ECSS-Q-40B
17 May 2002

Space product assurance

Safety

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

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

ISSN: 1028-396X

Price: € 20

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 shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational 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 standards.

Significant changes between this version and the previous version are:

- ECSS Harmonization Task Force results implemented,
- DRDs added,
- ISO review comments incorporated.

This Standard meets or exceeds the requirements of ISO DIS 14620-1.

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 version B cancels and replaces ECSS-Q-40A.

(This page is intentionally left blank)

Contents

Figures

Tables

1

Scope

1.1 General

This Standard defines the safety programme and the technical safety requirements that are 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 system safety programme, supported by risk assessment, which can be summarized as follows:

a. hazardous characteristics (system and environmental hazards) and functions with potentially hazardous failure effects are identified and progressively evaluated by iteratively performing systematic safety analyses;

b. the potential hazardous consequences associated with the system characteristics and functional failures are subjected to a hazard reduction sequence whereby:

   1. hazards are eliminated from the system design and operations;
   2. hazards are minimized;
   3. hazard controls are applied and verified.

c. the risks that remain after the application of a hazard elimination and reduction process are progressively assessed and subjected to risk assessment, in order to:

   1. show compliance with safety targets;
   2. support design trade-offs;
   3. identify and rank risk contributors;
   4. support apportionment of project resources for risk reduction;
   5. assess risk reduction progress;
   6. support the safety and project decision-making process (e.g. waiver approval, residual risk acceptance).

d. the adequacy of the hazard and risk control measures applied are formally verified in order to support safety validation and risk acceptance;

e. safety compliance is assessed by the project and safety approval obtained from the relevant authorities.

1.2 Field of application

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

1.3 Tailoring

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

NOTE Tailoring is the process by which individual requirements of specifications, standards and related documents are evaluated, and made applicable to a specific programme or project by selection, and in some exceptional cases, modification of existing or addition of new requirements.
[ECSS-M-00-02A, clause 3]

2

Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. 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-00-03	Space project management — Risk management
ECSS-M-20	Space project management — Project organization
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 — Electrical, electronic and electromechanical (EEE) components
ECSS-Q-70	Space product assurance — Materials, mechanical parts and processes
ECSS-E-10	Space engineering — System engineering
ECSS-E-30-01	Space engineering — Fracture control

(This page is intentionally left blank)

3

Terms, definitions and abbreviated terms

3.1 Terms and definitions

The following terms and definitions are specific to this Standard in the sense that they are complementary or additional to those contained in ECSS-P-001.

3.1.1
accident
undesired event arising from operation of any project-specific items which results in:

a. human death or injury;

b. loss of, or damage to, hardware, software or facilities which could then affect the accomplishment of the mission;

c. loss of, or damage to, public or private property; or

d. detrimental effects on the environment.

NOTE Accident and mishap are synonymous.

[ISO 14620-1]

3.1.2
cause
that which produces an effect; that which gives rise to any action, phenomenon or condition

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

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

NOTE 3 Adapted from ECSS-P-001A, Rev.1.

3.1.3
caution condition
condition which has the potential to degrade into a warning condition, and which might require specific action, including the implementation of special procedures or restrictions on the operation of the system

[ECSS-P-001A, Rev.1]

3.1.4
common-cause failure
failure of multiple items occurring from a single cause which is common to all of them

[NUREG/CR-2300 PRA:1982]

3.1.5
common-mode failure
failure of multiple identical items that fail in the same mode

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

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

3.1.6
contingency procedure
preplanned procedure to be executed in response to a departure from specified behaviour

[ECSS-P-001A, Rev.1]

3.1.7
critical fault
fault which is assessed as likely to result in injury to persons, significant material damage, or other unacceptable consequences

[IEC 50:1992]

3.1.8
emergency
condition when potentially catastrophic or critical hazardous events have occurred, where immediate and preplanned safing action is possible and is mandatory in order to protect personnel

NOTE Adapted from ECSS-P-001A, Rev.1.

3.1.9
fail-safe
design property of an item which prevents its failures from resulting in critical faults

[IEC 50:1992]

3.1.10
failure
termination of the ability of an item to perform a required function

[IEC 50:1992]

3.1.11
fault, noun
<state> state of an item characterized by inability to perform as required, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources

NOTE 1 A fault is often the result of a failure of the item itself, but can exist without prior failure.

NOTE 2 Adapted from IEC 50:1992

3.1.12
fault, noun
<event> unplanned occurrence or defect in an item which may result in one or more failures of the item itself or of other associated equipment

[IEC 50:1992]

NOTE An item may contain a sub-element fault, which is a defect that can manifest itself only under certain circumstances. When those circumstances occur, the defect in the sub-element will cause the item to fail, resulting in an error. This error can propagate to other items causing them, in turn, to fail. After the failure occurs, the item as a whole is said to have a fault or to be in a faulty state [definition 3.1.11 above].

[ECSS-P-001A, Rev.1]

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

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

[ISO 14620-2:2000]

NOTE "Items" include human beings.

3.1.14
hazardous command
command that can remove an inhibit to a safety-critical function or activate a hazardous subsystem

3.1.15
hazardous event
occurrence leading to undesired consequences and arising from the triggering by one (or more) initiator events of one (or more) hazards

NOTE Adapted from ECSS-P-001A, Rev.1.

3.1.16
incident
unplanned event that could have been an accident but was not

[ECSS-P-001A, Rev.1]

3.1.17
inhibit
design feature that provides a physical interruption between an energy source and a function actuator

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

NOTE 1 Two inhibits are independent if no single failure can eliminate more than one inhibit.

NOTE 2 Adapted from ECSS-P-001A, Rev.1.

3.1.18
operator error
failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator

[ISO 14620-1]

3.1.19
organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

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

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

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

[ISO 9000:2000]

3.1.20
programme
coordinated set of activities, not necessarily interdependent, that continues over a period of time and is designed to accomplish broad scientific or technical goals or increased knowledge in a specific subject

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

NOTE 1 A programme can comprise several projects.

NOTE 2 A programme can last several years.

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

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

[ISO 14620-1]

3.1.21
project
unique set of coordinated activities, with definite starting and finishing points, undertaken by an individual or organization to meet specific objectives within defined schedule, cost and performance parameters

[BS 6079]

3.1.22
purchaser
customer in a contractual situation

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

3.1.23
residual risk
risk remaining in a system after completion of the hazard reduction and control process

[ECSS-P-001A, Rev.1]

3.1.24
risk
quantitative measure of the magnitude of a potential loss and the probability of incurring that loss

[ECSS-P-001A, Rev.1]

3.1.25
safe state
state that does not lead to critical or catastrophic consequences

[ISO 14620-1]

3.1.26
safety
system state where an acceptable level of risk with respect to:
- fatality,
- injury or occupational illness,
- damage to launcher hardware or launch site facilities,
- damage to an element of an interfacing manned flight system,
- the main functions of a flight system itself,
- pollution of the environment, atmosphere or outer space, and
- damage to public or private property

is not exceeded

NOTE 1 The term “safety” is defined differently in ISO/IEC Guide 2 as “freedom from unacceptable risk of harm”.

3.1.27
safety-critical function
function that, if lost or degraded, or as a result of incorrect or inadvertent operation, can result in catastrophic or critical consequences

NOTE Adapted from ECSS-P-001A, Rev.1.

3.1.28
safing
action of containment or control of emergency and warning situations or placing a system (or part thereof) in a predetermined safe condition

NOTE Adapted from ECSS-P-001A, Rev.1.

3.1.29
supplier
organization or person that provides a product

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

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

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

[ISO 9000:2000]

3.1.30
system
set of interdependent elements constituted to achieve a given objective by performing a specified function

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

[IEC 50:1992]

3.1.31
system safety
application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle

[ISO 14620-1]

3.1.32
warning condition
condition where potentially catastrophic or critical hazardous events are imminent and where preplanned safing action is required within a limited time

NOTE Adapted from ECSS-P-001A, Rev.1.

3.2 Abbreviated terms

The following abbreviated terms are defined and used within this Standard.

