ECSS-Q-ST-30-02C
6 March 2009

Space product assurance

Failure modes, effects (and criticality) analysis (FMEA/FMECA)

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-Q-ST-30-02 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

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

Change log

ECSS-Q-30-02A 7 September 2001	First issue
ECSS-Q-30-02B	Never issued
ECSS-Q-ST-30-02C 6 March 2009	Second issue The main changes between ECSS-Q-30-02 A and the current version are the following: • General re-structuring of the standard, as follows: ▪ Clause on design requirements has been subdivided in four, to include dedicated clauses to FMEA, FMECA, Implementation and HSIA. ▪ Requirements on the content of deliverable documents have been moved to DRDs (normative annexes A to F). ▪ A new informative annex (Annex G) has been included as an example of a comprehensive list of part failure modes per family/group of component. ▪ Descriptive and orientation material has been separated from the normative material and moved either into NOTES, or to informative annexes H (Product design failure modes check list) and I (HSIA check list). • Normative text has been re-written to conform the ECSS drafting rules, and in particular to: ▪ Organize requirements such that they specify single needs, and are individually identified. ▪ Express requirements in such a way that they are verifiable and able to be used in business agreements by identifying the corresponding actor (customer/supplier). ▪ Be clear and avoid ambiguity and verbosity, to better specify the standard practices in a more direct and accurate way. • Introduction has been expanded to better explain the objectives of FMEA/FMECA. • More detail explanation of the applicability to complex integrated circuits, and to software, has been included in the Scope. • Missing definitions have been added in Clause 3. • Severity of consequences (Table 4-1) has been fully aligned with the corresponding ones in ECSS-Q-ST-30 “Dependability” and ECSS-Q-ST-40 “Safety”.

Table of contents

Figures

Tables

Introduction

The Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects, and Criticality Analysis (FMECA) are performed to systematically identify potential failures in:

— products (functional and hardware FMEA/FMECA);

— or processes (process FMECA)

and to assess their effects in order to define mitigation actions, starting with the highest-priority ones related to failures having the most critical consequences. The failure modes identified through the Failure Mode and Effect Analysis (FMEA) are classified according to the severity of their consequences. The Failure Mode, Effects, and Criticality Analysis (FMECA) is an extension of FMEA, in which the failure modes are classified according to their criticality, i.e. the combined measure of the severity of a failure mode and its probability of occurrence.

The FMEA/FMECA is basically a bottom-up analysis considering each single elementary failure mode and assessing its effects up to the boundary of the product or process under analysis. The FMEA/FMECA methodology is not adapted to assess combination of failures within a product or a process.

The FMEA/FMECA, is an effective tool in the decision making process, provided it is a timely and iterative activity. Late implementation or restricted application of the FMEA/FMECA dramatically limits its use as an active tool for improving the design or process.

Initiation of the FMEA/FMECA is actioned as soon as preliminary information is available at high level and extended to lower levels as more details are available. The integration of analyses performed at different levels is addressed in a specific clause of this Standard.

The level of the analysis applies to the level at which the failure effects are assessed. In general a FMEA/FMECA need not be performed below the level necessary to identify critical items and requirements for design improvements. Therefore a decision on the most appropriate level is dependent upon the requirements of the individual programme.

The FMEA/FMECA of complex systems is usually performed by using the functional approach followed by the hardware approach when design information on major system blocks become available. These preliminary analyses are carried out with no or minor inputs from lower level FMEAs/FMECAs and provide outputs to be passed to lower level analysts. After performing the required lower level FMEAs/FMECAs, their integration leads to the updating and refinement of the system FMEA/FMECA in an iterative manner.

The Software (S/W) is analysed only using the functional approach (functional FMEA/FMECA) at all levels.

The analysis of S/W reactions to Hardware (H/W) failures is the subject of a specific activity, the Hardware-Software Interaction Analysis (HSIA).

When any design or process changes are made, the FMEA/FMECA is updated and the effects of new failure modes introduced by the changes are carefully assessed.

Although the FMEA/FMECA is primarily a reliability task, it provides information and support to safety, maintainability, logistics, test and maintenance planning, and failure detection, isolation and recovery (FDIR) design.

The use of FMEA/FMECA results by several disciplines assures consistency and avoids the proliferation of requirements and the duplication of effort within the same programme.

1
Scope

This Standard is part of a series of ECSS Standards belonging to the ECSS-Q-ST-30 "Space product assurance - Dependability".

This Standard defines the principles and requirements to be adhered to with regard to failure modes, effects (and criticality) analysis (FMEA/FMECA) implementations in all elements of space projects in order to meet the mission performance requirements as well as the dependability and safety objectives, taking into account the environmental conditions.

This Standard defines requirements and procedures for performing a FMEA/FMECA.

This Standard applies to all elements of space projects where FMEA/FMECA is part of the dependability programme.

Complex integrated circuits, including Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs), and software are analysed using the functional approach. Software reactions to hardware failures are addressed by the Hardware-Software Interaction Analysis (HSIA).

Human errors are addressed in the process FMECA. Human errors may also be considered in the performance of a functional FMEA/FMECA.

The extent of the effort and the sophistication of the approach used in the FMEA/FMECA depend upon the requirements of a specific programme and should be tailored on a case by case basis.

The approach is determined in accordance with the priorities and ranking afforded to the functions of a design (including operations) by risk analyses performed in accordance with ECSS-M-ST-80, beginning during the conceptual phase and repeated throughout the programme. Areas of greater risk, in accordance with the programme risk policy, should be selectively targeted for detailed analysis. This is addressed in the RAMS and risk management plans.

This standard may be tailored for the specific characteristic and constrains of a space project in conformance 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 revision 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 more 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
ECSS-E-ST-32-02	Space engineering – Structural design and verification of pressurized hardware
ECSS-Q-ST-10-09	Space product assurance – Nonconformance control system
ECSS-Q-ST-30	Space product assurance – Dependability

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply.

