ECSS-Q-20-04A
31 March 2005

Space product assurance

Critical-item control

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-Q-20-04 Working Group, reviewed by the ECSS Product Assurance Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Introduction

Early identification of potential critical items provides valuable inputs to design engineering for their avoidance or elimination. Critical-item control provides management with acceptance rationale for those critical items that cannot be eliminated from the critical-item list, and identifies the means by which emanating risks can be controlled.

(This page is intentionally left blank)

Contents

Figures

1

Scope

This Standard defines the principles, process, implementation and requirements for critical-items control.

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

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

(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

(This page is intentionally left blank)

3

Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ECSS-P-001 and the following apply.

3.1.1
critical item
component, material, software, equipment, sub-assembly, function, process or technology, that requires special attention to prevent undesired consequences on the performance, quality, dependability or safety of the system

EXAMPLE Examples are provided in Annex C.

3.2 Abbreviated terms

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

Abbreviations	Meaning
AR	acceptance review
CDR	critical design review
CI	critical item
CIL	critical-item list
DRD	document requirements definition
ECSS	European Cooperation for Space Standardization
EEE	electronic, electrical, electromechanical
FMECA	failure modes, effects and criticality analysis
PA	product assurance
PDR	preliminary design review
PMP	parts, materials and processes
RAMS	reliability, availability, maintainability and safety
SPF	single-point failure

(This page is intentionally left blank)

4

Objectives of critical-item control

The objectives of critical-item control are to prevent the occurrence of failures in or problems with items through:

- provision of inputs to the risk management programme, identifying technical risks;
- identification of specific items likely to cause problems (critical items);
- identification of appropriate prevention and control measures;
- monitoring, implementation and verification of the control measures.

(This page is intentionally left blank)

5

Principles of critical-item control

5.1 Critical-item control concept

5.1.1 Critical items and critcal-item control

Critical items are potential threats to the performance, quality, dependability and safety of a system that need action to mitigate emanating risks and to prevent undesirable consequences.

5.1.2 Critical-item control process

The critical-item control process involves the:

- definition of the critical-item control requirements,
- identification and classification of critical items,
- selection, decision and implementation of critical-item control measures, and
- monitoring and communication of critical items.

5.1.3 Interfaces between critical-item control and risk management

By their nature critical items have the potential to introduce risks into a project. The potential threats to safety, dependability, performance and quality can be triggered within risk scenarios, which shall be dealt with by risk management.

While critical items are controlled through the CI control process, the associated risks are managed through the risk management process.

The interfaces between the risk management and critical-item control processes include (refer to Figure 1):

- critical-item inputs to the risk identification activity,
- risk classifications used to prioritize critical items,
- references between risk reduction and critical-item control measures,
- status of critical-item control implementation.