Abbreviation	Meaning
CCB	configuration control board
ECSS	European Cooperation for Space Standardization
EEE	electronic, electrical, electromechanical
FMECA	failure modes, effects and criticality analysis
FTA	fault tree analysis
GEO	geostationary orbit
GSE	ground support equipment
IEC	International Electrotechnical Commission
LEO	low Earth orbit
MIP	mandatory inspection point
NRB	nonconformance review board
NUREG-CR	US Nuclear Regulatory Commission contractor report
TRB	test review board
VTL	verification tracking log

4

Safety programme

4.1 Scope

a. The scope and content of the safety programme is to establish a safety management system to implement provisions of this Standard commensurate with the programme requirements.

b.

1. The system safety programme shall 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.
2. The supplier shall establish and maintain a system safety programme.
3. The supplier shall apply launch site and launch vehicle safety requirements regulations as defined in the project requirements to support efficient and effective achievement of system safety objectives.

c. The appropriate safety programme requirements of this Standard shall be applied to the implementation of the applicable launch site and launch vehicle requirements and regulations.

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

e. Tailoring shall not diminish the intent to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, and the environment from hazards associated with space systems.

4.2 Safety organization

4.2.1 General

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

4.2.2 Safety representative

Each supplier shall appoint a safety representative in accordance with ECSS-Q-00A, subclause 3.3.1 who is qualified by training or experience to perform safety functions.

4.2.3 Reporting lines

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

4.2.4 Safety integration

Safety shall be integrated in all project activities.

4.2.5 Coordination with others

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

4.3 Safety representative access and authority

4.3.1 Access

The safety representative shall have the right of access to safety-related data relevant to project safety, have unimpeded access to higher management and without organizational constraint on any aspect of project safety.

4.3.2 Delegated authority to reject – stop work

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

4.3.3 Delegated authority to interrupt operations

To properly control risk, the safety representative 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 conform to the agreed measures defined in the corresponding hazard report and derived approved hazard procedure.

4.3.4 Launch sequence

To properly control risk, the launch site safety authority representative shall have the delegated authority to interrupt the launch sequence at any time when the parameters monitored during the launch sequence deviate from the respective safety threshold or limit for these parameters and before the product becomes a hazard for ground populations.

4.3.5 Safety audits

a. The supplier shall perform safety audits of his own and his subsuppliers' project activities to verify conformance to project safety policy and requirements.

   NOTE A safety audit is an independent examination to determine whether the procedures specific to the safety requirements are implemented effectively and are suitable to achieve the specified objective.

b. The safety audits shall be part of the project audits as specified in ECSS-M-20A, subclause 4.2.6 - 4.2.9 and in accordance with ECSS-Q-00A, subclause 3.3.3.f.

c. The purpose of a safety audit shall be to identify safety problem areas and fields that are not covered by specific safety requirements.

4.3.6 Safety audit schedule and access

a. The customer shall be informed of the audit schedule.

b. Right of access shall be provided by the supplier as defined in ECSS-M-20A, subclause 4.2.6 for participation by the customer in the supplier safety audits and for the customer safety audits of the supplier and his project related activities.

4.3.7 Conformance

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

4.3.8 Approval of reports

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

4.3.9 Review

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

4.3.10 Representation on boards

a. Safety shall be represented at configuration control boards (CCBs), nonconformance review boards (NRBs), test review board (TRBs), and at qualification, and acceptance reviews, where safety requirements and safety-critical functions are involved.

b. Safety shall be further represented at all medical boards or equivalent where exposure or endurance limits are defined for flight and ground crews.

4.4 Safety risk management

4.4.1 Risks

Risk to human life, investments made, mission and environment shall be managed throughout the project by performing the following activities in accordance with ECSS-M-00-03:

a. allocation of safety requirements;

b. hazard identification;

c. hazard evaluation;

d. hazard prevention, reduction, and control;

e. hazard close out, including residual risk acceptance.

4.4.2 Hazard assessment

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

4.4.3 Preferred measures

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

4.5 Project phases and safety review cycle

4.5.1 Progress meetings

a. The supplier shall hold regular safety progress meetings with the customer and his subsuppliers as part of the project progress meetings as specified in ECSS-M-20A, subclause 4.2.2 - 4.2.5.

b. The relevant customer and supplier specialists shall attend the meetings.

c. The status of safety programme activities required by this Standard shall be reviewed.

4.5.2 Project reviews

4.5.2.1 General

a. The supplier shall support safety reviews by the customer and, as necessary, the appropriate safety approval authority of the project safety status e.g. the launcher authority.

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

c. The customer shall chair all safety reviews at prime supplier level.

d. A safety data package shall be prepared for each review.

e. Safety reviews should be performed in conjunction with the following milestones as outlined in ECSS-M-30 and the objectives as described in the respective following subclause.

4.5.2.2 Mission definition review

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

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

b. Main system level safety requirements were identified.

4.5.2.3 Preliminary requirements review

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

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

b. Project system level safety requirements were refined.

4.5.2.4 System requirements review

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

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

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

4.5.2.5 Preliminary design review

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

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

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

c. Verification methods for hazard controls were proposed.

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

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

f. Deviations from safety requirements were identified.

4.5.2.6 Critical design review

During the critical design review the supplier shall demonstrate that:

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

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

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

4.5.2.7 Qualification review

During the qualification review, the supplier shall demonstrate that:

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

b. All safety-critical functions were qualified.

4.5.2.8 Acceptance review

During the acceptance review the supplier shall demonstrate that:

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

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

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

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

4.5.2.9 Flight readiness review

During the flight readiness review the supplier shall demonstrate that:

a. The VTL (see annex C) shows no further open verifications.

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

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

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

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

4.5.2.10 Operational readiness review

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

4.5.2.11 Launch commitment meeting

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

4.5.2.12 In-orbit test review

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

4.5.2.13 End-of-life assessment

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

4.5.3 Safety programme review

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

a. as part of the scheduled project milestone reviews, or

b. as part of a dedicated safety review.

4.5.4 Safety data package

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

4.6 Safety programme plan

4.6.1 Implementation

The supplier shall show how the safety programme is implemented in the safety programme plan in accordance with ECSS-Q-00A, subclause 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 sub-plan.

4.6.2 Safety activities

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

b. The scope of safety programme tasks of human space flight programmes, and of space flight programmes with no interface to human space flight systems, is defined at annex A.

4.6.3 Definition

The plan shall define:

a. the safety programme tasks to be implemented;

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

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

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

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

4.6.4 Description

The plan shall include a description of the project safety organization, its responsibilities, and its working relationship with the reliability, maintainability, software product assurance, parts, materials and processes and quality assurance disciplines of product assurance, with configuration management according to ECSS-M-40, system engineering according to ECSS-E-10, design and other project functions and departments of organizations.

4.6.5 Safety and project engineering activities

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

4.6.6 Supplier and subsupplier premises

The plan shall describe how safety-related activities and requirements are defined for and controlled at suppliers' and subsuppliers' premises.

4.6.7 Conformance

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

4.7 Safety certification

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

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

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

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

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

4.8 Safety training

4.8.1 Overall training

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

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

1. general awareness briefings on safety measures to be taken at a given location or working environment;
2. basic technical training in the required safety techniques and skills (e.g. inspection, test, maintenance or integration), which is a prerequisite to fulfil the job function under consideration;
3. product specific training that focuses on the hazards related to the specific product.

4.8.2 Participation

Participation in the general awareness briefing shall be the precondition for all personnel accessing the area where the product is processed.

4.8.3 Basic technical training

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

4.8.4 Product specific training

All new project engineers, as well as the flight and ground crews, shall be given product specific training provided by specialists.

4.8.5 Records

Records of personnel having received training shall be maintained.

4.8.6 Identification

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

4.9 Accident-incident reporting and investigation

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

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

c. The supplier shall coordinate the investigation activities in cooperation with other supplier functional departments and subsuppliers as necessary.

d. The accident or incident investigation report shall remain open until the customer approves closure.

4.10 Safety documentation

4.10.1 General

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

b. As part of the project documentation, the supplier shall maintain a safety documentation file.

c. The safety documentation file shall be kept current and includes as applicable:

1. hazards analysis input data (e.g. design and operational data, either by document reference and issue or the document copy);
2. project hazards analyses;
3. supporting analyses and safety studies that are performed in support of hazard identification and evaluation;

EXAMPLE Functional, FMECA, warning time, caution and warning, sneak, engineering, software failure, human dependability, procedure, and contingency.