For the purpose of this Standard, the following term from ECSS-E-ST-32-02 applies:

leak-before-burst

3.2 Terms specific to the present standard

3.2.1 active redundancy

redundancy wherein all means for performing a required function are intended to operate simultaneously

[IEC 60050-191]

3.2.2 area analysis

study of man-product or man-machine interfaces with respect to the area where the work is performed

3.2.3 criticality

combined measure of the severity of a failure mode and its probability of occurrence

3.2.4 end effect

consequence of an assumed item failure mode on the operation, function , or status of the product under investigation and its interfaces

3.2.5 failure cause

presumed causes associated to a given failure mode

3.2.6 failure effect

consequence of an assumed item failure mode on the operation, function , or status of the item

3.2.7 failure propagation

physical or logical event caused by failure within a product which can lead to failure(s) of products outside the boundaries of the product under analysis

3.2.8 failure mode and effects analysis (FMEA)

analysis by which each potential failure mode in a product (or function or process) is analysed to determine its effects.

NOTE The potential failure modes are classified according to their severity.

[IEC 60050-191]

3.2.9 failure mode, effects and criticality analysis (FMECA)

FMEA extended to classify potential failure modes according to their criticality

[IEC 60050-191]

3.2.10 functional description

narrative description of the product functions, and of each lower level function considered in the analysis, to a depth sufficient to provide an understanding of the product and of the analysis

NOTE Functional representations (such as functional trees, functional block diagrams and functional matrices) are included of all functional assemblies to a level consistent with the depth of the analysis and the design maturity.

3.2.11 functional FMEA

FMEA in which the functions, rather than the items used in their implementation, are analysed

3.2.12 functional FMECA

FMECA in which the functions, rather than the items used in their implementation, are analysed

3.2.13 hardware FMEA

FMEA in which the hardware used in the implementation of the product functions is analysed

3.2.14 hardware FMECA

FMECA in which the hardware used in the implementation of the product functions is analysed

3.2.15 hardware-software interaction analysis

analysis to verify that the software is specified to react to hardware failures as required

3.2.16 process FMECA

FMECA in which the processes are analysed, including the effects of their potential failures

NOTE Processes such as manufacturing, assembling and integration, pre-launch operations.

3.2.17 protection device

device designated to perform a specific protective function

[adapted from "protection equipment" in IEC 60050 191]

3.3 Abbreviated terms

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

Abbreviation	Meaning
ASIC	application specific integrated circuit
CDR	critical design review
CIDL	configuration item data list
CIL	critical item list
CN	criticality number
DN	detection number
EEE	electronic, electrical, electromechanical
FDIR	failure detection, isolation and recovery
FESL	failure effect severity list
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FPGA	field programmable gate array
HSIA	hardware-software interaction analysis
H/W	hardware
PCB	printed circuit board
PN	probability (of occurrence) number
RAMS	reliability, availability, maintainability and safety
RB	requirements baseline
RBD	reliability block diagram
SEP	single event phenomena
SN	severity number
SOW	statement of work
S/W	software
TS	technical specification

4
FMEA requirements

4.1 General requirements

a. The FMEA shall be initiated for each design phase as indicated in clause 6 and updated to reflect design changes along the project life cycle.

NOTE The FMEA is an integral part of the design process as one tool to drive the design along the project life cycle.

b. The FMEA shall be used for the development of the product architecture, design justification and for the definition of test and operation procedures.

c. The FMEA shall be used for the identification of critical items.

NOTE 1 Refer to clause 4.3 for the identification of critical item.

NOTE 2 For each critical item the FMEA identifies recommendations for risk reduction if appropriate.

d. The FMEA shall be used in the definition of:

1. failure tolerance design provisions (i.e. redundancy, inhibits, FDIR),
2. special test considerations,
3. maintenance actions (preventive or corrective),
4. operational constraints.

e. All recommendations which result from the FMEA shall be evaluated, dispositioned and documented as part of the Dependability Recommendations in conformance with ECSS-Q-ST-30, clause 5.7)

f. The FMEA shall be performed according the following steps:

1. Describe the product (i.e. function or hardware) to be analysed, by providing:
   (a) functional descriptions,
   (b) interfaces,
   (c) interrelationships and interdependencies of the items which constitute the product,

(d) operational modes,

(e) mission phases.

NOTE The functional analysis, functional block diagram and reliability block diagram can be used as input for product definition.

2. Identify all potential failure modes for each item and investigate their effect on the item under analysis and on the product and operation to be studied.

3. Assume that each single item failure is the only failure in the product.

NOTE This implies that combination of failures are not considered.

4. Evaluate each failure mode in terms of the worst potential consequences and assign a severity category.

5. Identify failure detection methods.

6. Identify existing preventive or compensating provisions for each failure mode.

7. Provide for identified critical items (clause 4.3) corrective design or other actions (such as operator actions) necessary to eliminate the failure or to mitigate or to control the risk.

8. Document the analysis and summarize the results and the problems that cannot be solved by the corrective actions.

9. Record all critical items into a dedicated table as an input to the overall project critical item list (CIL).

NOTE Critical item control is described in ECSS-Q-ST-10-04.

4.2 Severity categories

a. A severity category classification, based on failure consequences, shall be assigned to each identified failure mode.

b. Severity categories shall be assigned without consideration of existing compensating provisions.

NOTE 1 The compensating provision is highlighted by the suffix.

NOTE 2 The objective is to provide a qualitative measure of the worst potential consequences resulting from item failure.

c. For analyses lower than system level the severity level due to possible failure propagation shall be identified as level 1 for dependability.

NOTE For example, for analysis at subsystem and equipment levels.

d. The number identifying the severity category shall be followed by a dedicated suffix as follows:

1. the suffix SH to indicate safety hazards;
2. the suffix R to indicate redundancy;
3. the suffix SP to indicate single point failures.

NOTE 1 For example, while 3SP indicates that the item failure mode under consideration can lead to the consequences listed in category 3, 3R indicates that the consequences listed in category 3 can occur only after the failure of all of the redundant items.

NOTE 2 The suffix SH is used before the other suffixes.

e. The severity categories shall be applied as indicated in Table 4-1.

