ECSS-Q-ST-10-04C
31 July 2008

Space product assurance

Critical-item control

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, 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.

This Standard has been prepared by the ECSS Executive Secretariat, endorsed by the Document and Discipline Focal points, and approved by the ECSS Technical Authority.

Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands
Copyright: 2008 © by the European Space Agency for the members of ECSS

Change log

ECSS-Q-20-04A 31 March 2005	First issue
ECSS-Q-20-04B	Never issued
ECSS-Q-ST-10-04C 31 July 2008	Main differences between ECSS-Q-20-04A (31 March 2005) and this version are: • Renumbering from ECSS-Q-20-04 to ECSS-Q-ST-10-04. • Clause "4 Objective of critical-item control" was moved to clause 4.1. • Clause "5.1 Critical-item control concept" moved to clause 4.2, whereas clause 5.1.2 was deleted since it is now covered by clause 5.2.1. • Clause "5.2 Critical-item control implementation" moved to clause 5.1. • Original requirements 5.3a to 5.3c have been deleted as discussed during the on-site meeting since they have to be incorporated in ECSS-Q-ST-10C. • Clause "6.1 Overview of the critical-item control process" moved to clause 5.2.1 and new requirement 5.2.1 was added as discussed during the on-site meeting. • Clauses 6.2 to 6.5 moved to clause 5.2 as clauses 5.2.2 to 5.2.5. • Original requirement 6.4.4c has been deleted as discussed during the on-site meeting since this requirement is redundant to the original requirement 6.4.3b (now: 5.2.4.2b). • Clause "6.6 Integration of CI control activities" is now summarised in clause 4.2.5. • Clause "6.6 Integration of CI control activities" and clause "7. Integration of critical-item control into the project life cycle" moved to clause 5.3 (done during on-site meeting). • DRD for critical-item list as new Annex A added. • Original Annex A was moved to Annex A.2.2 as discussed during the on-site meeting.

Table of contents

Figures

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 Standard provides the requirements for the implementation of the critical-item control process as described in ECSS-Q-ST-10.

1
Scope

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

Clause 4 is the informative part of this Standard whereas clause 5 and Annex A form the normative part.

This standard may be tailored for the specific characteristics and constraints of a space project, in accordance with ECSS-S-ST-00.

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-S-ST-00-01	ECSS system – Glossary of terms

3
Terms, definitions and abbreviated terms

3.1 Terms defined in other standards

For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply, in particular for the following terms:

critical item

3.2 Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
CI	critical item
CIL	critical-item list
PMP	parts, materials and processes
SPF	single-point failure

4
Overview of the critical-item control process

4.1 General

The objectives of the critical-item control process 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.

4.2 Critical-item control process

4.2.1 Critical items and critical-item control

Critical items are potential threats to the performance, quality, dependability and safety of a system that are controlled by a specific action plan in order to mitigate emanating risks and to prevent undesirable consequences.

4.2.2 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 are 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 4-1):