4. technical safety requirements file;
5. hazard and risk acceptance support documentation (e.g. analyses, qualification test procedures or drawings), either by document reference and issue or the document copy);
6. safety data packages (as appropriate to the project);
7. risk assessment data;
8. risk assessment reports;
9. safety review and safety audit results;
10. safety related nonconformances (including waivers) and failure documentation;
11. document review tracking data;
12. accident and incident data;
13. safety requirements conformance data;
14. verification tracking log ;
15. safety problem data;
16. safety lessons-learnt file.

4.10.2 Customer access

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

4.10.3 Supplier review

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

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

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

c. completion of verification activities;

d. the design and operational safety of the system;

e. the validity of safety analyses performed and documented.

4.10.4 Documentation

a. Records shall be maintained of the documents reviewed.

b. Safety documentation shall be updated to maintain currency.

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

4.10.5 Safety data package

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

b. The safety approval authority shall specify the content of the safety data package.

NOTE If the safety authority has not defined the content of the safety data package differently, the DRD at Annex D should be used.

c. The design and operational baseline that is the subject of the safety data package shall be defined by the actual configuration baseline as defined by 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 or equipment that makes up the system into the safety data package that is presented at the review.

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

4.10.6 Safety deviations and waivers

4.10.6.1 Request for deviation

Safety requirements that cannot be met shall be identified and a request for deviation or waiver shall be generated according to the requirements of ECSS-M-40.

4.10.6.2 Description, analysis and rationale

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

4.10.6.3 Identification and review

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

4.10.6.4 Assessment of deviation

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

4.10.6.5 Review and disposition

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

4.10.6.6 Certification authority approval

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

4.10.7 Verification tracking log

A verification tracking log shall be maintained in accordance with the document requirements definition (DRD), described in annex C, in which the completion steps associated with hazard control verification items are clearly stated. Once the verification methods have been documented in the hazard reports to mutual satisfaction of project and safety approval authorities, the verification tracking log establishes the verification record.

4.10.8 Lessons-learnt file

a. The supplier shall collect the safety lessons-learnt during the project as called for in ECSS-Q-00 and ECSS-M-20A, subclause 5.1.2. The supplier shall make sure that the lessons-learnt are used during the project, as far as they are relevant.

b. Safety lessons-learnt should consider as a minimum:

   1. the impact of newly imposed requirements;
   2. assessment of all malfunctions, accidents, anomalies, deviations and waivers;
   3. effectiveness of safety strategies of the project;
   4. new safety tools and methods that have been developed or demonstrated;
   5. effective versus ineffective verifications that have been performed;
   6. changes proposed to safety policy, strategy or technical requirements with rationale.

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

(This page is intentionally left blank)

5

Safety engineering

5.1 Safety engineering policy

5.1.1 General

Safety is an integral part of all project product assurance and engineering activities. It shall not be a stand-alone activity. The quality of all safety engineering related work shall be based on assurance that the system is designed, qualified, manufactured, and operated in accordance with ECSS product assurance requirements as given in ECSS-Q-00, ECSS-Q-20 and ECSS-Q-30.

5.1.2 Elements

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

5.1.3 Lessons-learnt

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

5.2 Safety design principles

5.2.1 Human life consideration

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

5.2.2 Design selection

The objective throughout the design phase shall be to ensure inherent safety through the selection of appropriate design features. Damage control, containment and isolation of potential hazards shall be considered in the design.

5.2.3 Hazard reduction precedence

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

a. Hazard elimination

   Hazards and hazardous conditions shall, consistent with the project constraints and mission objectives, be eliminated from the design and oper-

ational concepts by the selection of design technology, architecture and operational characteristics.

b. Hazard minimization

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

c. Hazard control – Safety devices

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

d. Hazard control – Warning devices

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

e. Hazard control – Special procedures

1. When it is not possible to reduce the magnitude of a hazard through the design, the use of safety devices or the use of warning devices, special procedures shall be developed to control the hazardous conditions for the enhancement of safety.
2. Special procedures can include emergency and contingency procedures, procedural constraints, or the application of a controlled maintenance programme.
3. Special procedures shall be verified by test and appropriate training shall be provided for personnel.
4. The requirement for hazard detection, signalling and safing by the flight crew to control time-critical hazards shall be minimized and shall not be implemented if an alternative means of reduction or control of hazardous conditions can be used.
5. To permit the use of real time monitoring, hazard detection and safing systems for hazard control, the availability of sufficient crew response time shall be verified. Acceptable safing procedures shall be developed and verified and the personnel trained.
6. Physical barriers, safe separation distances, minimal personnel allowance with access control, remote monitoring, tagout/lockout methods, and time-limited exposure shall be considered as means of hazard mitigation and risk reduction.
7. Special procedures are the least effective of the hazard control and risk reduction measures available.

5.2.4 Environmental compatibility

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

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

5.2.5 Safe without services

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

5.2.6 Fail-safe design

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

5.2.7 Hazard detection – signalling and safing

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

b. The system design shall provide the capability for detecting failures that result in degradation of failure tolerance with respect to the hazard detection, signalling and safing function. 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 that provide for the containment or control of emergency, warning and caution situations.

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

f. Dedicated safing functions shall be provided for emergency situations. Control of warning and caution situations shall be acceptable by system reconfiguration 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 – see subclause 5.3.2.

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

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

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

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

5.2.8 Debris, fallout and impact prevention

a. Space debris comprises any man-made Earth-orbiting object that is non-functional with no reasonable expectation of assuming its intended function. It includes for example non-operational spacecraft, spent rocket

stages, material released during operations, and fragments generated by space system breakup due to explosions and collisions.

b. 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.

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

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

e. Propellant, pressurized fluids, and stored electrical and mechanical energy that 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.

f. Space systems and space system elements, including launch vehicle stages, in orbits with a perigee altitude below 2 000 km shall remain in orbit for no longer than 25 years after completion of the operational mission.

g. The post-operational orbital lifetime of space systems and space system elements, including launch vehicle stages, in orbits with a perigee altitude below 2 000 km shall be limited to 25 years. This can be achieved by de-orbiting immediately after mission completion, or transfer to an orbit with a maximum orbital lifetime of 25 years.

h. The end-of-life manoeuvrability shall be established in accordance with launch and mission operations authority rules and regulations.

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

j. If separation of the apogee boost motor 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.

k. 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 that has a perigee at least 300 km above the geostationary orbit.

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

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

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

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

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

5.2.9 Access

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

5.3 Safety risk reduction and control

5.3.1 Severity

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

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

Severity		Consequence	
1)	Catastrophic hazards	i)	loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system;
		ii)	loss of launch site facilities or loss of system;
		iii)	severe detrimental environmental effects.
2)	Critical hazards	i)	temporarily disabling but not life-threatening injury, or temporary occupational illness;
		ii)	major damage to flight systems or loss or major damage to ground facilities;
		iii)	major damage to public or private property; or
		iv)	major detrimental environmental effects.
NOTE: In addition to the above two categories, other categories may be used to complete assessment of the safety risk being assumed. Two sample categories are shown in Table 2.			

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

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

b. The availability of:

1. design features which reduce the probability of a hazardous event occurring, but which do not affect its severity;
2. warning devices, crew safe haven, or crew escape capabilities

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

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

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

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

f. The expert assessment on determining limits for exposures that do not create a hazard, those that create critical hazards and those that create catastrophic hazards shall be performed by the responsible authority (e.g. medical board or radiation protection committee) early in the design phase.

g. The safety-engineering task shall relate allowed exposure levels (e.g. maximum allowable concentrations, maximum emission concentrations or radiation doses) into detailed safety requirements and measures.

5.3.2 Failure tolerance requirements

5.3.2.1 Basic requirements

Failure tolerance is one of the basic safety requirements that are used to control hazards. In accordance with ECSS-Q-30 the design of the system shall meet the following failure tolerance requirements:

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

b. No combination of

   1. two failures, or
   2. two operator errors, or
   3. one failure and one operator error

   shall have catastrophic consequences.

c. All hazards not controlled by conformance to failure tolerance shall be controlled by conformance to "design to minimum risk".