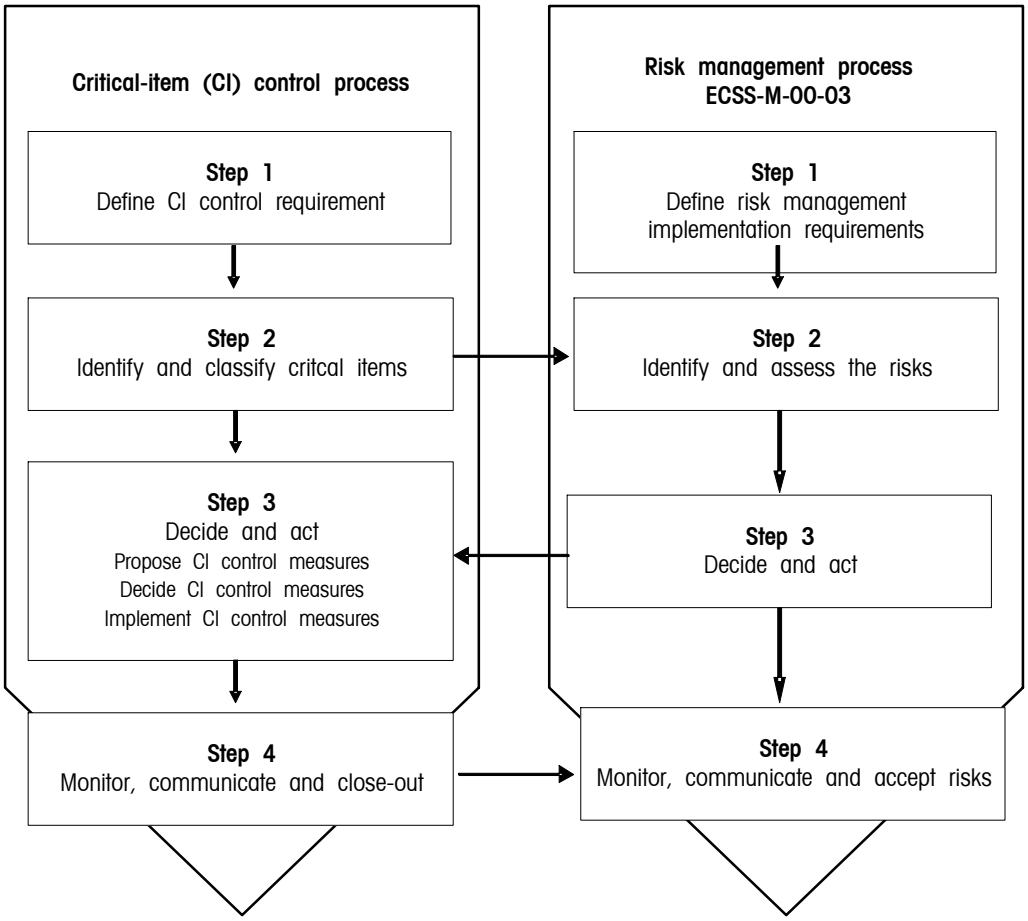

Figure 1: Critical-item control process, and its relation to the risk management process

5.1.4 Interfaces between critical-item control and product assurance

- Critical-item control is integrated with the product assurance (PA) programme of a project.
- Results from various PA analyses provide considerable inputs for critical-item identification (e.g. RAMS: FMECA results, hazard analysis results; PMP: non-qualified parts materials and processes; EEE: non-qualified parts or new technology; lessons learned from previous programmes).

5.1.5 Interfaces between critical-item control and product engineering

Critical-item control requirements affect both the specification of a product and the realization of the product. Therefore, the inputs and the outputs of the engineering process (e.g. technical specifications, and design documents) shall be reviewed for the identification and classification of critical items (taking into account the lessons learned from previous programmes). Critical-item control measures can establish constraints on the design and development process and shall be agreed with engineering.

5.2 Critical-item control implementation

a. Critical items shall be uniquely identified and classified according to the nature of their criticality.

   The critical-item identification process designates those items that require specific control measures to ensure that the technical performance of the end-product is as required.

b. The management of critical items shall include the following:

   1. A critical-item control plan shall be written at project level.
   2. The critical-item list (CIL) for the project shall be established and maintained throughout all the project phases to allow the tracking and monitoring of all the critical items identified.
   3. Specific control measures for the critical items shall be defined, in addition to the normal project activities.
   4. Evaluation points for assessing the implementation of critical-item control measures shall be identified. At evaluation points, the need to retain each item in the critical-item list shall be evaluated.
   5. The status of the critical items and of the relevant control measures shall be reported as part of the project progress reporting and at milestone reviews.

c. The criticality of an item can be reduced either by design or by procedural means. A critical item for which the associated risk is controlled by means of procedures shall receive particular attention in the further processing of the item.

d. All design, manufacturing, and test documentation related to critical items shall be identified and listed in the CIL. Document traceability shall be maintained by document number and issue.

e. Manufacturing, assembly, integration, testing, maintenance and operation involving a critical item shall be monitored for problems that can affect the performance of the item during the operational phase.

5.3 Critical-item control documentation

a. The CI control process shall be documented to ensure that the activities on critical items are properly defined, traced and verified during the life of the project.

b. Suitable formats for critical-item documentation are proposed in Annexes A and B.

c. The CI control programme shall be described in the CI control plan (stand-alone or as part of the project's product assurance plan). It shall define how the project implements the dedicated CI control requirements tailored from this Standard.

(This page is intentionally left blank)

6

Critical-item control process

6.1 Overview of the critical-item control process

The 4-step approach for the CI control process is illustrated in Figure 2.

