ECSS-Q-40-02A

14 February 2003

EUROPEAN COOPERATION

ECSS

FOR SPACE STANDARDIZATION

Space product assurance

Hazard analysis

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: € 10

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 documents.

This Standard has been prepared by the ECSS Hazard Analysis Working Group, reviewed by the ECSS Product Assurance Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Introduction

Safety analysis comprises hazard analysis, safety risk assessment and supporting analyses as defined in ECSS-Q-40. The objective of safety analysis is to identify, assess, reduce, accept, and control safety hazards and the associated safety risks in a systematic, proactive, complete and cost effective manner, taking into account the project's technical and programmatic constraints. Safety analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases, and by changes to a given project baseline.

Hazard analysis comprises the identification classification and reduction of hazards. Hazard analysis can be implemented at each level of the customer-supplier network. Hazard analysis activities at lower level can contribute to system level safety analysis. System level safety analysis can determine lower level hazard analysis activities.

Hazard analysis interfaces with dependability analysis, in particular FMECA. Safety risk assessment interfaces with quantitative dependability analysis, in particular reliability analysis. Safety risk assessment contributes to project risk management. Ranking of safety risks according to their criticality for project success, allowing management to direct its attention to the essential safety issues, is part of the major objectives of risk management.

Safety risk assessment is further addressed in ECSS Q-40-03.

(This page is intentionally left blank)

Contents

Foreword **3**

Introduction **5**

1 Scope **9**

2 Normative references **11**

3 Terms, definitions and abbreviated terms **13**
3.1 Terms and definitions 13
3.2 Abbreviated terms 15

4 Principles of hazard analysis **17**
4.1 Hazard analysis concept 17
4.2 Role of hazard analysis 20
4.3 Hazard analysis process 20
4.4 Hazard analysis implementation 21
4.5 Hazard analysis documentation 21

5 Objectives of hazard analysis **23**

6 Hazard analysis requirements and process **25**
6.1 Hazard analysis requirements 25
6.2 Overview of the hazard analysis process 25
6.3 Hazard analysis steps and tasks 27
6.4 Integration of hazard analysis activities 32

7 Hazard analysis implementation **33**
7.1 General considerations 33
7.2 Type of project considerations 33

7.3 Documentation of hazard analysis 33

Annex A (informative) Examples of generic hazards 35

Annex B (informative) Hazard and safety risk register (example) and ranked hazard and safety risk log (example) 37

Annex C (informative) Background information 41

C.1 Preliminary hazard analysis (PHA) 41
C.2 Subsystem hazard analysis (SSHA) 41
C.3 System hazard analysis (SHA) 42
C.4 Operating hazard analysis (OHA) 42

Bibliography 43

Figures

Figure 1: Hazards and hazard scenarios 17
Figure 2: Example of a hazard tree 18
Figure 3: Example of a consequence tree 18
Figure 4: Reduction of hazards 19
Figure 5: Interface to FMECA and CC&M analysis 19
Figure 6: The process of hazard analysis 20
Figure 7: The steps and cycles in the hazard analysis process 26
Figure 8: The nine tasks associated with the four steps of the hazard analysis process . . . 26
Figure 9: Example of a safety consequence severity categorization 27
Figure 10: Example of a hazard matrix 28
Figure 11: Example of a hazard manifestation list 29
Figure 12: Example of a hazard scenario 30

1

Scope

This Standard details the hazard analysis requirements of ECSS-Q-40B, 6.4.2; it defines the principles, process, implementation, and requirements of hazard analysis.

It 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.

(This page is intentionally left blank)

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-00-03	Space project management — Risk management
ECSS-M-30	Space project management — Project phasing and planning
ECSS-M-40	Space project management — Configuration management
ECSS-Q-40B	Space product assurance — System safety

(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
consequence tree
set of hazard scenarios leading to the same safety consequence

3.1.2
detection time
time span between the occurrence of the initiator event and its detection through the observable symptoms

3.1.3
hazard
existing or potential condition of an item that can result in a mishap

[ISO 14620-2]

NOTE 1 This condition can be associated with the design, fabrication, operation, or environment of the item, and has the potential for mishaps.
[ISO 14620-2]

NOTE 2 Hazards are potential threats to the safety of a system. They are not events, but the prerequisite for the occurrence of hazard scenarios with their negative effects on safety in terms of the safety consequences.

3.1.4
hazard acceptance
decision to tolerate the consequences of the hazard scenarios when they occur

3.1.5
hazard analysis
systematic and iterative process of the identification, classification and reduction of hazards

3.1.6
hazard control
preventive or mitigation measure, associated to a hazard scenario, which is introduced into the system design and operation to avoid the events or to interrupt their propagation to consequence

3.1.7
hazard elimination
removal of a hazard from a particular hazard manifestation

3.1.8
hazard manifestation
presence of specific hazards in the technical design, operation and environment of a system

3.1.9
hazard minimization
substitution of a hazard in the hazard manifestation by another hazard of the same type but with a lower potential threat

EXAMPLE High toxicity to low toxicity.

3.1.10
hazard reduction
process of elimination or minimization and control of hazards

3.1.11
hazard scenario
sequence of events leading from the initial cause to the unwanted safety consequence

NOTE The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

3.1.12
hazard tree
set of hazard scenarios originating from the same set of hazard manifestations

3.1.13
hazardous
property of an item and its environment which provides the potential for mishaps

[ISO 14620-2]

3.1.14
observable symptoms
evidence that indicates that an undesirable event has occurred

NOTE Observable symptoms appear during the propagation time.

3.1.15
reaction time
time span between the detection and the occurrence of the consequence

NOTE This is the time span available for mitigating actions after detection of the occurrence of the initiator event.

3.1.16
residual hazard
hazard remaining after implementation of hazard reduction

3.1.17
resolved hazard
hazard that is reduced, the reduction verified and the hazard considered acceptable

NOTE Resolved hazards are submitted for formal acceptance.