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

5.3.2.2 Software

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

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

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

5.3.2.3 Payload interface

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

5.3.2.4 Redundancy separation

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

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

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

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

5.3.2.5 Failure propagation

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

5.3.3 Design for minimum risk

5.3.3.1 General

Hazards related to the "design for minimum risk" shall be controlled by the safety-related properties and characteristics of the design. Failure tolerance requirements, as defined in 5.3.2.1, shall only be applied to the design as necessary to ensure that the credible failures that can affect the design do not invalidate safety-related properties.

NOTE Design for minimum risk is design for conformance with specific requirements that specify safety-related properties and characteristics that were baselined with the customer rather than implementing failure tolerance criteria. The failure tolerance criteria are only applied to these designs to assure that credible failures that can affect the design do not invalidate the safety-related properties of the design.

5.3.3.2 Fracture control

Where structural failure can have catastrophic or critical consequences, structures, pressure vessels, fasteners and load-bearing paths within mechanisms shall be designed in accordance with ECSS-E-30-01 Fracture control.

5.3.3.3 Safety factors

a. Structural safety factors shall be defined and applied.

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

5.3.3.4 Materials

Materials shall be selected and controlled 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 and microbiological growth) are either eliminated or controlled. If this is not feasible, the system design shall include the necessary provisions (e.g. containment of hazardous substances) to control hazardous events associated with material characteristics in accordance with the requirements of this Standard.

5.3.4 Probabilistic safety targets

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

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

   1. with respect to targets for the ground and flight personnel, the individual risk should not exceed that accepted for other professionally and comparably exposed personnel (e.g. risk for crew members should not exceed that for test pilots, risk for ground personnel should not exceed that for similarly exposed industrial workers);
   2. with respect to targets for the civil population, the total risk for the exposed ground population should not exceed that caused by other hazardous human activities (e.g. risk from overflight of commercial aircraft or chemical plants, as appropriate);
   3. the detailed project requirements on the acceptable level of risk shall be defined in the project risk management policy according to ECSS-M-00-03 and considered in the tailoring of the project specific safety requirements.

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

   1. identify and rank major risk contributors;
   2. support the decision-making process for those cases where nonconformances to the qualitative requirements are identified.

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

e. The allocation of "targets" to the various functions and subsystems is addressed in 6.2. The conformance with the quantitative requirements shall be performed through risk analysis (see 6.4.3).

5.4 Identification and control of safety-critical functions

5.4.1 Identification

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

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

5.4.2 Inadvertent operation

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

a. two independent inhibits, if it induces critical consequences, or

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

5.4.3 Provisions

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

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

b. the status of at least two inhibits on functions that, if inadvertently operated, could lead to catastrophic consequences to the flight and ground crew, including

1. notification in real time in case of failure detection,
2. announcement of any loss of operational redundancy,
3. notification of redundancy switch-over, or
4. changes of inhibit status.

5.4.4 Safe shutdown and failure tolerance requirements

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

5.4.5 Electronic, electrical, electromechanical

Electronic, electrical, electromechanical (EEE) components used to support safety-critical functions in flight standard hardware shall be selected and procured in accordance with the applicable programme requirements of ECSS-Q-60.

(This page is intentionally left blank)

6

Safety analysis requirements and techniques

6.1 General

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

b. Safety risks are the result of the hazardous characteristics associated with the:

   1. design, including the technology selected, the physical arrangement of elements, subsystems and equipment;
   2. operating modes;
   3. potential for operator error;
   4. operating environment;
   5. hazardous effects that result from the failure of functions.

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

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

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

6.2 Assessment and allocation of requirements

6.2.1 Safety requirements

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

6.2.2 Additional safety requirements

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

6.2.3 Define safety requirements – functions

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

6.2.4 Define safety requirements – subsystems

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

6.2.5 Justification

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

6.2.6 Functional and subsystem specification

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

6.3 Safety analysis

6.3.1 General

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

6.3.2 Mission analysis

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

6.3.3 Feasibility

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

6.3.4 Preliminary definition

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

6.3.5 Detailed definition, production and qualification

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

6.3.6 Utilization

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

6.3.7 Disposal

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

6.4 Specific safety analysis

6.4.1 General

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

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

6.4.2 Hazard analysis

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

b. Hazard analysis shall support the hazard reduction process.

c. Hazard analysis shall identify and evaluate:
   1. hazards associated with system design, its operation and the operation environment;
   2. the hazardous effects resulting from the physical and functional propagation of initiator events;
   3. the hazardous events resulting from the failure of system functions and functional components;
   4. time critical situations.

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

e. Hazard analysis includes a systematic analysis of the “system” operations and operating procedures that shall be performed in the detailed design and operational stages of a project.

NOTE This analysis evaluates the capability of the system to be operated safely, to determine the safest operating modes, and to evaluate the acceptability of the operating procedures.

f. The systematic analysis of system operation and operating procedures shall be repeated as the design and operational detail evolves, particular attention being paid to the system's operational modes and man-machine interfaces.

6.4.3 Safety risk assessment

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

b. Risk assessment shall be used to

1. support design trade-offs (risk comparison);
2. rank risk contributors;
3. identify major risk contributors;
4. support the safety decision-making process (e.g. for waivers and unresolved residual risks);
5. monitor the effectivity of the hazard control and risk reduction process by assessing safety risk trends;
6. assess conformance to probabilistic safety targets.

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

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

6.4.4 Safety analysis for hardware-software systems

6.4.4.1 Safety-critical function

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.

a. The scope and level of depth of the software safety analysis, identified by means of the functional failure analysis and the preliminary system level safety analyses and its performance, shall be coordinated with system fault tree analysis (FTA), hazard analysis, failure modes, effects and criticality analysis (FMECA) and sneak analysis, as appropriate.

6.4.4.2 Requirements definition phase

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

6.4.4.3 Architectural and detailed design phase

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

6.4.4.4 Software code

When the software code becomes available, the supplier shall

a. analyse for correctness and completeness;

b. verify that the software safety requirements have been implemented;

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

6.5 Supporting assessment and analysis

6.5.1 General

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

6.5.2 Warning times analysis

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

b. The analysis shall determine the

   1. time interval during which the event shall be detected and the response action taken;
   2. detection capability of the proposed design with respect to detection sensitivity and detection time;
   3. resultant time available for response;
   4. adequacy of the proposed design or contingency procedures, including emergency evacuation, rescue, system reconfiguration, redundancy switching, and maintenance.

c. The detection times shall be determined from the

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

6.5.3 Caution and warning analysis

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

   1. emergency, warning, and caution parameters;
   2. the required safing functions and capabilities;
   3. limit sensing requirements;
   4. the applicability of the individual “caution and warning” functions to the different mission phases.

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

6.5.4 Common-cause and common-mode failure analysis

6.5.4.1 Multiple failures

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

6.5.4.2 Identification of requirements and scope

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

6.5.4.3 Identification of common-cause failures

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

6.5.4.4 Analysis of common-mode failures

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

6.5.4.5 Integration of results

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

6.5.5 Fault tree analysis

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

6.5.6 Human dependability analysis

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

b. When human dependability analysis is carried out, it shall be

   1. 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;

   2. developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.

6.5.7 Failure modes, effects and criticality analysis

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

6.5.8 Sneak analysis

6.5.8.1 Applicability

a. The aim of sneak analysis is to identify “sneak circuits”, i.e. unexplained paths for a flow of mass, energy, data or logical sequence, that under certain conditions can initiate an undesired function or inhibit a desired function. Sneak circuits are not the result of failure but are latent conditions inadvertently designed into the system.

b. During design and development phases the following should be subject to sneak analysis:

1. functions whose failure would result in catastrophic consequences;
2. emergency, warning and dedicated safing sub-functions;
3. flight crew escape and rescue supporting sub-functions.

6.5.8.2 Use of results

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

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

1. sub-functions or items that do not conform to the applicable safety requirements, or which cannot be verified as conforming to those requirements, shall be analysed;
2. command and control sub-functions shall be included;
3. electrical power distribution sub-functions shall be included;
4. passive sub-functions (e.g. primary or secondary structures, passive thermal control) shall be excluded.

6.5.9 Zonal analysis

6.5.9.1 Definition

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.

6.5.9.2 Redundancy and objectives

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

a. basic installation rules and space practices;

b. interaction between subsystems;

c. implication of human errors;

d. effects of external events.