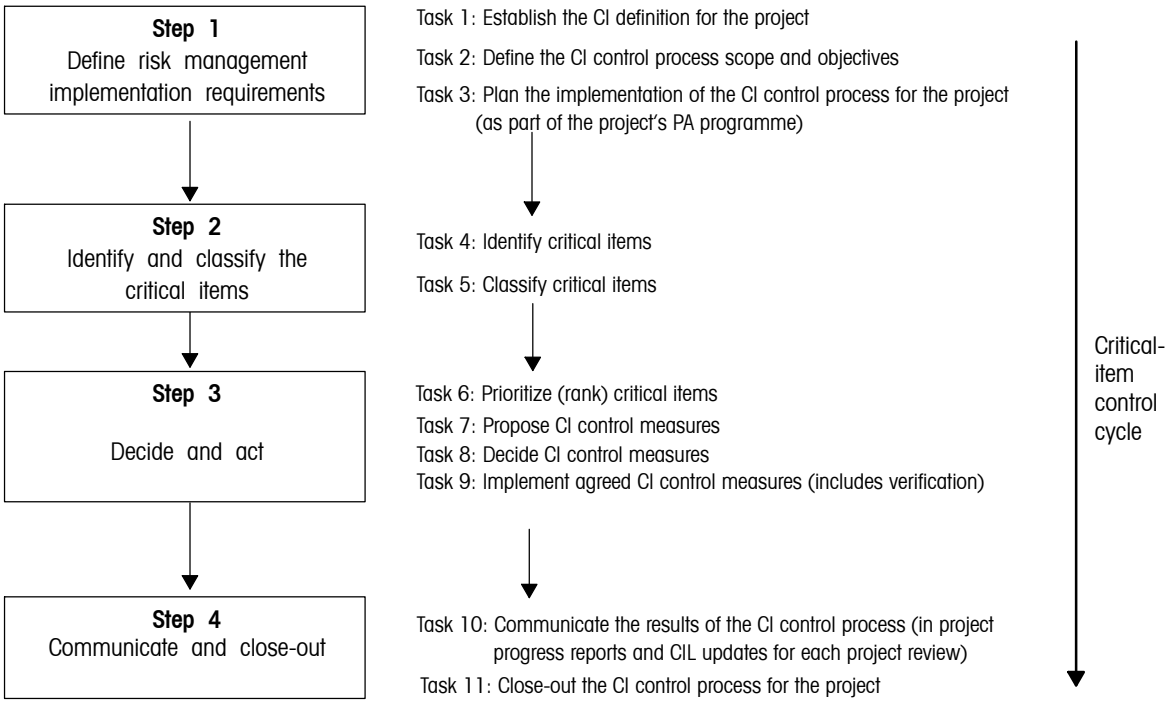

Figure 2: Tasks associated with the 4-step approach of the CI control process

6.2 Step 1: Define CI control requirement

6.2.1 General

The implementation of CI control in a project starts with Step 1, which is performed at the beginning of the project and comprises Tasks 1 to 3.

6.2.2 Task 1: Establish the CI definition for the project

The following activities are included in this task:

a. Identify applicable requirements.

EXAMPLE — Customer requirements relevant to the criteria to identify the critical item (this should coincide with the definition in subclause 3.1).

— Document requirements description (DRD) for establishing the critical items list (CIL) and the CI control plan.

— Risk management plan applicable to the project.

b. Define requirements for interfacing suppliers to identify lower level critical items in accordance with the project policy applied.

c. Establish the CI classification criteria.

EXAMPLE Refer to risk index scheme provided in ECSS-M-00-03.

d. Establish scoring schemes for the ranking of critical items commensurate with the applicable project risk management policy as defined in the project risk management plan.

EXAMPLE Refer to risk magnitude provided in ECSS-M-00-03.

6.2.3 Task 2: Define the CI control process scope and objectives

Establish the purpose and application boundaries of CI control.

6.2.4 Task 3: Plan the implementation of the CI control process for the project

a. Assign the responsibility for CI control management, in accordance with the product assurance plan.

b. Specify forms and the CI control programme documentation.

c. Describe the flow of activities (process) within the project (e.g. review, documentation preparation, and approval).

6.3 Step 2: Identify and classify the critical items

6.3.1 General

The purpose of the tasks defined hereafter is to identify critical items and to classify them according to the above categories.