3.1.18
scenario propagation time
time span between the occurrence of the initiator event and the occurrence of the consequence

3.1.19
severity of safety consequence
measure of the gravity of damage with respect to safety

3.2 Abbreviated terms

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

CC&M	common cause and common failure mode analysis
DRD	Document requirements definition
ECSS	European Cooperation for Space Standardization
FMECA	failure modes, effects and criticality analysis
GSE	ground support equipment
NASA	National Aeronautics and Space Administration
OHA	operating hazard analysis
PHA	preliminary hazard analysis
SHA	system hazard analysis
SSHA	subsystem hazard analysis

(This page is intentionally left blank)

4

Principles of hazard analysis

4.1 Hazard analysis concept

Hazard analysis is based on the following hazard analysis concept, which is depicted in Figures 1 to 4.

Hazards, which are present through hazard manifestations in the system, are activated if initiating events (i.e. cause) occur. Hazard scenarios reflect the system behaviour to the activated hazards in terms of event propagation from causes to safety consequences, as depicted in Figure 1. The occurrence of events is coupled to observable symptoms in the system. Safety consequences are characterized by their severity.

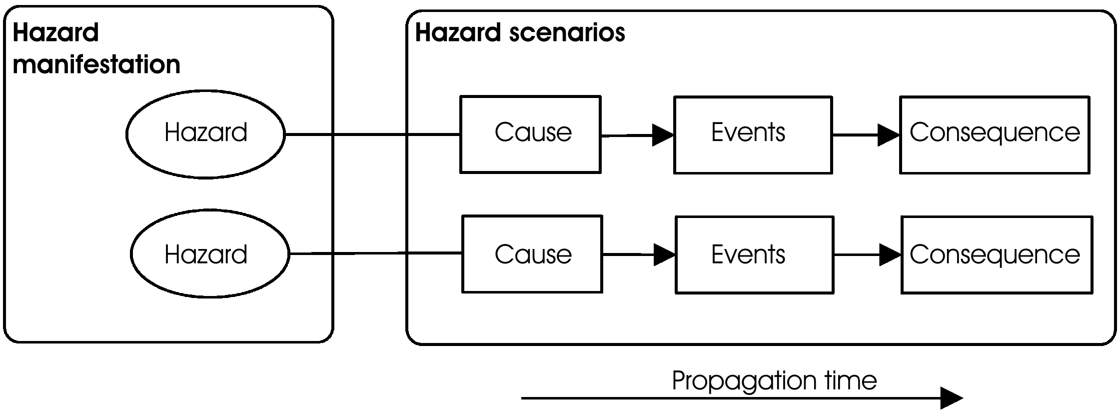

Figure 1: Hazards and hazard scenarios

Different hazard scenarios can originate from the same hazard. Furthermore, different hazard scenarios can lead to the same safety consequence. For an example, see Figure 12. The collection of hazard scenarios originating from the same hazard manifestation is collated into a hazard tree, as illustrated in Figure 2. The collection of hazard scenarios leading to the same safety consequence is collated into a consequence tree, as illustrated in Figure 3.

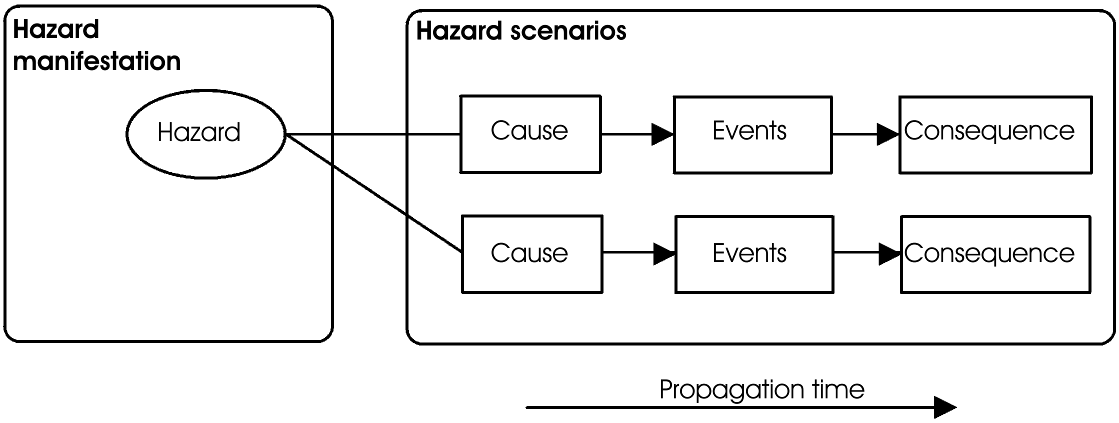

Figure 2: Example of a hazard tree

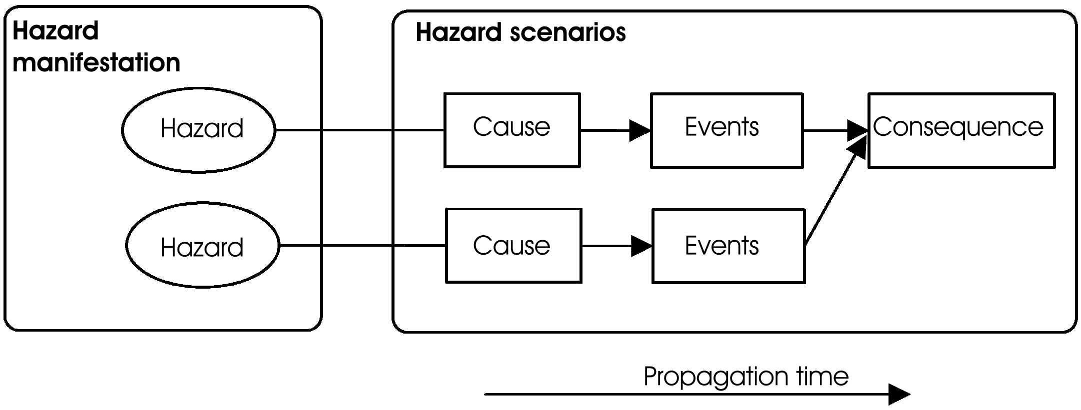

Figure 3: Example of a consequence tree

Hazards are reduced by either eliminating them or, if this is not possible, by minimizing and controlling them, as shown in Figure 4. Hazards are eliminated through the removal of specific potentially safety threatening system characteristics. Hazards are minimized through reducing the level or amount of specific potentially safety threatening system characteristics. Hazards are controlled through the prevention of the occurrence or reduction of the likelihood and mitigation of the effects of events. Occurrence of the events can be detected through their observable symptoms.