6.5.10 Energy trace analysis

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

(This page is intentionally left blank)

7

Safety verification

7.1 General

a. To assure that safety is built into the product, a system shall be in place that tracks all hazards and related risks, to relate all verifications of the corresponding hazard uniquely to unambiguous causes and controls.

b. As detailed in ECSS-E-10 test, analysis, inspection and "review of design" are common techniques for verification of design features used to control hazards. To successfully complete the safety process positive feedback shall be provided on completion results for all verification items associated with a given hazard.

7.2 Tracking of hazards

7.2.1 Hazard reporting system

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

7.2.2 Status

a. The status shall be either "open" or "closed".

b. An "open" status shall, as a minimum, be indicated as

   1. controls defined and agreed within the supplier's project organization;
   2. verification methods defined and agreed within the supplier's project safety, engineering and management organization;
   3. verification completed and submitted to the customer for review and formal disposition.

7.2.3 Safety progress meeting

Status of hazard control and risk reduction activities shall be reviewed at safety progress meetings and formally documented and submitted for customer review at project safety reviews – see subclause 4.5.

7.2.4 Review and disposition

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

7.2.5 Documentation

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

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

7.2.6 Mandatory inspection points

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

7.3 Safety verification methods

7.3.1 Verification engineering and planning

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

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

7.3.2 Methods and reports

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

7.3.3 Verification requirements

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

7.3.4 Analysis

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

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

7.3.5 Inspections

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

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

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

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

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

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

7.3.6 Tests

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

7.3.7 Verification and approval

a. The supplier shall choose the safety verification method to be used that conforms to the requirements of this Standard.

b. Before use the method selected for the safety verification should be submitted for approval to the relevant safety approval authority.

c. The results of safety verification shall be submitted for approval to the relevant safety approval authority.

7.4 Qualification of safety-critical functions

7.4.1 Validation

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

7.4.2 Qualification

The safety-critical characteristics of all safety-critical functions shall be fully qualified by test. Safety-critical function qualification testing shall include the determination of performance margins considering worst case combinations of induced and natural environments and operating conditions. Qualification "by similarity" shall not be applied except after customer approval on a case-by-case basis.

7.4.3 Failure tests

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

7.4.4 Verification of design or operational characteristics

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

7.4.5 Safety verification testing

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

7.5 Hazard close out

7.5.1 Safety assurance verification

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

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

b. there have been no oversights;

c. the verifications reflect the as-built or as-modified status of the hardware;

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

e. all open verifications have been entered into the verification tracking log;

f. the verification tracking log is maintained to reflect the current status.

7.5.2 Safety approval authority

Close out of each hazard requires approval by the safety approval authority. Hazards shall not be considered for closure unless:

a. the hazard has been eliminated, or

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

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

7.6 Residual risk reduction

a. Safety risks associated with catastrophic or critical consequences, which have been subject to the application of the hazard reduction precedence, shall be classified as residual risks.

b. Residual risk shall be compared to the acceptable risk.

c. Where the residual risk exceeds the acceptable risk additional risk reduction action shall be taken.

8

Operational safety

8.1 Basic requirements

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

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

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

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

d. The design 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 shall be scoped to minimize 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 that cover nominal, contingency, and emergency operational modes, in order to preclude crew injury or inability to perform safety-critical functions.

8.2 Flight operations and mission control

8.2.1 Launcher operations

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

8.2.2 Contamination

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

8.2.3 Flight rules

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

8.2.4 Hazardous commanding control

Hazardous commanding control shall ensure that:

a. All hazardous commands shall be identified.

b. 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 included in the safety assessment.

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

d. Payload commands, which can result in catastrophic or critical hazardous consequences, shall not be performed until they are authorized and verified.

8.2.5 Mission operation change control

Mission operation change control shall ensure that:

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

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

8.2.6 Safety surveillance and anomaly control

a. During mission operations all product parameters, which were identified in the safety review process as safety status parameters, shall be monitored.

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

8.2.7 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 or have their propulsion engines shut off to prevent stages or debris from falling outside pre-defined safe areas.

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

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

8.3 Ground operations

8.3.1 Applicability

The requirements that follow at subclause 8.3.2 to 8.3.6 shall be applicable to ground operation locations where there is or are:

a. development, qualification or acceptance testing;

b. assembly, integration or test operations;

c. launch site operations;

d. servicing or turn-around operations; and

e. transportation or handling operations,

and where those locations:

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

8.3.2 Initiation

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

8.3.3 Review and inspection

To verify conformance to safety requirements, 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 to comply with the safety requirements.

8.3.4 Hazardous operations

a. Hazardous operations shall be monitored for conforming to safety requirements and procedures, and for the possible development of unforeseen hazardous situations.

b. Where necessary, contingency and emergency plans or procedures shall be established and verified prior to the commencement of the operation.

c. The safety representative shall have the authority to stop any operation that does not conform to safety requirements.

8.3.5 Launch and landing site

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

b. For ground operations, the analysis shall address:

1. the potential hazardous consequences of human error and procedural deficiencies;
2. the adequacy and maintenance of operational margins;
3. the potential for human exposure to hazards and hazardous effects;
4. the requirements for operator and flight crew training;
5. the adequacy of information and data provided by the flight hardware, ground support equipment (GSE), or test equipment, as appropriate, to support the performance of the operations in accordance with the applicable safety requirements.

8.3.6 Ground support equipment

Ground support equipment shall be subject to hazard analysis. Any GSE used in European space projects shall conform to EC essential safety requirements of any applicable new approach directive by the the EC.

(This page is intentionally left blank)

Annex A (normative)

Safety programme task

A.1 Mission analysis or requirements identification phase - Phase 0

a. The following tasks apply to human space flight space programmes.
   1. Analyse safety requirements and lessons-learnt associated with similar previous missions;
   2. Perform preliminary hazard analysis of the proposed system and operations concept to support concept trade-offs;
   3. Perform comparative safety risk assessment of the concept options;
   4. Identify the main project safety requirements;
   5. Plan safety activities for the feasibility phase;
   6. Support the mission definitions review.

b. For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the mission analysis phase:
   1. Tasks 1., 2., 4., 5. and 6. 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.
   2. Task 3. is not applicable.

A.2 Feasibility phase - Phase A

a. The following tasks apply to human space flight space programmes.
   1. 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;
   2. Support concept trades by identifying safety critical aspects of the concept options;
   3. Apply hazard elimination and minimization and make safety recommendations;
   4. Perform comparative risk assessments of the concept options;
   5. Identify system level safety critical functions;
   6. Identify system level project specific safety requirements;
   7. Plan safety activities for the project definition phase;

8. Support the preliminary requirements review.

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

1. Tasks 1., 2., 3., 5., 6., 7. and 8. 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.
2. Task 4. is not applicable.

A.3 Preliminary definition phase - Phase B

a. The following tasks apply to human space flight space programmes.

1. Update hazard analysis in support of design and mission concept definition activities, in order to optimize design and operational safety by the application of the hazard and risk reduction precedence, and in order to identify additional project specific safety requirements;
2. Update safety critical functions identification, and defines the specifically applicable failure tolerance requirements;
3. Identify emergency, warning, and caution situations;
4. Update the system risk assessment;
5. Identify project safety requirements;
6. Ensure that project requirement documentation and activities comply with project safety requirements;
7. Support a system requirements review;
8. Plan verification of safety requirements implementation;
9. Prepare the safety plan for the detailed definition, production and qualification phase.

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

1. Tasks 1., 2., 6., 7., 8. and 9. 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.
2. Tasks 3. and 4. are not applicable.

A.4 Detailed definition, production and qualification phase - Phase C/D

a. The following tasks apply to human space flight space programmes.