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

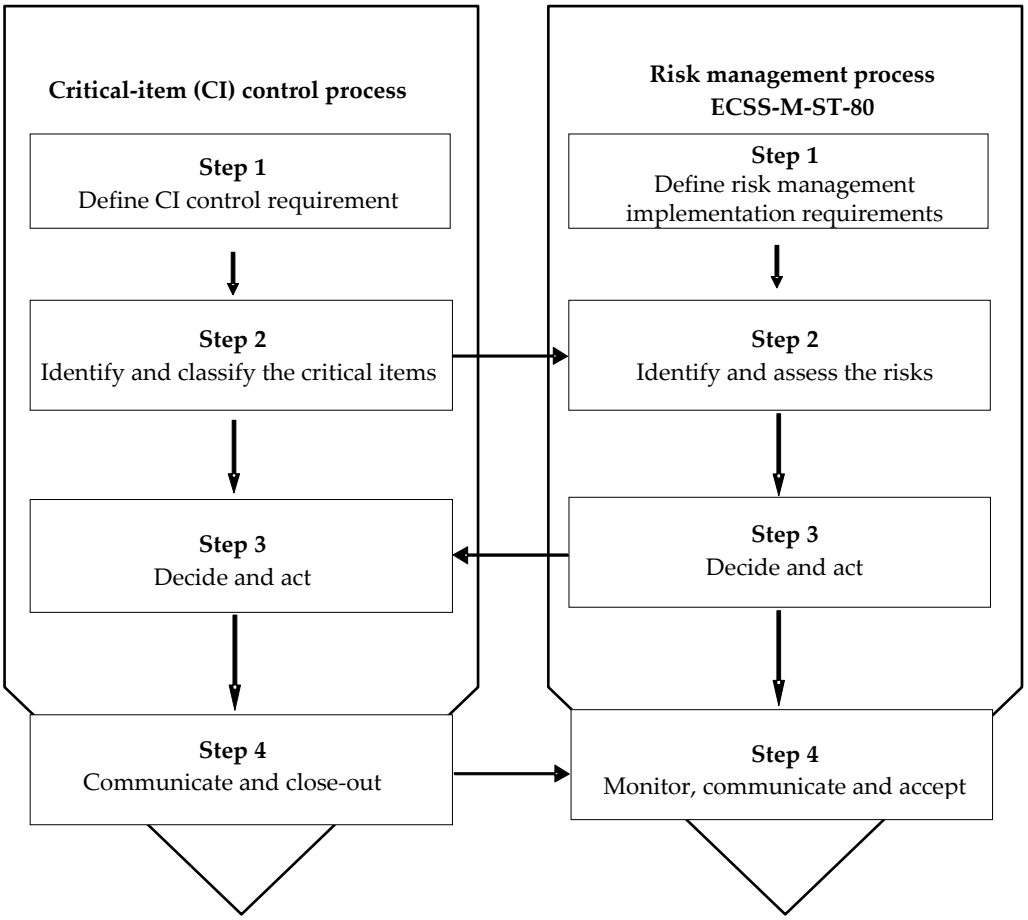

Figure 4-1: Critical-item control process, and its relation to the risk management process

4.2.3 Interfaces between critical-item control and product assurance

Critical-item control is part of the product assurance 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).

4.2.4 Interfaces between critical-item control and product engineering

Critical-item control requirements affect both the specification of a product and the realisation of the product. Therefore, the inputs and the outputs of the engineering process (e.g. technical specifications, and design documents) are 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 are agreed with engineering.

4.2.5 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 CIL evolves throughout the project life cycle starting with a preliminary CIL at PDR.

5
Requirements

5.1 Critical-item control process

5.1.1 General requirements

a. The supplier shall uniquely identify critical items.

b. The supplier shall classify critical items according to the nature of their criticality.

c. The supplier shall establish and maintain the critical-item list (CIL) for the project throughout all the project phases to allow the tracking and monitoring of all the critical items identified, in conformance with Annex A.

d. The supplier shall define specific control measures for the critical items.

e. The supplier shall define evaluation points for assessing the implementation of critical-item control measures.

f. At each evaluation point, the supplier shall evaluate the need to retain each item in the critical-item list.

g. The supplier shall report the status of the critical items and of the related control measures as part of the project progress reporting and at milestone reviews.

h. The supplier shall reduce the criticality of an item either by design or by procedural means.

NOTE A critical item for which the associated risk is controlled by means of procedures receives particular attention in the further processing of the item.

i. The supplier shall list all design, manufacturing, and test documentation related to critical items in the CIL.

NOTE Document traceability is maintained by document number and issue.

j. The supplier shall monitor manufacturing, assembly, integration, testing, maintenance and operation involving a critical item for problems that can affect the performance of the item during the operational phase.

5.2 Implementation requirements

5.2.1 General

a. The supplier shall implement the critical-item control process as shown in Figure 5-1.