NOTE The customer can tailor the severity categories to suit the programme specific needs.

Table 4-1: Severity of consequences

Severity category	Severity level	Description of consequences (failure effects)	
		Dependability effects (as specified in ECSS-Q-ST-30)	**Safety effects (as specified in ECSS-Q-ST-40)**
Catastrophic	1	Failure propagation (refer to 4.2c)	Loss of life, life-threatening or permanently disabling injury or occupational illness.
			Loss of an interfacing manned flight system.
			Severe detrimental environmental effects.
			Loss of launch site facilities.
			Loss of system.
Critical	2	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness.
			Major detrimental environmental effects.
			Major damage to public or private properties.
			Major damage to interfacing flight systems.
			Major damage to ground facilities.
Major	3	Major mission degradation	
Minor or Negligible	4	Minor mission degradation or any other effect	

f. The customer shall define the criteria for mission loss and mission degradation (major and minor).

NOTE 1 Example of such criteria is loss of one or more essential mission objectives.

NOTE 2 For analyses performed at subsystem, assembly or equipment level, the term "mission" is understood as functionality (i.e. the capability of meeting the specification requirements).

4.3 Identification of critical items

a. An item shall be considered a critical item if:

1. a failure mode is identified as single-point failure together with at least a failure consequence severity classified as catastrophic, critical or major, or

2. a failure mode has failure consequences classified as catastrophic.

NOTE The customer can tailor the criteria for critical item identification defining a failure mode as critical according to programme specific needs.

4.4 Level of analysis

a. The supplier shall analyse all failure modes leading to consequences with severity level 1, 2 and 3 down to a level allowing identifying all single point failures.

NOTE Different level of analysis to which failure modes are assessed can be agreed between the customer and the supplier.

b. The analysis shall provide failure effects on interfaces empathizing propagation of failure effects to redundant, cross-strapped, or interfacing assemblies.

c. For electronic equipment the FMEA shall include the analysis of part failure modes on interface circuitries.

NOTE A list of part failure modes is provided in Annex G.

4.5 Integration requirements

a. FMEAs of each level shall be integrated into their associated FMEA performed at one level higher.

b. The customer shall specify to the supplier the critical failure conditions (failure modes at customer level) which need to be focused on in the analyses at the level of the supplier.

c. In his FMEA, the supplier shall use the critical failure conditions identified by his customer as failure effects, when provided.

d. End effects identified by FMEA of each level shall become failure modes of their associated FMEA performed at one level higher.

e. Failure modes identified by FMEA of each level shall become failure causes of their associated FMEA performed at one level higher.

f. Additional failure modes shall be introduced at any level if missing (as failure effects) from lower level FMEAs.

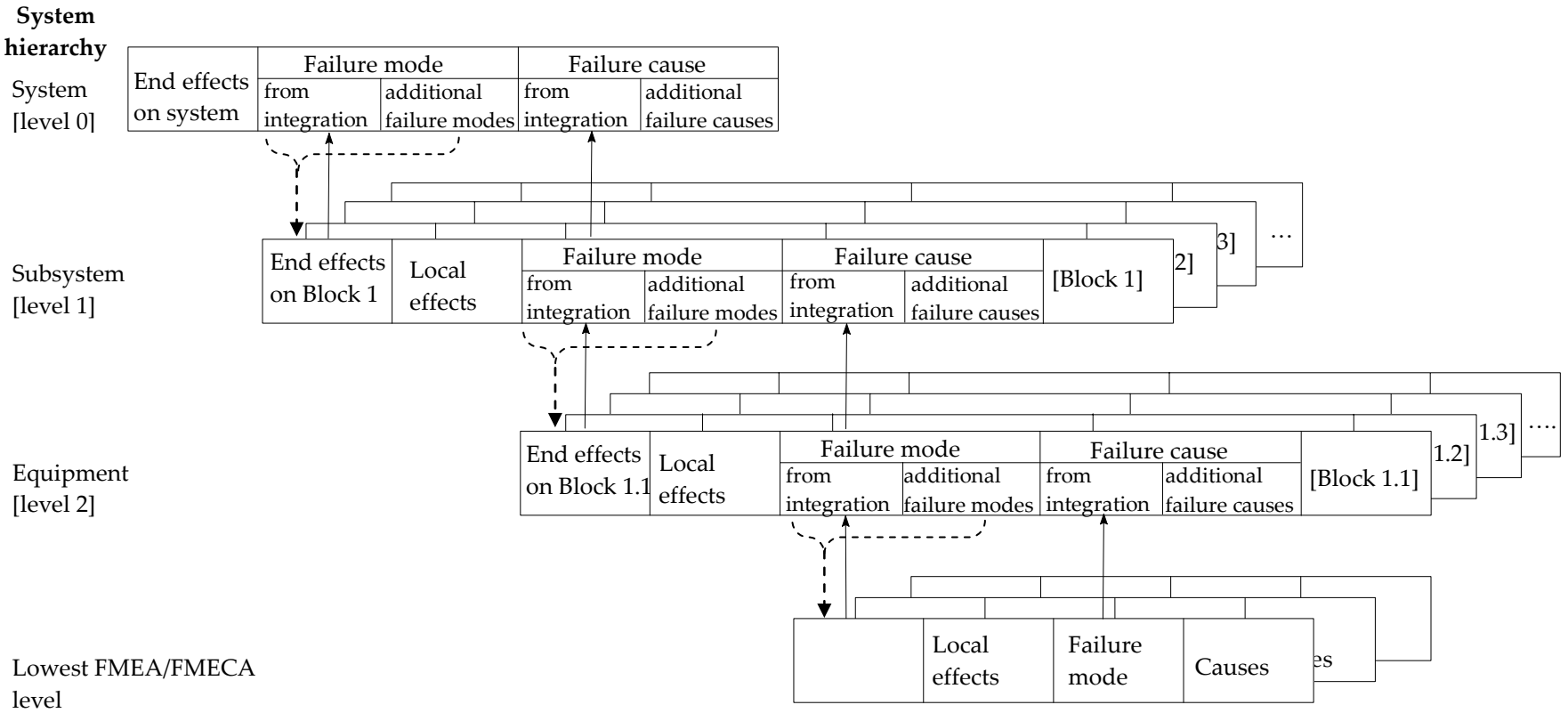
g. At any level, additional failure causes, which can not be assessed at lower level as failure modes, shall be introduced into the FMEA.