1. Perform detailed system level hazard analysis;
2. Perform supporting safety analysis;
3. Update the project technical safety requirements as necessary to incorporate the results of safety analyses;
4. Ensure that the project implementation and verification programme covers identified hazard control verification activities (e.g. reviews, inspections, analyses and tests);
5. Update safety critical functions identification, failure tolerance requirements, and identifies safety critical items;
6. Implement control programme for safety critical items;
7. Perform safety risk assessment in support of design optimization, project resource apportionment, control programme for safety critical items and project reviews;
8. Monitor verification of safety requirements implementation;
9. Verify and document hazard control implementation;

10. Perform project internal safety reviews and internal audits;
11. Identify, monitor and control project assembly, integration, testing and handling operations which are potentially hazardous to personnel or hardware;
12. Review and approve hazardous and safety critical operational procedures;
13. Perform accident-incident reporting and investigation;
14. Support customer safety reviews at major programme milestones;
15. Prepare a project safety “lessons-learnt” report;
16. Prepare operational phase safety plan.

b. For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the development and flight hardware phase:
   1. Tasks 1., 3., 4., 5., 6., 8., 9., 12. and 16. 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.
   2. Task 2. and 7. is not applicable.
   3. Tasks 10., 11., 13., 14. and 15. are fully applicable.

A.5 Operational phase - Phase E

a. The following tasks apply to human space flight space programmes.
   1. Issue the operational phase safety plan;
   2. Review operational procedures;
   3. Approve safety critical operational procedures;
   4. Identify and monitor hazardous operations;
   5. Support the flight readiness review, operational readiness review, launch readiness review and in-orbit flight reviews;
   6. Support ground and flight operations;
   7. Perform safety critical items control;
   8. Monitor and assess evolution of the system configuration and operations resulting from design fixes and updates;
   9. Update hazard analyses and implement additional hazard controls as necessary;
   10. Investigate safety related flight anomalies and trends;
   11. Update safety risk assessment as necessary to support operational decisions;
   12. Prepare disposal phase safety plan.

b. For space flight programmes with no interface to human space flight systems, the following tailoring is appropriate for the operational phase:
   1. Tasks 1., 2., 3., 5., 6., 7., 8., 9., 10. and 12. 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.
   2. Task 11. 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 conforms to international safety regulations by performing the necessary safety analysis.

c. Review the procedures of the disposal operations.

d. Support the end of life assessment.

Annex B (normative)

Hazard report — Document requirements definition (DRD)

B.1 Introduction

ECSS-Q-40 requires the performance of safety analysis and the compilation of hazard reports, which present data on identified hazards, on hazard reduction efforts and on follow-on activities for tracking purposes.

B.2 Scope and applicability

This document requirements definition (DRD) establishes the data content requirements for a “hazard report”.

B.3 References

B.3.1 Normative references

This DRD uses terminology and definitions controlled by:

ECSS-P-001	Glossary of terms
ECSS-Q-40	Space product assurance — Safety

B.3.2 Source document

This DRD establishes the data content requirements for a hazard report as controlled by ECSS-Q-40 Space product assurance - Safety. In the case of specific launcher/spacecraft hazard report DRDs those provided by the launcher/spacecraft organization shall be used.

B.4 Terms, definitions and abbreviated terms

For the purpose of this DRD the terms and definitions given in ECSS-P-001 and ECSS-Q-40 apply. No abbreviated terms are used other than DRD.

B.5 Description and purpose

Each hazard report documents the results of the systematic identification, evaluation, reduction, verification and tracking of hazards. Hazard reports form part of a safety data package.

B.6 Application and interrelationships

Safety analysis is performed as required in ECSS-Q-40 Space product assurance - Safety. Hazard analysis provides the mandatory input to completing the data elements of hazard reports. Hazard reports are compiled into safety data packages

B.7 Hazard report preliminary elements

B.7.1 Title

The title of the hazard report shall identify the applicable project and shall give a top - level summary of the hazards treated in the hazard report.

Example: “Pluto Flyer project – propulsion tank explosion hazard – loss of vehicle hazard”.

B.7.2 Title page

No title page shall be provided.

B.7.3 Contents

No contents list shall be provided.

B.7.4 Foreword

No foreword shall be provided.

B.7.5 Introduction

No introduction shall be provided.

B.8 Hazard report content

B.8.1 General information

The hazard report shall identify the following general information:

- the project documentation identification number, the title of the hazard report, date of release and release authority;
- the project phase;
- identification of which organizational entity prepared the document;
- information regarding the approval of the document;
- a statement of effectivity identifying which other documents are cancelled and replaced in whole or in part;
- the applicable requirements relevant to the hazard report.

B.8.2 System information

The hazard report shall identify the system design and operational configuration and environment, e.g. flight, integration and test, and ground.

B.8.3 Hazard description

The hazard report shall identify the following information on the hazards in the system:

- types of hazards;
- detailed description of their manifestation in the system design and operational configuration and environment.

B.8.4 Hazard information

The hazard report shall identify the following information on the hazard scenarios associated with the hazard:

- description of cause and initiator events associated with the hazard manifestation;
- summary description of the physical and functional propagation from initiator events to consequence;
- propagation time from causes to consequence;
- references to hazard analysis used for the identification of the scenarios.

B.8.5 Safety risk information

The hazard report shall identify the following information on the safety risk posed by the hazards as a minimum:

- consequence severity category;
- acceptability of the residual risk related to the hazard.

The following information may be optionally provided:

- likelihood;
- magnitude of safety risk.

B.8.6 Hazard reduction information

The hazard report shall identify the following information on the hazard reduction applied:

- implementation of safety requirements;
- hazard elimination or minimization and control actions;
- safety risk reduction potential of hazard reduction;
- hazard reduction verification means;
- implementation actions of hazard reduction;
- verification actions of hazard reduction;
- safety risk trend after hazard reduction (optional).

B.8.7 Hazard status information

The hazard report shall identify the following information on the status of the hazard:

- status of actions (open, closed);
- status of hazard (resolved, unresolved: as related to project phase);
- status of nonconformances and waiver;
- approval of hazard report;
- acceptance of residual risk associated with the hazard.

B.8.8 Examples

Example forms are shown at Figure B-1 - ECSS hazard report, Figure B-2 – ECSS hazard report continuation sheet and at Figure B-3 – Hazard report.

ECSS hazard report		No.:
Product:		Phase
Subsystem:	Type of hazard:	Date:
Hazard title:		Severity: Catastrophic Critical
Applicable safety requirements:		
Description of hazard:		
Hazard causes:		
Hazard controls:		
Safety verification methods:		
Approval phase	Supplier	Safety approval authority
Phase		
Phase		
Phase		

Figure B-1: Example of ECSS hazard report

ECSS hazard report continuation sheet	No.:
Product:	Phase
Hazard causes:	
Hazard controls:	
Safety verification methods:	
Status of verification:	

Figure B-2: Example of an ECSS hazard report continuation sheet

<table>
<tr><td>Project
WBS Ref.</td><td colspan="3">Organization</td><td>Source

Produced by</td><td colspan="4">Date and issue

Approved by</td></tr>
<tr><td colspan="8">No. HAZARD and SAFETY RISK TITLE:</td></tr>
<tr><td colspan="2">System design and operation:</td><td colspan="6">Hazard scenario titles and safety analysis reference:</td></tr>
<tr><td colspan="2"></td><td colspan="6">Description of hazard scenarios:

Causes
Events
Safety consequence
Propagation time</td></tr>
<tr><td colspan="2">Safety consequence severity (S)</td><td colspan="3">Likelihood (L)</td><td>Risk index</td><td>RISK</td><td>RED *</td><td>YELLOW *</td><td>GREEN *</td></tr>
<tr><td>Negligible</td><td>Marginal</td><td>Critical</td><td>Catastrophic</td><td>Minimum</td><td>Low</td><td>Medium</td><td>High</td><td>Maximum</td><td>(R = S × L)</td><td>Safety</td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td colspan="4" rowspan="2">Numerical risk and uncertainty contribution:</td></tr>
<tr><td colspan="5">Numerical estimate:</td></tr>
<tr><td colspan="4">Accept hazard and safety risk ❑</td><td colspan="4">Reduce hazard and safety risk ❑</td></tr>
<tr><td colspan="3">Hazard reduction measures and verification means

Hazard elimination:
Hazard minimization:
Hazard control:</td><td colspan="3">Implementation and verification</td><td colspan="2">Expected safety risk reduction

Severity, likelihood, risk index:
Numerical estimates:
Safety risk rank:</td></tr>
<tr><td colspan="6">Actions</td><td colspan="2">Status</td></tr>
<tr><td colspan="6">Agreed by project management

Safety risk acceptance</td><td colspan="2">Hazard status</td></tr>
</table>

* Enter "R" in the appropriate column: ranges of values for RED, YELLOW and GREEN are defined in the project risk management policy

Figure B-3: Example of a hazard report

Annex C (normative)

Safety verification tracking log — Document requirements definition (DRD)

C.1 Introduction

ECSS-Q-40 requires the compilation of hazard reports, which present data on identified hazards and associated safety risks, on hazard and safety risk reduction efforts and on follow on activities for tracking purposes. These activities have to be successfully completed prior to the next steps like integration of the item to the next higher level or prior to delivery. The safety verification tracking log at this point collects all the open verification items of the different hazard reports from the safety data package which has to be established or updated at the end of the project phase C/D (production and qualification phase; safety phase III). It provides the summary of the current verification status and supports the subsequent integration or processing steps in the project.

