and potential hazardous events and consequences;

b. Support concept trades by identifying safety critical aspects of the concept options;

c. Apply hazard elimination and minimisation and make safety recommendations;

d. Perform comparative risk assessments of the concept options;

e. Identify system level safety critical functions;

f. Identify system level project specific safety requirements;

g. Plan safety activities for the project definition phase;

h. Support the preliminary requirements review.

For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the conceptual phase:

Tasks a, b, c, e, f, g and h are only applicable for design and operational aspects related to launch site and launch vehicle safety, loss of the system, and for the prevention of debris creation during the mission.

Task d is not applicable.

A.3 Preliminary Definition Phase – Phase B

The following tasks apply to human space flight space programmes:

a. Update hazard analysis in support of design and mission concept definition activities, in order to optimise design and operational safety by the application of the hazard and risk reduction precedence, and in order to identify additional project specific safety requirements;

b. Update safety critical functions identification, and define the specifically applicable failure tolerance requirements;

c. Identify emergency, warning, and caution situations;

d. Update the system risk assessment;

e. Identify project safety requirements;

f. Ensure that project requirement documentation and activities comply with project safety requirements;

g. Support a system requirements review;

h. Plan verification of safety requirements implementation;

i. Prepare the safety plan for the detailed definition, production and qualification phase.

For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the definition phase:

Tasks a, b, f, g, h and i are only applicable for design and operational aspects related to launch site and launch vehicle safety, loss of system, and for the prevention of debris creation during the mission.

Tasks c and d are not applicable.

A.4 Detailed Definition, Production And Qualification Phase – Phase C/D

The following tasks apply to human space flight space programmes:

a. Perform detailed system level hazard analysis;

b. Perform supporting safety analysis;

c. Update the project technical safety requirements as necessary to incorporate the results of safety analyses;

d. Ensure that identified hazard control verification activities (reviews, inspections, analyses and tests etc.) are covered by the project implementation and verification programme;

e. Update safety critical functions identification, failure tolerance requirements, and identify safety critical items;

f. Implement control programme for safety critical items;

g. Perform safety risk assessment in support of design optimisation, project resource apportionment, control programme for safety critical items and project reviews;

h. Monitor verification of safety requirements implementation;

i. Verify and document hazard control implementation;

j. Perform project internal safety reviews and internal audits;

k. Identify, monitor and control project assembly, integration, testing and handling operations which are potentially hazardous to personnel and/or hardware;

l. Review and approve hazardous and safety critical operational procedures;

m. Perform accident/incident reporting and investigation;

n. Support customer safety reviews at major programme milestones;

o. Prepare a project safety ”lessons learned” report;

p. Prepare operational phase safety plan.

For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the development and flight hardware phase:

Tasks a, b, c, d, f, h, i, n and r are only applicable for design and operational aspects related to launch site and launch vehicle safety, loss of system, and for the prevention of debris creation during the mission.

Tasks g is not applicable.

Tasks l, m, o, p and q are fully applicable.

A.5 Operational Phase – Phase E

The following tasks apply to human space flight space programmes:

a. Issue the operational phase safety plan;

b. Review operational procedures;

c. Approve safety critical operational procedures;

d. Identify and monitor hazardous operations;

e. Support the flight readiness review;Operational readiness review, Launch Readiness Review and In-Orbit Flight Reviews

f. Support ground and flight operations;

g. Perform safety critical items control.

h. Monitor and assess evolution of the system configuration and operations resulting from design fixes and updates;

i. Update hazard analyses and implement additional hazard controls as necessary;

j. Investigate safety related flight anomalies and trends;

k. Update safety risk assessment as necessary to support operational decisions

l. Prepare disposal phase safety plan.

For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the operational phase:

Tasks a, b, c, e, f, g, h, i, j and l are only applicable for design and operational aspects related to launch site and launch vehicle safety, loss of system, and for the prevention of debris creation during the mission.

Task k is not applicable.

A.6 Disposal Phase – Phase F

a. Perform hazard analysis with respect to the disposal operations taking into account the system configuration and the resources available at end of life in order to identify impacts on ground population and the environment.

b. Check that the disposal operation complies with international safety regulations by performing the necessary safety analysis

c. Review the procedures of the disposal operations

d. Support the end of life assessment.