EXAMPLE A *hazard* to driving a car is "poor weather conditions", and the *hazard is manifested* by "ice on the road". The *cause* "rapid change of direction" can lead to the *event* "loss of control" and finally to the *consequence* "death of driver". *Hazard elimination* can be achieved by "delaying the journey", and *hazard minimization* by gritting the road. There are various methods for *hazard control* which impact on different parts of the process: "driving slowly" impacts on the cause; "using snow-chains" impacts on the link between cause and event; "fitting airbag" impacts on the link between event and consequence.

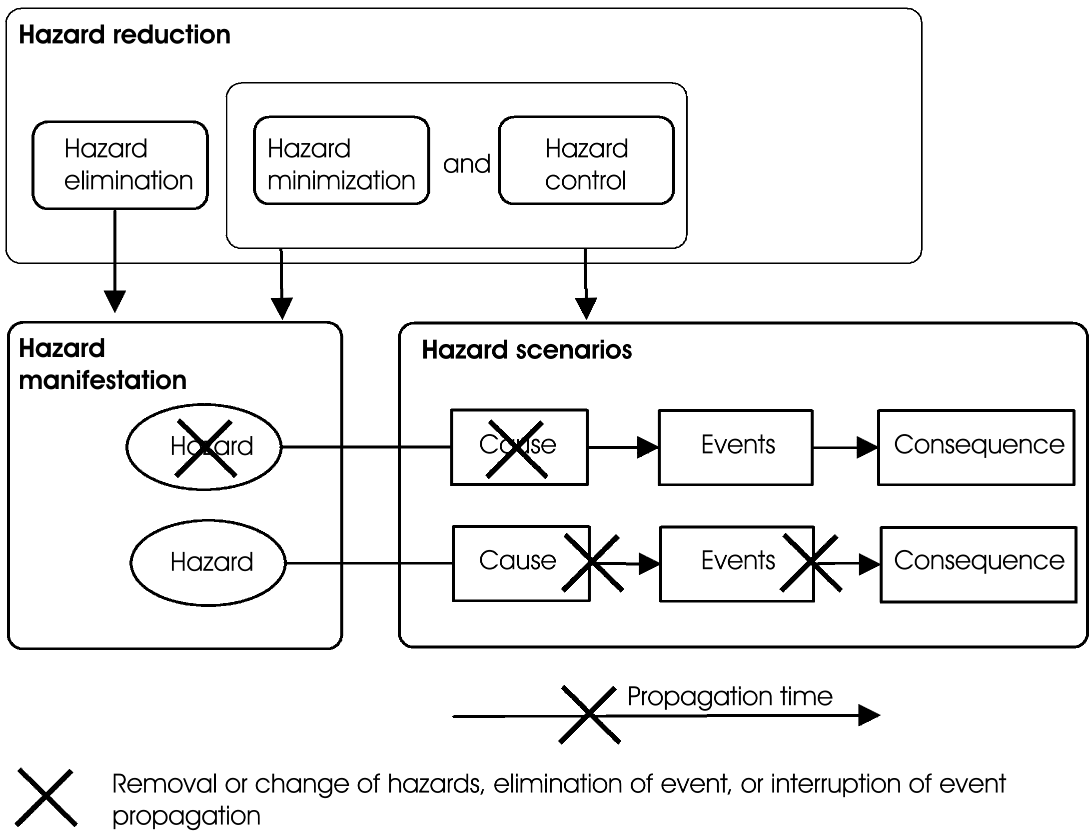

Figure 4: Reduction of hazards

Failure causes as identified through FMECA and other analyses, such as common cause and common failure mode analysis (CC&M), can represent causes of hazard scenarios, as depicted in Figure 5.

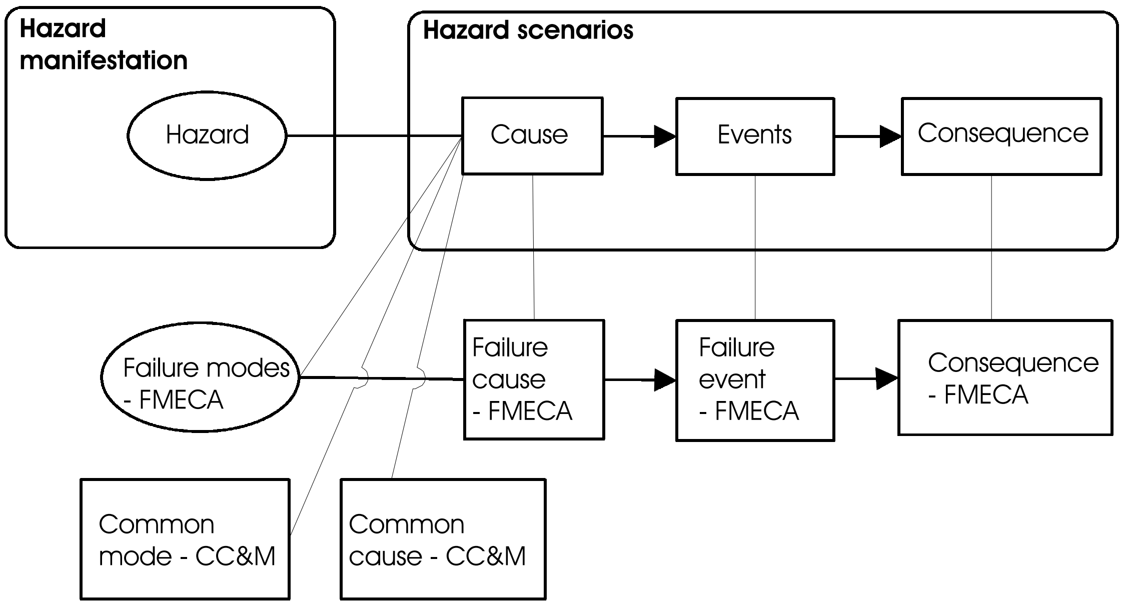

Figure 5: Interface to FMECA and CC&M analysis

4.2 Role of hazard analysis

Hazard analysis is the principal deterministic safety analysis which assists engineers and managers in including safety aspects in the engineering practices and the decision-making process throughout the project life cycle in design, construction, testing, operation, maintenance, and disposal, together with their interfaces.