NOTE Additional failures can be induced by physical layout or accommodation.

h. The effect of operational and failure behaviour of specific parts or equipment on other parts or equipment shall be assessed with regard to the physical layout of their mechanical, electrical and thermal interface.

NOTE 1 Examples of effects are temperature, vibration, movement, power demand and heat flow.

NOTE 2 A graphical representations of requirements 4.5a to 4.5h is given in Figure 4-1.



Dotted arrows present the flow down of critical failure conditions from upper level to lower level (see requirements 4.5b and 4.5c),

Line arrows present the bottom-up failure analysis integration process (see requirements 4.5a, 4.5d, 4.5e)

Figure 4-1: Graphical representation of integration requirements

4.6 Detailed requirements

a. All mission phases and related operational modes (including "safe mode"), unless otherwise agreed with the customer, shall be addressed by the FMEA.

b. The failure effects resulting from each failure mode shall be determined at the level of the item under investigation (local effect) and at the level of the product under analysis (end effect).

c. Failure modes that can propagate to interfacing functions, elements or functions and elements shall be identified.

d. The analysis shall indicate how each failure mode can be detected.

NOTE At a given level of analysis not all detection means and observable symptoms can be known. In the upper level analysis, the list of available detection means and observable symptoms is then completed.

e. Complex integrated circuits, including Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs), shall be analysed using the functional approach (functional FMEA).

NOTE Failures induced by physical layout or accommodation are considered for the complex integrated circuit.

f. At all levels S/W shall be analysed using only the functional approach (functional FMEA).

g. Software reactions to hardware failures shall be analysed by the Hardware-Software Interaction Analysis (HSIA) as specified in clause 7.

h. If requested by the customer and when human performance is a significant contributor to mission success or safety possible human errors shall be highlighted and documented.

NOTE 1 The FMEA should invoke the requirement for the performance of a human error effects analysis and a task analysis.

NOTE 2 Requirement 4.6h is generally applied to manned systems.

i. Failures requiring failure detection and recovery action in a time interval greater than the time to an irreversible consequence shall be identified and subjected to recommendation for corrective action.

j. For electromechanical and electrical equipment, assembly or subsystem additional product design aspects shall include:

1. failure modes resulting from the location of the components, causing failure propagation due to components being mounted too close to each other;

NOTE The location of the components is considered for external failure propagation or internal failure propagation in case of internal redundancy.

2. failure modes resulting from multi-application of individual components;

NOTE Example of multi-applications is the use of one integrated circuit for two redundant paths.

3. failure of grounding or shielding or insulation.

NOTE Annex H gives examples of check-list items for electromechanical and electrical equipment, assembly or subsystem.

4.7 FMEA report

a. The results of the FMEA shall be documented in a FMEA report in conformance with the DRD in Annex A.

5
FMECA requirements

5.1 General requirements

a. The customer shall determine the applicability of the FMECA requirements according to the specific project characteristics.

NOTE 1 The FMECA is a FMEA extended to classify potential failure modes according to their criticality, i.e. the combined measure of the severity of failure modes and their probability of occurrence.

NOTE 2 Typically FMECA is not performed for Telecommunication, Earth Observation & Scientific Spacecrafts and for ground segments.

b. All requirements reported in clause 4 shall apply with the exception of clause 4.3.

NOTE The acronym FMECA replaces FMEA.

5.2 Criticality ranking

a. The criticality number (CN) for a specific failure mode shall be derived from the severity of the failure effects and the probability of the failure mode occurrence.

b. A severity number (SN) shall be given to each assumed failure mode.

NOTE The existence of redundancy does not affect the severity classification and therefore relevant severity number. The highest numbers indicates the most severe categories.

c. The SNs shown in Table 5-1 shall be used.

Table 5-1: Severity Numbers (SN) applied at the different severity categories with associated severity level

Severity level	Severity category	SN
1	Catastrophic	4
2	Critical	3
3	Major	2
4	Negligible	1

d. An assessment of the probability of occurrence of the assumed failure mode during the specific mission shall be made.

NOTE In case of redundancy, the probability of failure of all redundant items is assessed with the support of the reliability analysis. The approach used for the assessment can be either qualitative or quantitative.

e. The qualitative approach based on engineering judgment shall be used if specific failure rate data are not available.

f. Failure mode probabilities of occurrence shall be grouped into defined levels which establish the qualitative failure probability level for entry into the FMECA worksheet column.

g. The probability levels and limits shall be approved by the customer.

h. Each level shall be identified by a probability number (PN).

NOTE 1 The probability of occurrence levels, limits of the levels and relevant PNs are shown in Table 5-2 as an example.

NOTE 2 The customer can tailor the probability levels to the individual programme through specific requirements and allocate the probability limits to the lower levels.

Table 5-2: Example of probability levels, limits and numbers

Level	Limits	PN
Probable	$P > 1E\text{-}1$	4
Occasional	$1E\text{-}3 < P \leq 1E\text{-}1$	3
Remote	$1E\text{-}5 < P \leq 1E\text{-}3$	2
Extremely remote	$P \leq 1E\text{-}5$	1

i. The quantitative approach shall be used when specific failure rates and probability of occurrence data are available.

j. Data sources, approved by the customer, shall be listed.

k. The data sources shall be the same as those used for the other dependability analyses performed for the programme.

l. The failure probabilities shall be ranked as per Table 5-2 and relevant entry (the PN) listed in the FMECA worksheet column.

m. The CN for a specific failure mode shall be developed from the severity of the failure effects and the probability of the failure mode occurrence.

n. The CN shall be calculated as the product of the ranking assigned to each factor: CN = SN x PN.

o. Failure modes having a high CN shall be given a higher priority in the implementation of the corrective actions than those having a lower CN.