6.3.2 Task 4: Identify critical items

The following activities are included in this task:

a. Review project documentation (design and engineering documents, supplier inputs).

b. Identify critical items in accordance with the project's definition (check-list for potential critical items is provided in Annex C).

c. For each critical item: identify clearly its nature of criticality.

d. List each critical item in the CIL and describe it in the associated critical item control form (formats provided in Annexes A and B).

6.3.3 Task 5: Classify critical items

Classify the critical items according to the criticality category defined in Task 1.

6.4 Step 3: Decide and act

6.4.1 General

In this step the criticality of items and options for control measures are identified and analysed. The most appropriate CI control strategy is determined, implemented and the implementation verified.

6.4.2 Task 6: Prioritize (rank) critical items

Identify the specific inputs from the risk management process and apply the ranking criteria for critical items defined in Task 1. Identify the prioritization of actions on the control of critical items.

6.4.3 Task 7: Propose CI control measures

a. The initial steps are:
   1. Identify suitable means by which critical items can be controlled.
   2. Refer to the examples of CI control measures in the form of design, operation, test and inspection related means and associated actions in Annex D.

b. Determine verification means regarding the implementation of the CI control measures. Identify methods for the implementation of these measures and assess the feasibility of their application.

6.4.4 Task 8: Decide on the CI control measures

a. Evaluate and assess the CI control measures and implementation methods with respect to their effectiveness and feasibility.

b. The following steps are taken in this activity:
   1. Select the CI control measures and implementation methods and define an optimized CI control strategy by prioritizing the implementation of CI control.
   2. Consider the impact of CI control on project resources including risks during the associated decision making and selection process.
   3. Consider the impact of the implementation of CI control measures on the acceptability of risks associated with the critical items.

c. Define verification means for the implementation of CI control.

d. Define success criteria for the implementation of CI control.

6.4.5 Task 9: Implement agreed CI control measures

The following activities are included in this task:

a. Implement the CI control strategy by applying the selected implementation methods.

b. Verify the implementation of CI control through application of the verification means. Apply the success criteria to demonstrate successful implementation and to identify areas of non-successful implementation, i.e. non-successfully controlled critical items.

c. Iterate Task 7 and 8 for non-successfully controlled critical items until they become successfully controlled or – if failing to do so – request disposition by higher management.

6.5 Step 4: Communicate and close-out

6.5.1 General

The purpose of this step is to monitor and communicate the status of critical items, and finally to support the close-out of the CI control process.

6.5.2 Task 10: Monitor and communicate the results of the CI control process

a. Assess and review all critical items periodically for status.

b. Assess critical items and associated control measures in particular when affected by nonconformances, anomalies (test and operation), problems and incidents.

c. Identify new critical items or changes to conditions under which critical items were previously evaluated.

d. Identify and communicate the evolution of CI status over the project evolution.

6.5.3 Task 11: Close-out the CI control process for the project

a. Submit the completed CIL for formal acceptance by project management.

b. Assess periodically the performance of the CI control processes and implement improvement of the effectiveness based on experience with project progress.

6.6 Integration of CI control activities

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

a. The top down approach from the system to lower level should be used to identify the required lower level inputs. The required inputs are linked to knowledge of the domain.

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

   The above assists in achieving the following results:

   1. proper allocation of the ranking scheme at the system level where applicable;
   2. proper development and implementation of CI control;
   3. identification of the not yet dispositioned items in a timely manner;
   4. assurance that all aspects relevant to the CI control are systematically considered.

Refer to Clause 7 for further recommendations for the integration of CI control into the project life cycle.

7

Integration of critical-item control into the project life cycle

7.1 Preliminary design review (PDR)

The preliminary version of the CIL shall include all the critical items identified by RAMS, PMP, EEE, QA and engineering disciplines that are already known in the early phases of the project (refer to Annex C).

In addition, the preliminary CIL shall include a list of recommendations for the elimination of design deficiencies by redesign in the detailed design phase.

In this phase, the preliminary CIL is used as a mean to present the nonconforming designs are presented to the programme management for initial evaluation and determination of the subsequent course of action.

7.2 Critical design review (CDR)

As per the PDR, during this phase the CIL shall continue to include and suitably document all the critical items identified in the different system analyses.