Hazard analysis provides essential input to the safety risk assessment for a system.

4.3 Hazard analysis process

The hazard analysis process comprises the steps and tasks necessary to identify and classify hazards, to achieve hazard reduction. The basic steps are:

- Step 1: define the hazard analysis implementation requirements;
- Step 2: identify and classify the hazards;
- Step 3: decide and act on the hazards;
- Step 4: track, communicate and accept the hazards.

The process of hazard analysis, including iteration of its tasks, is summarized in Figure 6.

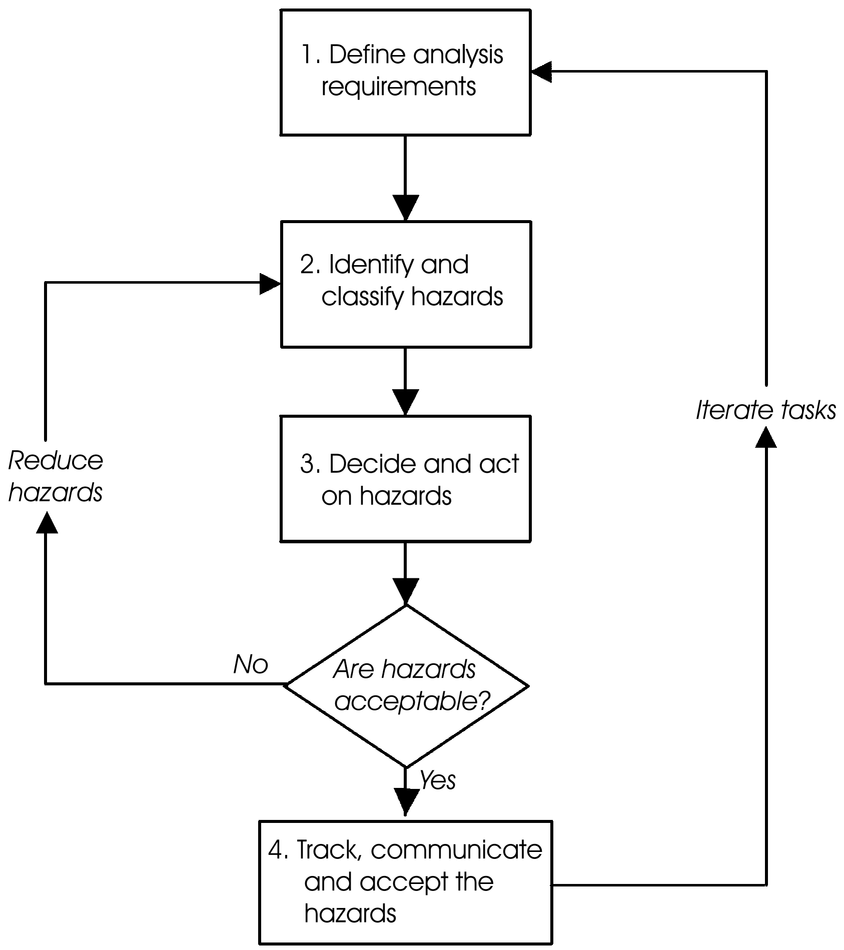

Figure 6: The process of hazard analysis

4.4 Hazard analysis implementation

Implementation of hazard analysis in a project is based on single or multiple, i.e. iterative, application of the hazard analysis process. The tasks associated with the individual steps of the hazard analysis process vary according to the scope and objectives specified for hazard analysis. The scope and objectives of hazard analysis depend on the type and phase of the project.

Hazard analysis requires commitment in each actor's organization, and the establishment of clear lines of responsibility and accountability. Project management has overall responsibility for the implementation of hazard analysis, ensuring an integrated, coherent hazard analysis approach.

4.5 Hazard analysis documentation

The hazard analysis process is documented to ensure that the scope and objectives of hazard analysis are established, understood, implemented and maintained, and that an audit trail can track the origin and rationale of all safety related decisions made during the life of the project.

(This page is intentionally left blank)

5

Objectives of hazard analysis

The general objectives of hazard analysis are to:

- assess the level of safety of a system in a deterministic way;
- increase the level of safety of a system through hazard reduction;
- initiate the use of hazard reduction to drive the definition and implementation of, for example, design and operation requirements, specifications, concepts, procedures;
- provide a basis for defining adequate safety requirements, determining the applicability of safety requirements, implementing safety requirements, verifying their implementation, and demonstrating compliance or non-compliance;
- provide input to safety risk assessment and overall risk management;
- support safety related project decisions;
- support safety submissions and reviews through documented evidence; and
- support safety certification of a system through documented evidence.

The specific objectives of hazard analysis with respect to a project-specific application are determined under Step 1 of the hazard analysis process — see subclause 4.3 and clause 6.

(This page is intentionally left blank)

6

Hazard analysis requirements and process

6.1 Hazard analysis requirements

The following hazard analysis requirements are defined:

a. The basis for hazard analysis shall be the four-step process comprising the nine tasks as defined in the following subclauses.

b. The outputs of hazard analysis shall be documented in accordance with the requirements of ECSS-Q-40B, annex B, Hazard report — Document requirements definition (DRD).

6.2 Overview of the hazard analysis process

The iterative four-step hazard analysis process is illustrated in Figure 7. The tasks within each of these steps are shown in Figure 8.

Step 1 comprises the establishment of the scope and purpose of hazard analysis, the hazard analysis planning (Task 1), and the definition of the system to be analysed (Task 2). Step 1 is performed at the beginning of a project. According to the scope and purpose, the implementation of the hazard analysis process consists of a number of "hazard analysis cycles" over the project's duration, comprising the necessary revisions of the analysis requirements and the Steps 2 to 4, subdivided in the seven Tasks 3 to 9.

The period designated in Figure 7 as the "Hazard analysis process" comprises all the phases of the project concerned, as defined in ECSS-M-30. The frequency and the events at which cycles are required in a project (only 3 are shown in Figure 7 for illustration purposes) depend on the needs and complexity of the project, and are defined during Step 1 at the beginning of the project.