5.3 Identification of critical items

a. An item shall be considered a critical item if:

1. a failure mode has failure consequences classified as catastrophic, or

2. a failure mode is classified as CN greater or equal to 6 in conformance with Table 5-3.

NOTE The customer can tailor the criteria for critical item identification defining a failure mode as critical according to programme specific needs.

Table 5-3: Criticality matrix

Severity category	SNs	Probability level			
		10^{-5}	10^{-3}	10^{-1}	1
		PNs			
		1	2	3	4
catastrophic	4	4	8	12	16
critical	3	3	6	9	12
major	2	2	4	6	8
negligible	1	1	2	3	4

5.4 FMECA report

a. The results of the FMECA shall be documented in a FMECA report in conformance with the DRD in Annex A.

6
FMEA/FMECA implementation requirements

6.1 General requirements

a. Formal delivery of the FMEA/FMECA shall be in accordance with the SOW.

NOTE Generally the report is presented at all design reviews.

b. In each phase, the FMEA/FMECA shall be reviewed, updated and changes recorded on a continuous basis to maintain the analysis current with the design evolution.

NOTE For the project phase definition refer to ECSS-M-ST-10.

c. The means of recording the FMEA/FMECA shall be agreed by the customer.

6.2 Phase 0: Mission analysis or requirements identification

In this phase the FMEA/FMECA is, typically, not performed.

6.3 Phase A: Feasibility

a. The FMEA/FMECA shall assist the trade-off among the various possible design concepts by assessing their impact on the project dependability and safety requirements.

NOTE The analysis contributes to the overall risk evaluation of each design concept. The functional approach is generally used.

b. The FMEA/FMECA shall make use of, as a minimum, the following inputs:

1. the mission requirements, in particular the dependability and safety requirements;
2. the design documentation of the different product concepts identified in phase 0;

3. the hierarchical decomposition of the product functions.

NOTE The function decomposition is generally derived from the functional analysis.

c. The FMEA/FMECA shall be performed to provide the following results:

1. evaluation of the conformance of each design concept function to the system dependability and safety requirements;
2. identification of critical failure scenarios;
3. identification of needs of focused analyses;

NOTE For example: fault tree.

4. identification of the features to be implemented for each analysed function in order to meet the system dependability and safety requirements.

NOTE 1 Example of the identified features are: functional redundancies or inhibits, possible alternative implementations.

NOTE 2 A report for FMEA/FMECA is, typically, not required for phase A.

6.4 Phase B: Preliminary definition

a. The FMEA/FMECA shall be performed either according to the functional approach (functional FMEA/FMECA) or to the hardware approach (hardware FMEA/FMECA).

NOTE A list of part failure modes is provided in Annex G.

b. Rationale for selection of the approach shall be provided considering the following criteria:

1. available design data;
2. product complexity and level of integration;
3. criticality of the product or function;
4. segregation of function.

c. The FMEA/FMECA shall:

1. support the trade-offs from the dependability and safety point of view;
2. support the definition of the requirements to be implemented in the product as redundancies, inhibits, operations to be followed to avoid hazards or loss of mission, and others, such as fail-safe, leak before burst, and maximum time allowable before compensation activation.

d. The FMEA/FMECA shall make use of, as a minimum, the following inputs:

1. The mission requirements and the mission profile.

2. The product specification, considering in particular the dependability and safety requirements.

   NOTE Examples of product specifications are: system or subsystem specification and performance specification.

3. The current hierarchical decomposition of the product functions.

   NOTE The function decomposition is generally derived from the functional analysis.

4. The design of the product architecture.

   NOTE Examples of product architecture are: design description, drawings and interfaces description.

5. Available information from the product safety analyses relevant to hazard causes and controls.

6. When applicable, available information from maintenance analysis relevant to replaceable unit definition.

7. When available, FMEA/FMECAs performed at lower integration levels.

8. For lower level FMEA/FMECAs, agreed list of parts failure modes

9. For FMECA, item failure rates from data sources agreed by the customer.

e. The FMEA/FMECA shall provide the following results:

1. Inputs for dependability and safety requirements to be allocated for implementing the prevention and compensation methods and for minimizing the single point failures and the identified critical failure scenarios.

   NOTE The dependability and safety requirements are in priority allocated to the product and lower levels. Recommendation to higher levels can be raised too.

2. Input to safety analyses: identification of hazardous consequences due to failures at lower levels and relevant identified prevention and compensation methods.

3. When applicable, input to maintainability analyses.

   NOTE Example of the input is the identification of replaceable units for meeting the dependability and safety requirements.

4. Input to software criticality analysis.

   NOTE Example of the input is the identification of software functional failure consequences.

5. Input to the critical function list or critical item list.

   NOTE Example of these inputs is the identification of the critical items as defined in clause 4.3 or 5.3.

6. Inputs for developing the FDIR system.

7. For each hardware or function failure mode, the detection parameters that are generated following the occurrence of the failure as observable symptoms.

   NOTE Examples of observable symptoms are: warning signal, sensor information, equipment status and current and voltage monitors).

8. When available as design information, the precise monitor in terms of acquisition channel name.

9. The monitor lists, as input for the FDIR development.

   NOTE The objective is to allow the definition of algorithms, which detect any occurred failure in front of the registered detection signals.

f. Identification of failures requiring failure detection and recovery action in a time interval greater than the time to an irreversible consequence together with recommendation for corrective action.

   1. The propagation time (Tp) between the occurrence of the failure and the manifestation of the irreversible consequences

   2. Input to operation definition activity.

      NOTE An example of this input is the identification of crew and system operations to be implemented to prevent or control critical dependability and safety events.

g. The FMEA/FMECA report shall be issued according to the SOW.

6.5 Phase C: Detailed definition

a. The FMEA/FMECA shall be performed according to the hardware approach (hardware FMEA/FMECA).

   NOTE 1 In this phase the hardware can be uniquely identified from the engineering design data. In some cases the functional approach or a combination of the two approaches can be used (rationale for selection to be provided and agreed by the customer).