At this point in the programme, the CIL shall be used to address all the nonconforming designs to the programme management for formal evaluation and decision (i.e. acceptance or redesign).

During the CDR the CIL shall be evaluated and the results of the evaluation constitutes a preliminary indication of which items are candidates for programme acceptance, based on accepted criticality definitions, and which items require a redesign activity.

The integrated CIL shall be retained as the interim programme CIL until each of the items on the CIL is either baselined via programme approval or removed from the CIL based upon a design change.

7.3 Acceptance review (AR)

At the conclusion of the CDR, suitable actions shall be taken to prepare the CIL programme acceptance documentation for the identified critical items.

For all the cases where design changes are not imposed but where the items continue to be part of the CIL, appropriate programme acceptance documentation shall be developed using the retention rationale previously identified in the CDR CIL and updated as appropriate.

Each time a design change is imposed after its implementation, the CIL shall be updated to reflect the new configuration and the affected critical item shall be removed from the list. However, if the design change is not considered sufficient to eliminate criticality of the item, the CIL retention rationale shall be revised as necessary and the programme acceptance documentation shall be developed.

From the end of the CDR up to the conclusion of the AR, the status of the CIL open items, i.e. of the items where requests for programme acceptance have not been approved, shall be submitted to management at subsequent milestone reviews to aid in assessment of the readiness of the system and the associated risks.

If design changes occur during this phase, the CIL shall be updated to reflect the changes.

At the end of the AR, action closure shall be verified and approved for the non-eliminated critical items (as defined in the CIL).

Annex A (informative)

Critical-item list form

No.	Critical item	Risks associated	Reference doc.	Criticality level	Cause	Control activities	Due date	Status

No.	Unique item identifier.
Critical item	Identified critical item (e.g. unit, subsystem, equipment, component, material, process, and function).
Risks associated	Technical risk(s) associated with the critical item (refer to the associated entry in the Risk Register).
Reference doc.	Reference document in which the item is identified as critical.
Criticality level	In accordance with the critical item classification as defined in subclause 6.3.
Cause	Description of the cause which makes this item critical.
Control activities	(Refer to subclause 6.4.3 Task 7) Planned activities to reduce or control the risk and statement of verification of the control implementation (e.g. design and operational requirements, test, inspection and failure history).
Due date	Expected completion date of activities.
Status	Status of action: Open / Closed (with ref. to close-out docs.)

(This page is intentionally left blank)

Annex B (informative)

Critical-item control form

Critical-item identification	CI no.
Subsystem: Equipment: Item: Function:	
Title:	
Mission phase:	
Description of event (related to the critical item):	
Effects/risks at: - Product level: - Subsystem level: - System level:	
Possible causes:	
Problem identification reference:	
Severity category: Single-point failure (Yes/No): Propagation time:	Likelihood category: Detectability (Yes/No):
Applicable requirements:	

Item is confirmed critical by	Discipline	PA	Engineering	Project manager
	Name: Date: Signature:			

<table>
<tr><td colspan="3">Critical-item control sheet</td><td colspan="2">Sheet No.</td></tr>
<tr><td colspan="5">Measures proposed:</td></tr>
<tr><td>Measures adopted:</td><td>a) Specification</td><td>b) Design/definition</td><td colspan="2">c) Tests</td></tr>
<tr><td></td><td>d) Inspection procedures</td><td>e) Operational procedures</td><td colspan="2">f) In-flight detection</td></tr>
<tr><td rowspan="4">Potential risk reduction:

- Severity category:
- Likelihood category:</td><td rowspan="2">Risk to be reduced</td><td>Open</td><td></td></tr>
<tr><td>Confirmed</td><td></td></tr>
<tr><td rowspan="2">Accepted risk</td><td>Attenuated</td><td></td></tr>
<tr><td>Closed</td><td></td></tr>
<tr><td colspan="5">Effectiveness/rationale for retention/close-out documents:</td></tr>
</table>

(This page is intentionally left blank)

Annex C (informative)

Check-list for potential critical items

C.1 Examples of critical items

EXAMPLE 1 An item is critical if it is not qualified or validated for the application in question (or has caused problems previously which remained unresolved).

EXAMPLE 2 An item is critical if it is difficult to demonstrate design performance.