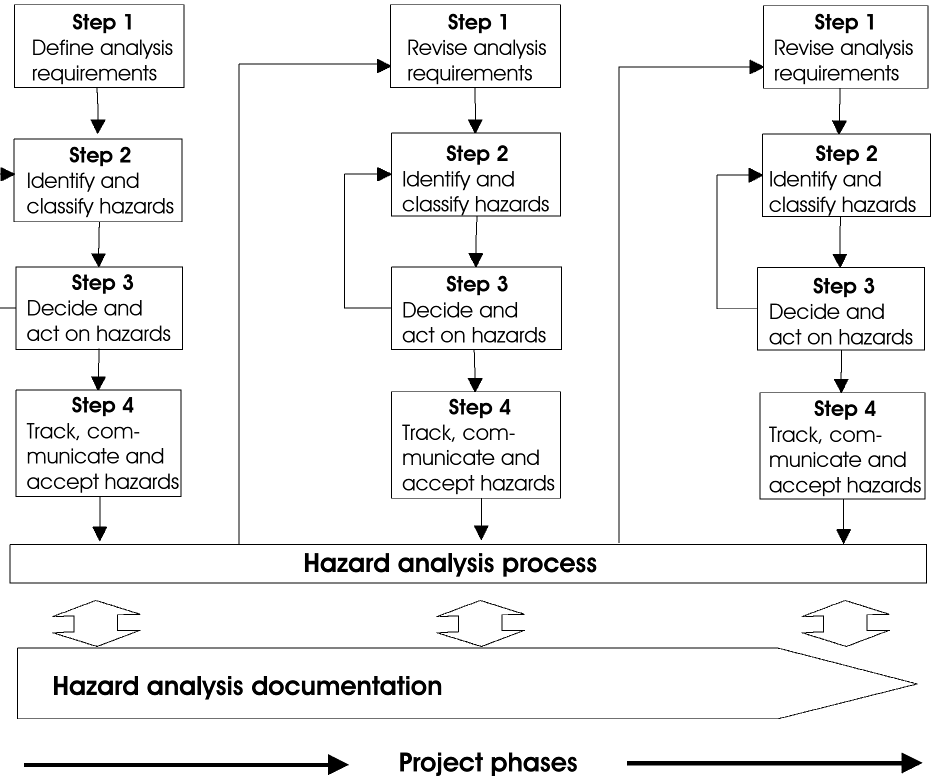

Figure 7: The steps and cycles in the hazard analysis process

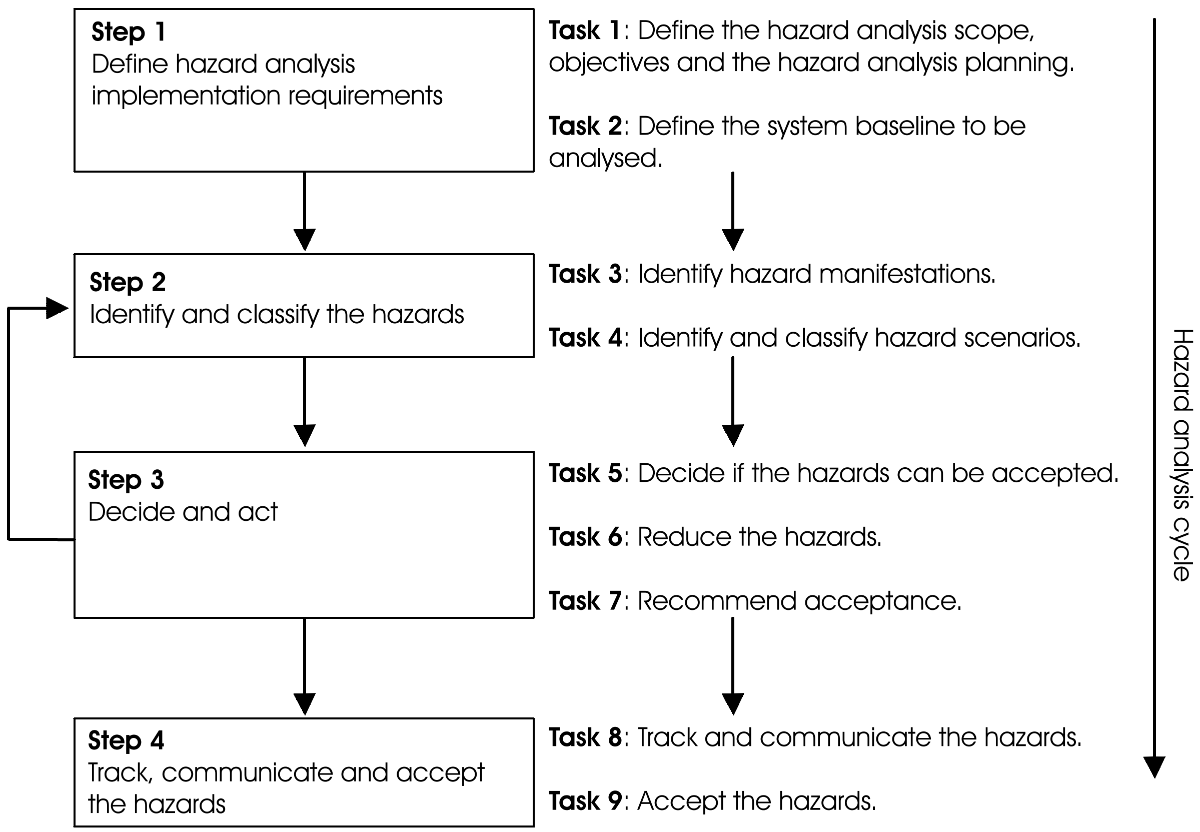

Figure 8: The nine tasks associated with the four steps of the hazard analysis process

6.3 Hazard analysis steps and tasks

6.3.1 Step 1: Define hazard analysis implementation requirements

6.3.1.1 Introduction

The implementation of hazard analysis in a project starts with Step 1, which is performed at the beginning of the project and comprises Tasks 1 and 2.

6.3.1.2 Task 1: Define the scope, the objectives of hazard analysis and the hazard analysis planning

The following activities are included in this task:

a. Establish the purpose and application boundaries of hazard analysis.