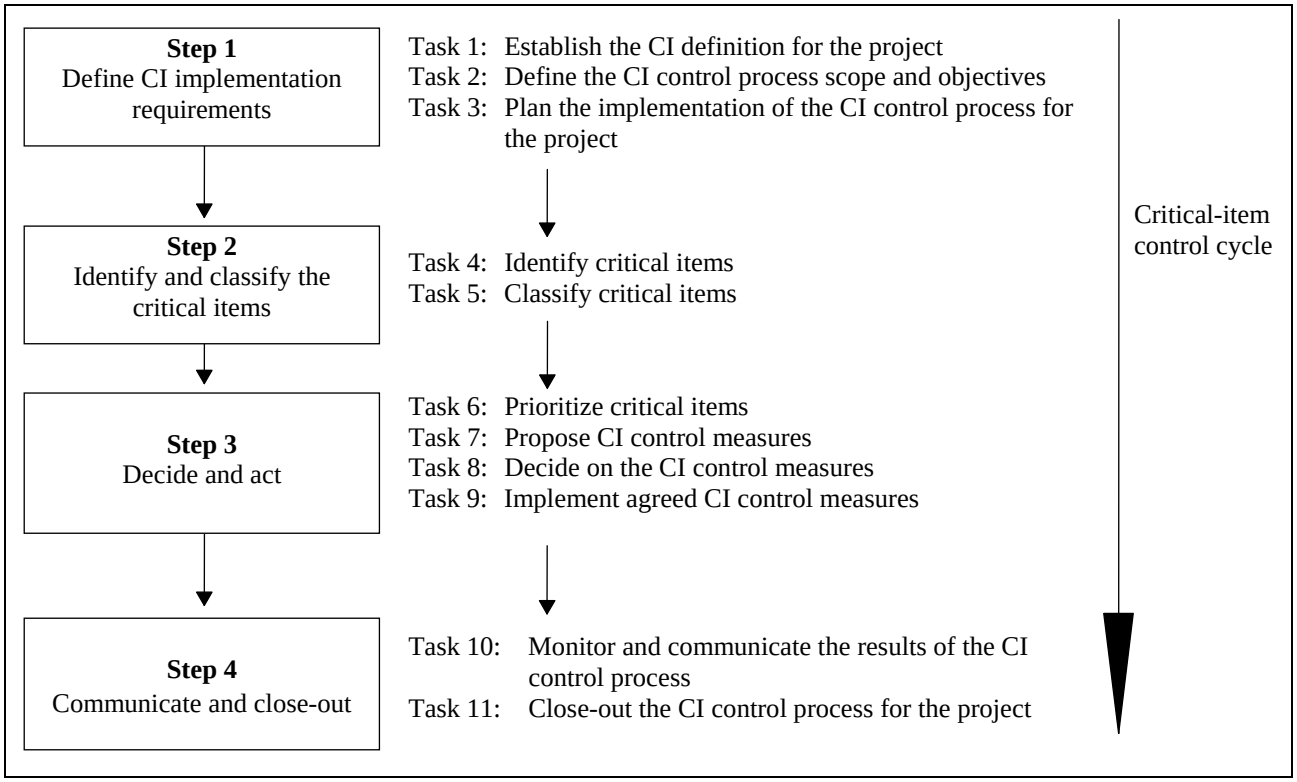

Figure 5-1: Tasks associated with the 4-step approach of the CI control process

5.2.2 Step 1: Define CI control requirement

5.2.2.1 Task 1: Establish the CI definition for the project

a. The supplier shall identify the applicable requirements for CI control and document the implementation approach chosen in the project's Product Assurance Plan

b. The supplier shall establish the CI classification criteria.

c. The supplier shall 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.

NOTE Risk ranking is provided in ECSS-M-ST-80.

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

a. The supplier shall define the purpose and application boundaries of CI control in the critical-item control plan.

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

a. The supplier shall assign the responsibility for CI control management, in accordance with the product assurance plan.

b. The supplier shall specify forms and the CI control programme documentation.

NOTE Examples of CI control forms are provided in Annex B.

c. The supplier shall describe the flow of activities (process) within the project.

NOTE Activities can be: review, documentation preparation and approval.

5.2.3 Step 2: Identify and classify the critical items

5.2.3.1 Task 4: Identify critical items

a. The supplier shall identify critical items within his project in accordance with the project's documentation and CI definition.

NOTE 1 Project documentation like design and engineering documents and supplier inputs.

NOTE 2 Check-list for potential critical items is provided in Annex C.

b. For each critical item the supplier shall identify its nature of criticality.

c. The supplier shall list each critical item in the CIL in conformance to Annex A.

NOTE The supplier can describe critical items in the associated critical-item control form as per Annex B.

5.2.3.2 Task 5: Classify critical items

a. The supplier shall classify the critical items according to the criticality category defined in 5.2.2.1b.