   NOTE 2 A list of part failure modes is provided in Annex G.

b. The FMEA/FMECA shall allow to verify that the design fulfil the dependability and safety requirements, allocated to all of the project levels (system, subsystem and lower levels) in phase B.

c. The FMEA/FMECA shall review all of the following inputs and use those applicable:

   1. The detailed mission and performance requirements and the environmental conditions.

2. The dependability and safety requirements from the technical specification.
3. The hierarchical decomposition of the product functions as derived from the updated functional analysis.
4. The detailed mission profile (definition of the mission phases or modes).
5. The detailed design architecture (design description, drawings, interfaces description).
6. The detailed description of hazard causes and hazard control implementation in the design architecture from the relevant safety analysis.
7. Definition of the Replaceable Units from the maintenance analysis.
8. FMEA/FMECAs performed at lower integration level.
9. For lower level FMEA/FMECAs, agreed list of parts failure modes.
10. For FMECA, item failure rates from data sources agreed by the customer.
11. Definition of the crew and product operations.
12. Definition of the embedded monitors available for discovering any anticipated failure mode and of the automatic sequences to react to any malfunction from the FDIR analysis.
13. Definition of the remote and man controlled (crew or ground operators) monitors available for discovering any anticipated failure mode and of the procedures to react to any malfunction from the FDIR analysis.

d. The FMEA/FMECA shall provide the following results:

1. Identification of the methods for preventing or compensating failure effects of critical items.

   NOTE Examples of these methods are: redundancies and inhibits.

2. Verification that the anticipated actions are able to prevent or control the consequences.
3. Identification of remaining single point failures and identification of compensating features if the elimination is not possible or impractical.
4. Input to safety analyses.

   NOTE An example of this input is the identification of the implemented preventing or compensating methods for each identified hazardous consequence.

5. Input to the critical function list or critical item list.

   NOTE An example of this input is the identification of the items (component or equipment) to be

considered critical according to the provided criticality definition.

6. Input to the FDIR system activity:

   (a) list of specific monitor parameters that allow the failure to be detected;

   (b) verification of the effectiveness of the recovery methods or proposal of alternative methods;

   (c) identification of failure modes that are not monitored.

7. Input to operation definition activity,

   NOTE Examples of these inputs are the identification of crew and system operations implemented to prevent or control critical dependability and safety events and verification of their capability to effectively control the failure consequences.

8. Input to test definition activity (if required at the analysed integration level).

   NOTE Examples of input to test definition activity are:

   - List of failure modes with relevant effects and observable symptoms provided for generating test requirements and procedures.
   - Identification of functional paths and redundancies that cannot be tested.
   - Identification of tests to verify the assumptions used within the FMEA/FMECA that the system reacts according to the anticipated manner.

9. Input to user manual and operation procedures.

   NOTE For example, at system level the list of failure modes with relevant effects and observable symptoms are provided for establishing data recording requirements, and to determine the required frequency of monitoring in testing, check-out and mission use.

10. Input to contingency analysis.

    NOTE The FMEA/FMECA provide input such as failure detection means-observable symptoms and compensating provisions for the implementation of the contingency analysis.

e. The FMEA/FMECA report shall be issued according to the SOW.

6.6 Phase D: Production or ground qualification testing

a. The FMEA/FMECA performed in phase C shall be updated with regard to design changes decided after the critical design review (CDR) and according to test results.

b. The FMEA/FMECA shall be utilized as a diagnostic tool in order to support the failure diagnosis during the qualification and the elimination of potential failures.

6.7 Phase E: Utilization

a. The FMEA/FMECA performed at system level in phase C/D shall be utilized as support to diagnostic activities (in-flight and on ground) in order to support the system maintenance and restoring.

b. In case of design evolution (mainly for ground segment) the FMEA/FMECA shall be updated.

6.8 Phase F: Disposal

a. In this phase the system level FMEA/FMECA shall be used together with the system safety analysis to support the identification of potential hazardous characteristics of used items (items at the end of its utilization phase) or of the design to define system disposal activities.

NOTE Examples of potential hazardous characteristics are material and radiation.

7
Hardware-software interaction analysis (HSIA)

7.1 Overview

HSIA is an activity performed to ensure that the software reacts in an acceptable way to hardware failures. Particular attention is paid to each failure mode of hardware used in compensatory provisions (redundancy, protection) and controlled by software.

The HSIA can be performed with the aid of the check-list shown in Annex I. The questions can be tailored to the project.

7.2 Technical requirements

a. The HSIA shall be performed concurrently with the FMEA/FMECA to influence the hardware design and the software requirements.

b. The HSIA shall be used to verify that the software specifications as expressed in the requirements baseline (RB) or the technical specification (TS) cover the hardware failures according to the applicable FDIR requirements.

NOTE For more details on RB and TS, see ECSS-E-ST-40

c. Suppliers of products combining H/W and S/W shall perform a HSIA covering all hardware failures which can interact with internal S/W.

d. In the performance of the System HSIA, the supplier shall integrate the HSIAs performed at one level lower than the level of the supplier.

e. For each failure mode the following information shall be used:

1. Symptoms triggering the software action (observable symptoms from FMEA/FMECA).

NOTE Refer to the RB or TS relevant section for justification.

2. Action of the software.

NOTE Refer to RB or TS relevant section for justification

3. Effect of the software action on the product functionality (through induced possible sequence software-hardware effects).

f. The HSIA shall be performed to provide the following results:

1. inputs to the list of critical items;

NOTE For example: no or nonconforming software action and software action having adverse effects on hardware.

2. inputs for FDIR policy;

3. recommendations.

NOTE For example: hardware or software to be added or modified.

g. Nonconforming cases shall be identified and formally dispositioned in conformance with ECSS-Q-ST-10-09.

h. The HSIA shall be documented by completing a form in conformance with the DRD in Annex D.

i. Findings and recommendations arising from the HSIA shall be recorded and tracked together with the ones coming from FMEA/FMECA.