   Define the type of project (see subclause 7.2) and relevant part of the project life cycle.

b. Identify applicable safety requirements.

   Define customer requirements and interfacing contractor requirements.

c. Define the hazard analysis approach commensurate with the purpose and including the required depth of analysis.

   Define the input requirements for safety risk assessment according to ECSS-Q-40-03, if applicable.

   Identify relevant input data for hazard analysis, such as FMECA and CC&M, similar analysis from, for example, other projects, experience data, system models and expert judgement.

d. Establish scoring schemes for the severity of safety consequences for the classification of hazard scenarios commensurate with the applicable project risk management policy according to ECSS-M-00-03 and with ECSS-Q-40, which are typically as shown in the example given in Figure 9.

   According to ECSS-Q-40B, the consequence severity categories "Catastrophic" and "Critical" shall be used for any space projects and applications. In addition, other categories may be used to complete the assessment of the safety consequences.

Category	Severity	Severity of safety consequence
I	Catastrophic	Loss of life, life-threatening or permanently disabling injury or occupational illness; Loss of an element of an interfacing manned flight system; Loss of launch site facilities or loss of system; Severe detrimental environmental effects.
II	Critical	Temporarily disabling, but not life-threatening injury or illness; Major damage to flight systems or loss of or major damage to ground facilities; Major damage to public or private property; Major detrimental environmental effects.
III	Marginal	Minor injury, minor disability, minor occupational illness; Minor system or environmental damage.
IV	Negligible	Less than minor injury, disability, occupational illness; Less than minor system or environmental damage.

Figure 9: Example of a safety consequence severity categorization

e. Plan the hazard analysis application.

f. Establish criteria to determine the actions to be taken on hazards, hazard reduction and the associated decision levels in the project structure.

g. Define hazard acceptance criteria for individual hazards and hazard scenarios.

h. Define the strategy, and the formats to be used for documenting hazard analysis data and communication of relevant data to the decision-makers, and for monitoring the hazards.

i. Describe the review, decision and implementation flow within the project concerning all hazard analysis matters.

6.3.1.3 Task 2: Define the system baseline to be analysed

The following activities are included in this task:

a. Define and describe the design and operation subjected to hazard analysis, such as drawings, procedures and test reports.

b. Revise the system baseline definition for each hazard analysis cycle with the level of detail available at that time. Refer to configuration files, as defined by ECSS-M-40, for a valid configuration baseline definition.

6.3.2 Step 2: Identify and assess the hazards

6.3.2.1 Introduction

The purpose is to identify hazard manifestations, and hazard scenarios and to classify them according to the consequence severity.

6.3.2.2 Task 3: Identify hazard manifestations

The following activities are included in this task:

a. Identify generic hazards (for examples see annex A) applicable to the system design and operation using a hazard matrix, an example of which is illustrated in Figure 10.

b. Identify and give a detailed definition of system specific hazards and describe them in the form of hazard manifestations, an example of which is illustrated in Figure 11.

The example in Figure 10 shows part of a hazard matrix, in this case for the ground operation phase. Each element of the matrix indicates the applicability of the generic hazard to the corresponding subsystem.

Hazard matrix for ground operation			
Generic hazards	Subsystem elements		
	Propulsion subsystem	Instruments	Communication subsystem
High pressure	X	-	-
High temperature	-	-	-
Toxicity	X	X	-
Flammability	X	-	-
X = applicable	- = not applicable		

Figure 10: Example of a hazard matrix

The example in Figure 11 shows part of a hazard manifestation list. Each row of the list describes the manifestation of the hazard for each subsystem within each specific mission phase.

Hazard manifestation list		
Mission phase	**Subsystem**	**Hazard manifestation**
Ground operation	Propulsion	Filling of Y litres of toxic propellant into two tanks at a pressure of X1 Pa
	Instruments	Painting and seal material used in instrument cabinet A emitting toxic fumes if exposed to fire
In-orbit operation	Propulsion	Propellant lines under pressure at X2 Pa
	Instruments	Painting and seal material used in instrument cabinet A emitting toxic fumes if exposed to fire

Figure 11: Example of a hazard manifestation list

6.3.2.3 Task 4: Identify and classify the hazard scenarios

The following activities are included in this task:

a. Identify the hazard scenarios associated with the hazard manifestations by identifying the causes, events and safety consequences, according to the hazard analysis planning. This involves:

1. The determination of events triggering the hazards, i.e. causes, description of the causes in terms of definition of physical or functional failures or other physical phenomena, which bring about the activation of the hazards.
2. The determination of the physical propagation of events from a cause to the consequences, through investigation of the physical layout of the system and assessment of mechanisms involving physical damage propagation, and description of the physical behaviour of the system in response to the occurrence of the causes.
3. The determination of the functional propagation of events from a cause to the consequences through investigation of the functional layout of the system and assessment of mechanisms involving functional failure propagation, and description of the functional behaviour of the system in response to the occurrence of the causes.
4. A combination of the above cases 1. to 3.
5. The identification of common cause and mode phenomena (see ECSS-Q-40-01) and their propagation to safety consequences, and description of the physical and functional behaviour of the system in response to the occurrence of these events.
6. The determination of time-related event propagation and the description of the physical and functional behaviour of the system in response to the occurrence of these events.
7. The determination of operation sequence induced event propagation associated with operational steps and procedures, and description of the physical and functional behaviour of the system in response to the occurrence of these events.
8. The determination of failure events, as determined in the FMECA (see ECSS-Q-30-02), propagating to safety consequences.

b. Identify the propagation time, the observable symptoms and the detection time for each hazard scenario.

c. Determine the consequence severity of each hazard scenario according to the severity categorization defined in Task 1.

d. Determine the hazard trees by identifying all hazard scenarios originating from one and the same hazard manifestation.

e. Determine the consequence trees by identifying all hazard scenarios leading to one and the same safety consequence.

f. Use the hazard and consequence trees to screen for additional hazard scenarios.

g. Identify information sources, interfacing analysis e.g. FMECA and methods used to support the identification process and to justify the hazard scenarios.