EXAMPLE 3 An item is critical if it is highly sensitive to the conditions under which it is produced or used (e.g. contamination, radiation).

EXAMPLE 4 An item is critical if it has the potential to degrade the quality of the product significantly, and hence the ability of the end-product to accomplish defined mission objectives.

EXAMPLE 5 An item is critical if major difficulties or uncertainties are expected in the procurement, manufacturing, assembly, inspection, test, handling, storage and transportation, that have the potential to lead to a major degradation in the quality of the product.

C.2 Potential RAMS critical items

- Item not meeting the applicable failure tolerance requirement.
- Item constituting a residual single-point failure (SPF).
- Fracture critical item (pressure vessel, structural item whose failure can result in catastrophic or critical consequences).
- Limited-life and limited-cycle item (item with useful life duration or operating cycles limitation; item prone to wear out, drift or degradation below minimum required performance in less than the storage and mission time).
- Item not meeting applicable derating requirements.
- Item considered critical at the conclusion of the worst case analyses.

C.3 Potential critical components, materials and processes

- Long-lead items (adverse impact of item procurement on project schedule).
- EEE components subject to export licence constraints.
- EEE components containing dangerous elements.
- EEE components sensitive to radiation environment in space.
- EEE components sensitive to ON/OFF switching.
- Components, material and processes new or not qualified or not validated for intended application.
- Item with a known history of flight failures.
- Item highly sensitive to manufacturing processes.

C.4 Software critical items

- List of critical software components, as per ECSS-Q-80B, subclause 6.2.2.
- Software items whose performances could be difficult to obtain.
- Software items not observable after integration in equipment.
- Software items not modifiable in the operational environment.
- Software items with strong intrinsic complexity.
- Software development tools with limited maintenance w.r.t. mission lifetime.

C.5 Items critical for integration

- Material with long manufacturing or procurement duration.
- Items that cannot be checked and tested after integration.
- Item presenting risks to the personnel (including in the event of inopportune controls).
- Item requiring special handling procedures.

C.6 Miscellaneous critical items

- Item difficult to control or implement.
- Material with particular constraints for storage.
- Item having posed as yet unsolved problems, at the time of a preceding utilization.
- Material sensitive to transport conditions.
- Item issued from lessons-learned internal database, if applicable.

Annex D (informative)

Examples of critical-item control measures

D.1 Design and operation

Identify specific design features that minimize the probability of occurrence of the failure mode and its causes. Where applicable, relate the design features to the specific causes. Typical controlling features include safety factors, use of special materials, unique physical or chemical characteristics or properties, critical dimensions, and other measurable parameters under design control. Describe the redundancy configuration, if applicable, and list the remaining success paths after first failure. Discuss performance degradation, if any, as failures occur or as life limits expire.

Assess:

- design and operation features that prevent the occurrence of a cause through e.g. safety features;
- design and operation features that prevent or interrupt the physical propagation of a cause to an event through introduction of, for example, physical barriers;
- design and operation features that prevent or interrupt the functional propagation of a cause to an event through introduction of, for example, functional redundancy;
- 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;
- design and operation features that reduce the severity of a consequence through introduction of a safing, escape or rescue feature or function;
- procedures or changes in operational steps and procedures.

D.2 Tests

Identify specific tests accomplished to detect failure modes and causes during acceptance tests, certification tests, and pre-launch and on-orbit check-out tests.

D.3 Inspection

Identify specific inspection criteria which are included to determine that specific failure mode causes are not inadvertently manufactured into the hardware or that hardware is not degraded.

(This page is intentionally left blank)

Bibliography

ECSS-M-00-02A	Space project management — Tailoring of space standards
ECSS-M-00-03	Space project management — Risk management
ECSS-Q-80B	Space product assurance — Software product assurance

(This page is intentionally left blank)

ECSS Document Improvement Proposal

1. Document I.D.	2. Document date	3. Document title
ECSS-Q-20-04A	31 March 2005	Critical-item control

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

ECSS Secretariat ESA ESTEC (TEC-QR) P.O. Box 299 2200 AG Noordwijk The Netherlands	Phone: +31-71-565-3952 Fax: +31-71-565-6839 e-mail: ECSS-Secretariat@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)