C.2 Scope and applicability

This DRD establishes the data content requirements for a Safety verification tracking log.

C.3 References

C.3.1 Normative references

This DRD uses terminology and definitions controlled by:

ECSS-P-001	Glossary of terms
ECSS-Q-40	Space product assurance — Safety

C.3.2 Source document

This DRD establishes the data content requirements for a Safety Verification Tracking Log as controlled by ECSS-Q-40 Space product assurance - Safety.

C.4 Terms, definitions and abbreviated terms

For the purpose of this DRD the terms and definitions given in ECSS-P-001 and ECSS-Q-40 apply. No abbreviated terms are used other than DRD.

C.5 Description and purpose

For every safety data package a safety verification tracking log collects all the open safety verification items from the different hazard reports of the safety data package at the end of the production and qualification phase of the project. It provides managerial information of the intended verification effort and gives reference to the close out documents (e.g. test reports, analyses, and flight procedures). Depending on the number and severity of the open verification items it can be the basis for the decision to put the next processing steps (like acceptance or integration into the next higher level) into hold. The safety verification tracking log is part of the safety data package at the end of the qualification phase.

C.6 Application and interrelationships

The different safety verification tasks i.e. hardware and software changes, tests, review of design activities, analyses, inspections and development of procedures are performed as agreed per "hazard reports" of the flight safety data package and the ground safety data package (or a combination thereof) as required in ECSS-Q-40 Space product assurance - Safety. These and other more managerial information like constraints and schedule among others provide input to complete the safety verification tracking log. The safety representative in the project is also responsible for the maintenance of the safety verification tracking log.

C.7 Hazard report preliminary elements

C.7.1 Title

The title of the Safety verification tracking log as a part of a safety data package shall identify the project for which it has been established and the applicability for open items close out of flight or ground safety

EXAMPLE "Cardiolab - Safety verification tracking log Ground".

C.7.2 Title page

No title page shall be provided.

C.7.3 Contents

No contents list shall be provided.

C.7.4 Foreword

No foreword shall be provided.

C.7.5 Introduction

No introduction shall be provided.

C.8 Safety verification tracking log content

C.8.1 General information

The Safety verification tracking log shall identify the following general information:

a. the project documentation identification number;

b. applicability for flight or ground safety verifications;

c. indication of the specific page number followed by the total number of pages;

EXAMPLE "page 2 of 4".

d. name of the equipment, payload or experiment for which the safety data package has been established;

e. the mission or flight to which the equipment, payload or experiment has been manifested (if applicable);

f. dates of compilation or generation and update.

NOTE To provide a quick and reliable verification status it is recommended to use the format of a table for the compilation of the data.

C.8.2 Log number

For each verification item to be tracked a unique identifier shall be used. The safety representative assigns the designations and includes them on the safety verification tracking log included in the safety data package.

C.8.3 Hazard report number

The identification number of the hazard report containing the verification item shall be indicated.

C.8.4 Safety verification number

The verification method or the verification means shall be transferred word by word from the hazard report including the procedures by number and title.

C.8.5 Ground operations constrained

The input of "yes" or "no" indicates whether this safety verification constrains any ground operations.

a. If "yes" for flight tracking log: an attachment shall be provided that identifies which ground operation is constrained. The safety representative shall give notification to the safety review panel.

b. If "yes" for ground tracking log: the ground operation constrained by this verification shall be indicated specifically (e.g. step in a procedure) or generally (e.g. upon arrival or first use).

C.8.6 Independent verification required, "yes" or "no"

For the verification of hazard controls in catastrophic hazards where non-flight equipment replaces part of the flight equipment to test a flight function the verification has to be performed independently by a third party which was not involved in the design and qualification of the flight model.

C.8.7 Scheduled date

The planned date for the completion of the verification shall be indicated.

C.8.8 Method of closure/comments

The indication shall be given of the title and number of the tests, review of designs, inspections and analyses by which this verification is formally closed. Any appropriate information or remarks may be added.

Safety verification tracking log		Flight ❑	Ground ❑	page ___ of ___
Project ID:				
Equipment, payload, mission			Issue date	updated

Log no.	Hazard report number	Safety verification number	Safety verification method (Identify procedures by number and title)	Ground operations constrained	Independent verification required	Scheduled completion date	Completion date	Method of closure/comments (Provide reference ID)

Figure C-1: Verification tracking log

Annex D (normative)

Safety data package — Document requirements definition (DRD)

D.1 Introduction

As required by ECSS-Q-40, this document describes for each safety data package the structure and data to be documented.

D.2 Scope and applicability

D.2.1 Scope

D.2.1.1 General

This document requirements definition (DRD) establishes the data content requirements for the safety data package.

This DRD does not define format, presentation or delivery requirements for the safety data package.

D.2.1.2 Applicability

This DRD is applicable to all projects using the ECSS Standards.

D.2.2 References

D.2.2.1 Glossary and dictionary

This DRD uses terminology and definitions controlled by:

ECSS-P-001	Glossary of terms
ECSS-Q-40	Space product assurance — Safety

D.2.3 Terms, definitions and abbreviated terms

D.2.3.1 Terms and definitions

For the purposes of this DRD the terms and definitions given in ECSS-P-001 and in ECSS-Q-40 apply.

D.2.3.2 Abbreviated term

The following abbreviated term is defined and used within this DRD.

Abbreviation	Meaning
SDP	safety data package

D.3 Description and purpose

The safety data package is established for each project to document the safety analysis that has been performed by the supplier. The system description provided is sufficient to allow the reader to understand the system and its operation. The safety discussion enables the reader to understand the risk management decisions made based on the projects risk policy. The data collected in the package are a complete documentation of the systems safety as appropriate to the phase of the project the safety review is linked to.

D.4 Application and interrelationship

The document is prepared for each safety review performed.

D.5 SDP preliminary elements

D.5.1 Title

The document to be created based on this DRD shall be titled "[insert a descriptive modifier] safety data package".

The descriptive modifier shall be selected to clearly identify the applicable product and safety review phase. The modifier shall distinguish between flight and ground safety reviews.

EXAMPLE 1 Project: "Title alpha" flight safety review Phase III (safety verifications completed) – safety data package.

EXAMPLE 2 Project: "Title beta" ground safety review Phase CDR (hazard controls defined, verification methods proposed) – safety data package.

D.5.2 Title page

The title page for this document shall identify the project document identification number, title of the document, date of release and release authority.

D.5.3 Contents

The contents shall identify the title and location of every clause and major subclause, figure, table and annex contained in the document.

D.5.4 Foreword

A foreword shall be included which describes as many of the following items as are appropriate:

a. identification of which organizational entity prepared the document;

b. information regarding the approval of the document;

c. identification of other organizations that contributed to the preparation of the document;

d. a statement of effectively identifying which other documents are cancelled and replaced in whole or in part;

e. a statement of significant technical differences between this document and any previous document;

f. major changes of the safety risk policy or its implementation;

g. major system changes affecting safety.

D.5.5 Introduction

An introduction may be included to provide specific information or commentary about the technical content.

D.6 Content

D.6.1 Scope and applicability

D.6.1.1 General

This clause shall be numbered 1 and shall describe the scope, applicability and purpose of the SDP.

D.6.1.2 Scope

This subclause shall be numbered 1.1 and shall contain the following statements:

"This SDP contains the results obtained for the [insert product and SDP identifier] of the [insert project identifier] project.

This SDP is based on the requirements of the [insert project safety requirements document identifier]."