The example in Figure 12 shows part of a hazard scenario list. Each row of the list describes the scenario for each manifestation of the hazard for each subsystem within each specific mission phase.

Hazard scenario list for in-orbit phase				
Hazard Manifestation	**Cause - Events - Consequence**	**Consequence Severity**	**Observable Symptoms**	**Propagation and reaction time**
In-orbit - pressurized manned module: Meteorite debris environment	Meteorite debris impact - shell rupture - explosion - loss of spacecraft and astronauts	Catastrophic	None	Ptime: 1 s Rtime: N/A
	Meteorite debris impact - shell damage - leakage - loss of spacecraft and astronauts	Catastrophic	Module pressure drop	Ptime: 3 min Rtime: < 3 min

Figure 12: Example of a hazard scenario

6.3.3 Step 3: Decide and act

6.3.3.1 Introduction

In this step the acceptability of hazards and hazard reduction options is analysed and the appropriate hazard reduction strategy is determined.

6.3.3.2 Task 5: Decide if the hazards can be accepted

The following activities are included in this task:

a. Apply the hazard acceptance criteria to the hazards as defined in Task 1.

b. Identify the acceptable hazards and those that are subjected to hazard reduction.

c. For acceptable hazards, proceed directly to Step 4; for unacceptable hazards proceed to Task 6.

6.3.3.3 Task 6: Reduce the hazards

The following activities are included in this task:

a. Determine measures in the form of design and operation features through which the hazards can be eliminated.

b. Where hazards cannot be eliminated, determine measures in the form of design and operation features through which hazards can be minimized and controlled. For hazard control, identify the preventive and mitigation measures in the following order of precedence:

1. Design and operation features that prevent the occurrence of a cause through e.g. safety features.
2. Design and operation features that prevent or interrupt the physical propagation of a cause to an event through introduction of e.g. physical barriers.
3. Design and operation features that prevent or interrupt the functional propagation of a cause to an event through introduction of e.g. functional redundancy.
4. Design and operation features that prevent or interrupt the functional propagation of a cause to an event through introduction of an emergency, warning and caution function.
5. Design and operation features that reduce the severity of a consequence through introduction of a safing, escape or rescue feature or function.
6. Procedures or changes in operational steps and procedures.

c. Determine hazard reduction success, failure and verification criteria.

d. Determine verification means and methods for the implementation of hazard reduction.

e. Select and prioritize the hazard reduction measures.

f. Verify hazard reduction through application of the verification means and methods.

g. Identify the resolved and unresolved hazards.

6.3.3.4 Task 7: Recommend acceptance

The following activities are included in this task:

a. Submit the hazard data.

b. Present the unresolved hazards for further action.

c. Provide the rationale and supporting data for resolution and acceptance of the hazards.

6.3.4 Step 4: Track, communicate and accept the hazards

6.3.4.1 Introduction

The purpose of this step is to track, update, iterate and communicate hazards, and finally to accept the residual hazards.

6.3.4.2 Task 8: Track and communicate the hazards

The following activities are included in this task:

a. Periodically assess and review all identified hazards and update the results after each iteration of the hazard analysis process.

b. Identify changes to existing hazards, and subsequently initiate new hazard analysis.

c. Verify the performance and the effect of the hazard reduction activities.

d. Identify and communicate the evolution of hazards over the project life cycle.

6.3.4.3 Task 9: Accept the hazards

The following activities are included in this task:

a. Submit the residual hazards to formal hazard acceptance.

b. Assess the performance of the hazard analysis processes and implement improvement of the effectiveness based on experience with project progress.

6.4 Integration of hazard analysis activities

Hazard analysis activities are performed at different levels of the customer-supplier chain. The lower level hazard analysis activities are integrated into the system level hazard analysis activities. The proper and effective integration of these tasks is of major importance and is typically achieved by applying the following:

a. The top down approach from the system to lower level is to identify the required lower level hazard analysis inputs. The required inputs are linked to knowledge of the domain.

b. The lower level task is to consider that domain and to develop and provide the required input to the next level up.

c. The system level task, using a bottom-up approach, logically and effectively integrates the lower level hazard analysis inputs into the system level hazard analysis.

The above assists in achieving the following results:

a. Proper allocation of the consequence severity categories at system level.

b. Proper development and implementation of hazard reduction.

c. Identification of the unresolved hazards in a timely manner.

d. Assurance that all aspects are considered in order to optimize and harmonize hazard reduction.

7

Hazard analysis implementation

7.1 General considerations

a. Hazard analysis is implemented as a team effort, with tasks and responsibilities being assigned to the functions and individuals within the project organization with the relevant expertise in the areas of safety and engineering concerned by a given hazard.

b. The results of hazard analysis are used as input to project reviews and project management during the evolution of the system.

c. Annex C provides background information on traditionally performed hazard analyses.

7.2 Type of project considerations

Hazard analysis activities differ according to the type of project and required safety effort. However, the hazard analysis process is the same in each case. Hazard analysis activities are linked to different types of projects, such as:

a. Hazard analysis at sub-supplier level for safety of part of the spacecraft design and the operation of a manned or unmanned mission and as input to system safety efforts.

b. Hazard analysis at prime supplier level for system safety of total space system design and the operation of a manned or unmanned mission.

c. Hazard analysis at any supplier level for payload safety.

d. Hazard analysis at any supplier level for safety of spacecraft verification activities.

e. Hazard analysis at any supplier level for safety of other ground activities, operations and launch.

7.3 Documentation of hazard analysis

a. Hazard analyses are documented to ensure that all associated decisions are traceable and defensible.

b. Every task of the hazard analysis process is documented.

c. Example forms for summarizing the results of the tasks are presented in ECSS-Q-40B DRD for hazard reports. See annex B of this Standard for examples.