5.2.4 Step 3: Decide and act

5.2.4.1 Task 6: Prioritise critical items

a. The supplier shall identify the inputs from the risk management process and shall apply the ranking criteria for critical items as defined in 5.2.2.1c.

b. The supplier shall prioritise the actions on the control of critical items.

5.2.4.2 Task 7: Propose CI control measures

a. The supplier shall identify means by which critical items can be controlled.

NOTE 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. The supplier shall determine verification means regarding the implementation of the CI control measures.

c. The supplier shall identify methods for the implementation of these measures and assess the feasibility of their application.

5.2.4.3 Task 8: Decide on the CI control measures

a. The supplier shall evaluate and assess the CI control measures and implementation methods with respect to their effectiveness and feasibility by:

1. Selecting the CI control measures and implementation methods.
2. Defining a CI control strategy by prioritising the implementation of CI control.
3. Assessing the impact of CI control on project resources including risks during the associated decision making and selection process.
4. Assessing the impact of the implementation of CI control measures on the acceptability of risks associated with the critical items.

b. The supplier shall define success criteria for the implementation of CI control.

5.2.4.4 Task 9: Implement agreed CI control measures

a. The supplier shall implement the CI control strategy by applying the selected implementation methods.

b. The supplier shall verify the implementation of CI control through application of the verification means.

c. The supplier shall apply the success criteria to demonstrate successful implementation and to identify areas of non-successful implementation, i.e. non-successfully controlled critical items.

d. The supplier shall iterate task 7 (requirements 5.2.4.2a to 5.2.4.2c) and task 8 (requirements 5.2.4.3a to 5.2.4.3b) for non-successfully controlled critical items until they become successfully controlled or - if failing to do so - request disposition by higher management.

5.2.5 Step 4: Communicate and close-out

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

a. The supplier shall assess and review all critical items periodically for status.

b. The supplier shall assess critical items and associated control measures when affected by nonconformances, anomalies (test and operation), problems and incidents.

c. The supplier shall identify new critical items or changes to conditions under which critical items were previously evaluated.

d. The supplier shall identify and communicate the evolution of CI status over the project evolution.

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

a. The supplier shall submit the completed CIL for formal acceptance by the next higher level project management.

b. The supplier shall assess periodically the performance of the CI control processes and implement improvement of the effectiveness based on experience with project progress.

5.3 Integration of CI control activities

5.3.1 Consolidation and gathering method

a. The top down approach from the system to lower level shall be used to identify the required lower level inputs.

NOTE 1 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.

NOTE 2 Those inputs are linked to knowledge of the domain.

b. The bottom-up approach from lower level to system level tasks shall be used for the integration of lower results.

NOTE 1 This bottom-up approach integrates logically and effectively the lower level inputs into the system level activities.

NOTE 2 Top down and bottom-up approaches assists in achieving the following results:

- proper allocation of the ranking scheme at the system level where applicable;
- proper development and implementation of CI control;

- identification of the not yet dispositioned items in a timely manner;
- assurance that all aspects relevant to the CI control are systematically considered.

NOTE 3 Further recommendations for the integration of CI control into the project life cycle are given in the subsequent clauses.

5.3.2 Preliminary design review (PDR)

a. At PDR, the CIL shall cover 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).

NOTE 1 In addition, the preliminary CIL includes a list of recommendations for the elimination of de-sign deficiencies by redesign in the detailed design phase.

NOTE 2 In this phase, the preliminary CIL is used as a mean to present the nonconforming designs to the programme management for initial evaluation and determination of the subsequent course of action.

5.3.3 Critical design review (CDR)

a. During the CDR the CIL shall be subject to evaluation.

NOTE 1 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 are candidates for redesign.

NOTE 2 As per the PDR, during this phase the CIL continues to include and document all the critical items identified in the different system analyses.

NOTE 3 At this point in the programme, the CIL is used to address all the nonconforming designs to the programme management for formal evaluation and decision (i.e. acceptance or redesign).

b. 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.

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

5.3.4 Acceptance review (AR)

a. Prior to AR, the supplier shall develop the closeout documentation for all critical items.

b. When the customer has agreed that no design change is implemented for a critical item, the closeout documentation shall contain the retention rationale.

c. After implementation of design change, the supplier shall update the CIL to reflect the new configuration status and the affected critical item shall be closed within the CIL.

d. From the end of the CDR up to the conclusion of the AR, the supplier shall include the status of the CIL open items in the PA progress report.

e. At the end of the AR, the supplier shall verify the action closure for open critical items and shall provide it for customer approval.