7.3 Implementation requirements

a. The HSIA shall be performed in early phase of design, typically in phase B, to support the definition of software requirements (RB).

NOTE No formal documentation of the analysis is necessary.

b. In phases C/D of the design, the HSIA shall be used to verify software requirements (RB/TS).

c. The HSIA shall be released according to clause 7.2.

8
Process FMECA

8.1 Purpose and objective

Process FMECA is the application of the FMECA methodology to processes. Its purpose is to identify potential critical process steps and to determine their effects on:

- Safety;
- product;
- process itself;
- programmatic aspects.

Possible typical weak points are human errors, failures of related hardware, or environmental stress in existing or planned processes, such as:

- manufacturing;
- assembly or integration;
- ground operations (e.g. mating a satellite to the launcher, filling or draining of tanks, pre-cooling of cryogenic equipment);
- tests;
- in-orbit operations.

The objective of the process FMECA is to initiate measures to eliminate the potential critical process steps or to reduce their criticality to an acceptable value.

The process FMECA should be performed by the process specialist supported if required by the Dependability and Safety specialist.

8.2 Selection of processes and inputs required

a. Process FMECA shall be performed on processes agreed with the customer.

NOTE 1 These processes are those considered to have effects as reported in Table 8-1.

NOTE 2 The inputs needed to start the work depend strongly on the process to be analysed.

Typical inputs are:

- working and control plan;

- assembly procedure;
- integration procedure;
- test procedure;
- handling procedure (manual).

8.3 General process FMECA requirements

a. A Process FMECA report shall be issued, in conformance with Annex E.

b. The documentation of the process FMECA shall be accomplished by completing the columns of the Process FMECA worksheet in conformance with the DRD in Annex F.

c. The severity of failure effects shall be identified by assigning a severity number (SN) according to a table agreed with the customer.

NOTE Table 8-1 gives an example of definitions for Severity Numbers (SN) for some categories of failure effects. It can be customised or completed depending on the process analyzed and on the purpose of the analysis.

d. The probability of occurrence of failure modes shall be identified by assigning a probability number (PN) according to a table agreed with the customer.

NOTE Table 8-2 gives an example of Probability numbers (PN) for probability of occurrence.

e. The probability of detection of failure modes shall be identified by assigning a detection number (DN) according to a table agreed with the customer.

NOTE Table 8-3 gives an example of Detection numbers (DN) for probability of detection.

f. The criticality number (CN) shall be defined as the product of the numbers assigned to failure mode severity, probability of occurrence, and probability of detection according to:

$$CN = SN \times PN \times DN$$

g. Since a failure mode can have more than one failure effect, the highest SN shall be considered.

NOTE The value of SN, PN, and DN are based on engineering judgement and previous experience.

The CN value is in the range from 1 to 64, whereby the meaning of the extremes is:

- negligible, i.e. there is no risk if CN = 1;
- extremely critical, i.e. there is an extremely high risk if CN = 64.

Table 8-1: Example of Severity numbers (SN) for severity of failure effects

SN	Definition			
	Safety related effects	**Process result (i.e. product) related effects**	**Process related effects**	**Programmatic related effects**
4	• Loss of life, life threatening or permanently disabling injury or occupational illness • Loss of site facilities • Severe detrimental environmental effects	N/A	The process is not recoverable and needs to be modified	• Financial loss > 50 % of overall programme cost • Schedule impact > 4 months
3	• Temporary disabling but not life threatening injury, or temporary occupational illness • Major damage to site facilities • Major damage to public or private property • Major detrimental environmental effects	Loss of the product	Repetition of several process steps or of the complete process	• Financial loss between 50 % and 30 % of overall programme cost • Schedule impact between 2 weeks and 4 months
2		Major degradation of the product	Repetition of the faulty step	• Financial loss between 30 % and 10 % of overall programme cost • Schedule impact between 1 day and 2 weeks
1		No or minor degradation of the product	No or minor impact on the analysed process	• Financial loss < 10 % of overall programme cost • Schedule impact lower than 1 day

Table 8-2: Probability numbers (PN) for probability of occurrence

PN	Definition
4	Very likely
3	Likely
2	Unlikely
1	Extremely unlikely

Table 8-3: Detection numbers (DN) for probability of detection

DN	Definition
4	Extremely unlikely
3	Unlikely
2	Likely
1	Very likely

8.4 Identification of critical process steps

a. A process step shall be considered critical if:

1. the severity number SN ≥ 3, or
2. the probability number PN = 4, or
3. the detection number DN = 4, or
4. the criticality number CN ≥ 12

NOTE The customer can tailor the criteria for critical process step identification according to specific needs.

8.5 Recommendations for improvement

a. If the process step is regarded as critical (according to the criteria in clause 8.4) a recommendation shall be given.

b. The relevant failure modes shall then be analysed again on the same process FMECA worksheet to show the improvement, i.e. to show how the Criticality Number is reduced.

NOTE This is done by assuming that the recommendation is already implemented, so that it can be entered as an existing provision. If, as result of this second analysis run, the acceptance criteria of clause 8.4 are still not met, a second recommendation is made and analysed, and so on, until the acceptance criteria are met, or it can be shown and justified that no further risk reduction is feasible.

c. If no further risk reduction is feasible a justification for acceptability shall be given.

NOTE A case example is when the severity of a failure effect cannot be modified.

8.6 Follow-on actions

8.6.1 General

a. Decisions of the Project Management after consideration of the recommendations for improvement shall be:

1. Case 1: the recommendation is implemented, or
2. Case 2: the recommendation is rejected, or
3. Case 3: an alternative recommendation is made.

NOTE Decisions on recommendations always involve the assessment of the impact on safety.

8.6.2 In case 1:

a. An actionee and a due date shall be entered for the implementation.

b. The analysis result of the implementation shall be compared with the results leading to the original recommendation.

c. In case of discrepancies, a clarification shall be entered and the relevant analysis steps repeated.

d. In case of no discrepancy, a close-out reference shall be entered.