(This page is intentionally left blank)

Annex B (informative)

Typical Content of a Safety Data Package

The typical content of a safety data package is indicated for each milestone review in table B–1. In the following the content of each table entry is outlined, if not already explained elsewhere in this standard.

* SYSTEM DESCRIPTION FROM SAFETY VIEWPOINT

This chapter of the Safety Data Package shall contain a description of the safety related features of the system. The level of depth of the description shall be consistent with the phase of the programme. The above description shall include, but not necessarily be limited to, the following:

* characteristics of the system functional architecture versus the applicable safety requirements (e.g. failure tolerance; emergency, warning, caution and safing;
* characteristics of the proposed layout of the system versus the applicable safety requirements (e.g. failure tolerance, prevention of failure propagation;
* description of the safety margins in the various phases of the system mission;
* compatibility of the proposed system design and operational scenario with the natural environment (e.g. meteoroids, debris, radiation) in which the system operates;
* description of the tasks required to be performed by the space system crew (where present) and ground personnel and their relation with safety;
* hazardous characteristics of the materials used,
* characteristics of the hardware and software items used to implement the emergency, warning, caution and safing functions;
* description of contingency and emergency procedures;
* description of the interfaces with the ground support equipment and related ground operations.

The above data should be supported by schematics and drawings when this is beneficial for the clarity of the description,

Traceability between the ‘system description from a safety viewpoint’ and the design and operational data contained in the project documentation shall be provided,

* SAFETY TECHNICAL REQUIREMENTS

The Safety Data Package shall contain, or refer to, specification documents generated by the supplier where the safety technical requirements are included.

* Identification of safety critical functions

The Safety Data Package shall contain the list of safety critical functions in the system.

The Safety Data Package shall contain the analyses used to identify and categorise the various system functions as safety critical or not.

* Hazard Analysis
* Warning Time Analysis
* Caution and Warning Analysis
* Safety Risk Assessment
* Fault Tree Analysis
* Design for minimum risk data
* Software Safety Analysis
* Supporting Analyses
    * Human dependability
    * Sneak analysis
* Safety critical items list
* Hazardous Ground Operations List and Procedures
* Waiver Status Log
* Accident/Incident Status Log
* Safety Review Action Items List
* Conclusion

Table B–1: Typical content of a safety data package at various milestones

SDP Contents	Phase 0	Phase A	Phase B	Phase B	Phase C	Phase D		Phase E			
	MDR	PRR	SRR	PDR	CDR	QR	AR	FRR	LRR	CR	EOM
SDP Content Description		X	X	X	X	X	X	X	X	X	X
System Description from Safety Viewpoint	X	X	X	X	X	X	X	X	X	X	X
Safety Requirements			X	X	X	X	X	X	X	X	X
Safety Analyses											
Identify Safety critical function	X	X	X	X	X	X	X	X	X	X	X
Hazard Analyses		X	X	X	X	X	X	X	X	X	X
WTA (1)				X	X	X	X	X	X	X	X
CWA (1)				X	X	X	X	X	X	X	X
Risk Assessment	X	X	X	X	X	X	X	X	X	X	X
Design to Minimum Risk Data			X	X	X	X	X	X	X	X	X
(Supporting Analyses)			X	X	X	X	X	X			
Summary Safety Data											
Safety Critical Items List				X	X	X	X	X	X	X	X
Safety Significant Operations List (Hazardous Operations)				X	X	X	X	X	X	X	X
Waiver Status Log				X	X	X	X	X	X	X	X
Accident/Incident Status Log					X	X	X	X	X	X	X
Safety Review Action Item List			X	X	X	X	X	X	X	X	X
Conclusion	X	X	X	X	X	X	X	X	X	X	X
(1) Only for MANNED SYSTEMS											

NOTE
AR = Acceptance Review
CDR = Critical Design Review
CR = Commissioning Review
CWA = Caution & Warning Analysis
EOM = End of Mission
FRR = Flight Readiness Review
LRR = Launch Readiness Review
MDR = Mission Definition Review
PDR = Preliminary Design Review
PRR = Preliminary Requirements Review
QR = Qualification Review
SDP = Safety Data Package
SRR = System Requirements Review
WTA = Warning Time Analysis