Annex A (normative)
Critical-item list - DRD

A.1 DRD identification

A.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-10-04, requirements 5.1.1c and 5.2.3.1c

A.1.2 Purpose and objective

The purpose of this list is to summarise all critical items.

A.2 Expected response

A.2.1 Contents

<1> Number

a. This list shall uniquely identify the critical item.

<2> Critical item

a. This list shall identify the critical item.

NOTE A critical item can be a unit, subsystem, equipment, component, material, process, and function.

<3> Risks associated

a. This list shall contain the technical risk(s) associated with the critical item.

NOTE This can be a reference to the associated entry in the Risk Register.

<4> Document reference

a. This list shall contain a reference to the document in which the item is identified as critical.

b. This list shall further contain a reference to the design, manufacturing and test documentation related to the critical item.

<5> Criticality level

a. This list shall include the criticality level of the critical item in accordance with the critical item classification as defined in clause 5.2.3.

<6> Cause

a. This list shall contain the description of the cause which makes this item critical.

<7> Control activities

a. This list shall contain planned activities to reduce or control the risk as defined in 5.2.4.2.

b. This list shall contain the statement of verification of the control implementation as defined in 5.2.4.2.

<8> Due date

a. The list shall show the expected completion date of the control activities.

<9> Status

a. The list shall provide the status of action as “Open” or “Closed”.

b. In case of closed action, the list shall provide the reference to the close-out document.

A.2.2 Special remarks

The supplier can use the following template:

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 clause 5.2.3
Cause	Description of the cause which makes this item critical.
Control activities	(Refer to clause 5.2.4.2 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.)

Annex B (informative)
Critical-item control form

Figure B- 1 and Figure B- 2 are examples of critical-item control forms.

<table>
<tr><td colspan="3">Critical-item identification</td><td colspan="3">CI no.</td></tr>
<tr><td colspan="6">Subsystem:
Equipment:
Item:
Function:</td></tr>
<tr><td colspan="6">Title:</td></tr>
<tr><td colspan="6">Mission phase:</td></tr>
<tr><td colspan="6">Description of event (related to the critical item):</td></tr>
<tr><td colspan="6">Effects/risks at: - Product level:
- Subsystem level:
- System level:</td></tr>
<tr><td colspan="6">Possible causes:</td></tr>
<tr><td colspan="6">Problem identification reference:</td></tr>
<tr><td colspan="3">Severity category:
Single-point failure (Yes/No):
Propagation time:</td><td colspan="3">Likelihood category:
Detectability (Yes/No):</td></tr>
<tr><td colspan="6">Applicable requirements:</td></tr>
<tr><td rowspan="2">Item is confirmed critical by</td><td>Discipline</td><td>PA</td><td>Engineering</td><td>Project manager</td></tr>
<tr><td>Name:
Date:
Signature:</td><td></td><td></td><td></td></tr>
</table>

Figure B- 1 Example of a critical–item identification list (CIL form)

<table>
<tr><td colspan="4">Critical-item control sheet</td><td colspan="2">Sheet No.</td></tr>
<tr><td colspan="6">Measures proposed:</td></tr>
<tr><td>Measures adopted:</td><td colspan="2">a) Specification
d) Inspection procedures</td><td colspan="2">b) Design/definition
e) Operational procedures</td><td>c) Tests
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="6">Effectiveness/rationale for retention/close-out documents:</td></tr>
</table>

Figure B- 2 Example of a critical–item control sheet

Annex C (informative)
Check-list for potential critical items

C.1 Examples of critical items

- An item is critical if it is not qualified or validated for the application in question (or has caused problems previously which remained unresolved).
- An item is critical if it is difficult to demonstrate design performance.
- An item is critical if it is highly sensitive to the conditions under which it is produced or used (e.g. contamination, radiation).
- 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.
- 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.
- EE 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.
- 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 with respect to 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 utilisation.
- 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 minimise 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 the following:

- 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 saving, 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.

Bibliography

ECSS-S-ST-00	ECSS system — Description, implementation and general requirements
ECSS-M-ST-80	Space project management — Risk management
ECSS-Q-ST-10	Space product assurance — Product assurance management