D.6.1.3 Purpose

This subclause shall be numbered 1.2 and shall contain the following statements:

"This SDP provides evidence that the safety analysis required been performed and the related safety risk reduction measures are being implemented."

D.6.2 References

D.6.2.1 General

This clause shall be numbered 2 and shall contain the following subclauses.

D.6.2.2 Normative references

This subclause shall be numbered 2.1 and shall contain the following statements:

"The following normative documents contain provisions which, through reference in this text, constitute provisions of this document. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

[insert document identifier] [insert document title]."

Typically the reference documents are as a minimum the product specification, the operations manuals, any specific safety requirements document and the safety assurance plan.

D.6.2.3 Informative references

This subclause shall be numbered 2.2 and shall contain the following statement:

"The following documents, although not a part of this SDP, amplify or clarify its contents:

[insert document identifier] [insert document title]."

D.6.3 Terms, definitions and abbreviated terms

D.6.3.1 General

This clause shall be numbered 3 and shall contain the following subclauses.

D.6.3.2 Terms and definitions

This subclause shall be numbered 3.1 and shall list any applicable project dictionary or glossary, and all unusual terms or terms with a meaning specific to the SDP with the definition for each term.

If a project dictionary or glossary is applicable, insert the following sentence:

"The definitions of [insert title and identifier of applicable dictionaries or glossaries] apply to this document."

Insert the following sentence:

"The following terms and definitions are specific to this document:

[insert term] [insert definition]."

D.6.3.3 Abbreviated terms

This subclause shall be numbered 3.2 and shall list all abbreviated terms used in the analysis report with the full meaning or phrase for each abbreviated term.

D.6.4 System description

This clause shall be numbered 4 and shall provide detailed description of the system being reviewed. The description shall be sufficiently detailed to allow an independent safety assessment by a safety specialist.

For this purpose all functional subsystem elements shall be described.

EXAMPLE Structure;
mechanics;
electronics including grounding concept, wiring and fusing;
laser;
pyrotechnics.

D.6.5 Operations description

This clause shall be numbered 5 and shall provide detailed description of the operation of the system being reviewed. The description shall be sufficiently detailed to allow an independent safety assessment by a safety specialist.

For this purpose all operational subsystem elements shall be described.

EXAMPLE Ground operations;
baseline data collection;
flight operations;
commanding;
decommissioning.

D.6.6 Safety discussion

This clause shall be numbered 6 and shall describe the basic assumptions, the analysis technique used including the software and associated models (if any) and the boundary conditions and validity of the safety analysis. It shall help to guide the reader to understand how the projects risk policy is implemented in the project. All decisions on safety issues made in the process of the safety assessment shall be documented. New analysis results shall be presented and the conclusions summarized.

D.6.7 Safety data

This clause shall be numbered 7 and shall provide all mandatory safety data.

All hazard reports shall be filed in this clause under 7.2. Generic hazard reports shall be separated from unique hazard reports. All safety related nonconformance reports and waivers shall be filed here. A copy of all documents referred to as close out documentation in the respective hazard report shall be filed either by means of a copy or by reference to another document.

(This page is intentionally left blank)

Annex E (normative)

Accident-incident report — Document requirements definition (DRD)

E.1 Introduction

As required by ECSS-Q-40, this document describes for each accident-incident report the structure and data to be documented.

E.2 Scope and applicability

E.2.1 Scope

This document requirements definition (DRD) establishes the data content requirements for the accident-incident report.

This DRD does not define format, presentation or delivery requirements for the accident-incident report.

E.2.2 Applicability

This DRD is applicable to all projects using the ECSS Standards.

E.3 References

E.3.1 Glossary and dictionary

This DRD uses terminology and definitions controlled by:

ECSS-P-001	Glossary of terms
ECSS-Q-40	Space product assurance — Safety

E.4 Terms, definitions and abbreviated terms

E.4.1 Terms and definitions

For the purposes of this DRD the terms and definitions given in ECSS-P-001 and in ECSS-Q-40 apply.

E.4.2 Abbreviated terms

The following abbreviated terms are defined and used within this DRD.

N/A

E.5 Description and purpose

As required by ECSS-Q-40 the accident-incident report is established for each project to document any mishap that has occurred.

E.6 Application and interrelationship

The document is prepared for each mishap, which has occurred, as required by ECSS-Q-40.

E.7 Accident-incident report data elements

E.7.1 Title

The document to be created based on this DRD shall be entitled "[insert a descriptive modifier] Accident-incident report".

The descriptive modifier shall be selected to clearly identify the applicable product and phase.)

E.7.2 Accident-incident description

This data element shall provide a detailed description of the occurred chain of events.

E.7.3 Accident-incident assessment

This data element shall document the assessment that has been performed.

E.7.4 Accident decision and reporting

This data element shall describe decisions that have been reached by the authority responsible for implementation. If the conclusion of the assessment is that the accident-incident has had an effect on the project, i.e. the safety of the product or its operation, the organizations safety representative shall be informed. In this case, the accident-incident report becomes part of the project's safety data and is documented in the safety data package.

Annex F (informative)

Typical content of a safety data package

F.1 System description from safety viewpoint

This part 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 as a minimum include the following:

a. characteristics of the system functional architecture versus the applicable safety requirements (e.g. failure tolerance, emergency, warning, caution and safing;

b. characteristics of the proposed layout of the system versus the applicable safety requirements (e.g. failure tolerance and prevention of failure propagation;

c. description of the safety margins in the various phases of the system mission;

d. compatibility of the proposed system design and operational scenario with the natural environment (e.g. meteoroids, debris and radiation) in which the system operates;

e. description of the tasks required to be performed by the space system crew (where present) and ground personnel and their relation with safety;

f. hazardous characteristics of the materials used,

g. characteristics of the hardware and software items used to implement the emergency, warning, caution and safing functions;

h. description of contingency and emergency procedures;

i. description of the interfaces with the ground support equipment and related ground operations.

Schematics and drawings should support the above data 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.

F.2 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.

F.3 Identification of safety critical functions

a. The safety data package shall contain the list of safety critical functions in the system.

b. The safety data package shall contain the analyses used to identify and categorise the various system functions as safety critical or not.

1. Hazard analysis
2. Warning time analysis
3. Caution and warning analysis
4. Safety risk assessment
5. Fault tree analysis
6. Design for minimum risk data
7. Software safety analysis
8. Supporting analyses
   (a) Human dependability
   (b) Sneak analysis
9. Safety critical items list
10. Hazardous ground operations list and procedures
11. Waiver status log
12. Accident-incident status log
13. Safety review action items list
14. Conclusion

Bibliography

BS 6079:1996	Project management — Guide to project management
ECSS-M-00-02A	Space project management — Tailoring of space standards
IEC 50:1992	Electricity, electronics and telecommunications multilingual dictionary
ISO/IEC Guide 2:1996	Standardization and related activities — General vocabulary
ISO 8402:1994 [1)]	Quality management and quality assurance — Vocabulary
ISO 9000:2000	Quality management systems — Fundamentals and vocabulary
ISO 14620-1:—[2)]	Space systems — Safety requirements — Part 1: System safety
ISO 14620-2:2000	Space systems — Safety requirements — Part 2: Launch site operations

NUREG-CR-2300-Volume 1 1983, A guide to the performance of probabilistic risk assessments for nuclear power plants

The Oxford English Dictionary (Second edition)

1) Obsolete.

2) To be published.

(This page is intentionally left blank)

ECSS Document Improvement Proposal

1. Document I.D.	2. Document date	3. Document title
ECSS-Q-40B	17 May 2002	Safety

4. Recommended improvement (identify clauses, subclauses and include modified text or graphic, attach pages as necessary)

5. Reason for recommendation

6. Originator of recommendation

Name:	Organization:	
Address:	Phone: Fax: e-mail:	**7. Date of submission:**

8. Send to ECSS Secretariat

Name:	Address:	Phone: +31-71-565-3952
W. Kriedte	ESTEC, P.O. Box 299	Fax: +31-71-565-6839
ESA-TOS/QR	2200 AG Noordwijk	e-mail: Werner.Kriedte@esa.int
	The Netherlands	

Note: The originator of the submission should complete items 4, 5, 6 and 7.

This form is available as a Word and Wordperfect-file on internet under
http://www.ecss.nl

(This page is intentionally left blank)