(This page is intentionally left blank)

Annex A (informative)

Examples of generic hazards

a. **Thermodynamic and fluidic**
Pressure (difference, high, low, vacuum)
Temperature (difference, high, low)
Heat transfer
Fluid jet
Thermal properties of materials

b. **Electrical and electromagnetic**
Voltage (high, medium, low)
Static electricity
Electric current (high, medium, low)
Magnetic field (induced, external)
Ionization
Sparks

c. **Radiation**
Light (infrared, visible, ultraviolet, laser)
Radioactivity (alpha, beta, gamma rays)
Open fire

d. **Chemical**
Toxicity
Corrosiveness
Flammability
Explosiveness
Asphyxiant
Irritant

e. **Mechanical**
Physical impact or mechanical energy
Mechanical properties of materials (e.g. sharp, rough, slippery)
Vibration

f. **Noise**

Frequency and intensity

g. **Biological**

Human waste

Micro-organism

Carcinogenic

h. **Psychological**

i. **Physical**

Confined space

j. **Environment - space**

Zero gravity

Vacuum

Atmospheric composition

Contaminants, pollutants

Meteorite and space debris

Temperature (difference, low, high)

Radiation

South Atlantic anomaly

k. **Environment - Earth**

Environmental extremes

Natural disasters

Lightning

Annex B (informative)

Hazard and safety risk register (example) and ranked hazard and safety risk log (example)

Hazard and safety risk register *(Example, see also ECSS‑Q‑40‑03 and ECSS‑M‑00‑03)*

Project WBS Ref.	Organization	Source Controlled by Supported by	Date and issue Approved by

Hazard description and safety risk magnitude

No.	Hazard scenario title
Hazard manifestation	Cause, events and safety consequence

Safety consequence severity (S)				Likelihood (L)					Risk Index	Risk	Red*	Yellow*	Green*
Negligible	Marginal	Critical	Catastrophic	Minimum	Low	Medium	High	Maximum	$(R = S \times L)$	Safety			
IV	III	II	I	E	D	C	B	A	Numerical risk and uncertainty contribution:				
				Numerical estimate:									

Hazard and safety risk decision and action

Accept hazard and safety risk ☐	Reduce hazard and safety risk ☐	
Hazard reduction measures Hazard elimination: Hazard minimization: Hazard control:	Hazard reduction verification means	Expected safety risk reduction Severity, likelihood, risk index: Numerical estimates: Safety risk rank:
Actions		Status
Agreed by project management		Hazard status

* Enter “R” in the appropriate column: correspondence of the risk index scores for red, yellow and green are defined in the project risk management policy

Ranked hazard and safety risk log *(Example)*

Project			Organization				Date and issue
Rank	**No.**	**Hazard scenario title**	**Risk ***	**Red**	**Yellow**	**Green**	**Actions and status**
			Safety				
			Safety				
			Safety				
			Safety				
			Safety				
			Safety				
			Safety				
			Safety				

* Enter “R” from Hazard and safety risk register

(This page is intentionally left blank)

Annex C (informative)

Background information

C.1 Preliminary hazard analysis (PHA)

The purpose of the PHA is to identify safety-critical areas, to identify and evaluate hazards, and to identify design and operations requirements needed in the programme concept phase.

The PHA is performed to document an initial risk assessment of a concept or system. It is based on the best available data, including data from similar systems and lessons learned from other programmes The PHA provides consideration of the following, as a minimum, for the identification and evaluation of hazards:

a. Hazards sources (e.g. propellants, lasers, explosive, toxic substances, corrosives, hazardous construction materials, pressure systems and other energy sources).

b. Safety-related interface considerations among various parts or elements of the analysed item, facilities and GSE (e.g. material compatibility, contamination, electromagnetic interference, inadvertent activation, fire or explosion initiation and propagation, and hardware and software controls).

c. Environmental constraints, including the operating environment (e.g. drop, shock, vibration, extreme temperature, noise, exposure to toxic substances, confined space, fire, electrostatic discharge, lightning, electromagnetic effects, and ionizing and non-ionizing radiation).

d. Operating test, maintenance, and emergency procedures.

e. Facilities, support equipment and training.

f. Safety-related equipment, safeguards and possible alternative approaches (e.g. monitoring, interlocks, redundancies, hardware or software fail-operational — fail-safe design consideration, fire protection, personal protective equipment, ventilation and noise or radiation attenuation).

C.2 Subsystem hazard analysis (SSHA)

The purpose of the SSHA is to identify hazards to personnel, vehicles, and other systems. The hazards can be caused by: loss of function; accidental activation; energy source; hardware failure; software deficiencies; interaction of components with subsystem; inherent design characteristics such as sharp edges and incompatible materials; and environmental conditions.

It defines the safety-critical functions, component fault conditions, generic hazard, safety-critical operations and environments associated with the subsystem.

C.3 System hazard analysis (SHA)

The purpose of the SHA is quite similar to the SSHA, but related to the system level. Once the subsystem levels have been established, a combination of subsystems makes up a system.

The SHA accomplishes the same purpose as the SSHA, but in terms of the interfaces and the overall system performance and operation.

C.4 Operating hazard analysis (OHA)

The purpose of the OHA is to identify hazards and recommend risk reduction alternatives in procedurally controlled activities during all phases of intended system usage. It can generally be part of the system hazard analysis (SHA), since it is interrelated with system safety features.

OHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons and equipment and considers the following:

a. planned system configuration at each activity phase,

b. facility interfaces,

c. planned environments,

d. supporting tools or other equipment specified in use,

e. operation or task sequence and limitations,

f. potential for unplanned events including hazards introduced by human error, and

g. the requirements for warnings, cautions and special emergency procedures.

The OHA should be conducted in parallel with development of procedures for manufacturing, processing and operation.

Bibliography

ECSS-Q-30-02	Space product assurance — Failure modes, effects and criticality analysis (FMECA)
ECSS-Q-40-01[1)]	Space product assurance — Common cause and common failure mode analysis
ECSS-Q-40-03[1)]	Space product assurance — Safety risk assessment
ISO 14620-2:2000	Space systems — Safety requirements — Part 2: Launch site operations

1) 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-40-02A	14 February 2003	Hazard analysis
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: W. Kriedte ESA-TOS/QR	Address: ESTEC, P.O. Box 299 2200 AG Noordwijk The Netherlands	Phone: +31-71-565-3952 Fax: +31-71-565-6839 e-mail: Werner.Kriedte@esa.int

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

An electronic version of this form is available in the ECSS website at: http://www.ecss.nl/
At the website, select "Standards" - "ECSS forms" - "ECSS Document Improvement Proposal"

(This page is intentionally left blank)