NOTE For example, the reference to the change notice

8.6.3 In case 2:

a. The term "rejected" shall be entered (as close-out reference) together with the rationale for rejection.

NOTE The rationale is within the responsibility of the project.

8.6.4 In case 3:

a. An actionee and a due date shall be entered for the implementation of the alternative recommendation.

b. The modified situation shall be treated on the same process FMECA worksheet to identify the improvements.

NOTE The final closing of the action by the project can only be:

- acceptance according to case 1, or
- rejection according to case 2.

Annex A (normative) FMEA/FMECA report – DRD

A.1 DRD identification

A.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement 4.7a.

A.1.2 Purpose and objective

The purpose of the FMEA/FMECA report is to document the results of the FMEA/FMECA.

A.2 Expected response

A.2.1 Scope and content

<1> Cover sheet

a. The FMEA/FMECA report shall include the title of the analysis and reference number, issue, revision and date, supplier sign-off date, and the names and signatures of the analyst(s) and the approval authority.

<2> Introduction

a. The FMEA/FMECA report shall provide concise statements on the objectives of the analysis including definition of the level of the analysis.

<3> Documents

a. The FMEA/FMECA report shall list the applicable and reference documents, including design reference, analyses performed by lower level suppliers, used in the preparation of the FMEA/FMECA.

<4> Acronyms and abbreviations

a. The FMEA/FMECA report shall list of acronyms, abbreviations and definitions of special terms used.

<5> Product

a. The FMEA/FMECA report shall include narrative description of the product functions to provide an understanding of the analysis.

b. The FMEA/FMECA report shall include a functional partition in the design between hardware and software, including a reference to the corresponding HSIA shall be addressed.

<6> Block diagrams and schematics

a. The FMEA/FMECA report shall include block diagrams and schematics to assist in describing the product, provide schematic diagrams, functional block diagrams and reliability block diagrams (RBDs) to a level consistent with the depth of the analysis and with design maturity.

NOTE Functional tree is also useful to describe functional relationships.

b. An appropriate identification number shall be used to provide consistent identification and complete visibility of the relationship between each block and the applicable failure modes.

<7> Design

a. The FMEA/FMECA report shall provide the definition of the status of the design of the product under analysis by reference to a configuration document.

NOTE For example, CIDL.

b. If the design is not mature enough to provide this document, then the design shall be defined by reference to reports used to perform the analysis.

c. Description and listing of any incomplete design areas shall be identified.

<8> Basic rules and assumptions

a. The FMEA/FMECA report shall include the description of the ground rules adopted for the analysis (including list of items omitted from the analysis) and all the assumptions made regarding mission phases and times, operational modes, environmental conditions, failure modes and failure criteria.

NOTE This list is not conclusive.

b. All rules and assumptions shall be approved by the customer.

NOTE For information a list of failure modes for EEE parts is provided in Annex G.

c. The list of failure modes of each part may be amended or additional modes included, depending on specific applications.

<9> Failure detection or isolation criteria

a. The FMEA/FMECA report shall describe the FDIR policy and criteria including reference to relevant documents and to detection reference.

NOTE The detection reference includes telemetry, housekeeping data, and health check.

<10> Results and recommendations

a. The FMEA/FMECA report shall provide results and recommendations based upon the detailed analysis presented by the FMEA/FMECA worksheets.

<11> Critical items

a. The FMEA/FMECA report shall provide a list of all the critical items identified (as per 4.3 or 5.3, respectively) including item identification and cross-reference with FMEA/FMECA worksheets.

<12> Failure Effect Summary List (FESL)

a. The FMEA/FMECA report shall provide a list of the failure effects leading to consequences classified in severity category 1, 2 and 3 and identify all relevant failure modes including item identification and cross-reference with FMEA/FMECA worksheets.

<13> Status on recommendations

a. The FMEA/FMECA report shall make reference to the document providing the status of the recommendations.

<14> FMEA/FMECA Worksheets

a. The FMEA/FMECA report shall include the FMEA/FMECA worksheets in conformance with Annex B/Annex C, respectively.

A.2.2 Special remarks

None.

Annex B (normative)
FMEA worksheet – DRD

B.1 DRD identification

B.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement Annex A.2.1<14>a.

B.1.2 Purpose and objective

The purpose of the FMEA worksheet is to document the analysis performed in a tabular form.

B.2 Expected response

B.2.1 Scope and content

<1> Header information

a. The FMEA worksheet shall contain the identity of the product (hardware or function) and the identity of corresponding equipment, subsystem, and system (as applicable).

<2> Identification number

a. The FMEA worksheet shall contain the identification number for traceability purposes.

<3> Item/block

a. The FMEA worksheet shall contain

   1. the name of the item or function being analysed, and
   2. the block of the reliability block diagram that is applicable to the analysis entry.

<4> Function

a. The FMEA worksheet shall contain a concise statement of the function performed by the item.

<5> Failure mode

a. The FMEA worksheet shall contain the identification and description of all potential failure modes of the item or function under analysis.

NOTE With reference to 4.5d, end effects of lower level FMEA are failure modes of the higher level FMEA.

<6> Failure cause

a. When requested, the FMEA worksheet shall contain the identification and description of the most probable causes associated with the assumed failure mode.

NOTE 1 With reference to 4.5e failure modes of lower level FMEA are failure causes of the higher level FMEA.

NOTE 2 The failure cause are generally not identified when components are analysed (equipment level FMEA).

<7> Mission phase/Operational mode

a. The FMEA worksheet shall contain a concise statement of the mission phase and operational mode in which the failure is assumed to occur.

NOTE These elements can be addressed in the header of the worksheet. Although all of the different mission phases or operational modes are taken into account, the record of results is limited to the phase or mode in which the worst failure effects occur.

<8> Failure effects

a. The FMEA worksheet shall contain the identification of the consequences of each assumed failure mode at local effects and end effects levels.

NOTE 1 Local effects

Local effects concentrate specifically on the impact of the failure mode on the operation, function, or status of the item identified in the second column of the worksheet. The local effects are recorded when different from the failure modes.
The purpose of defining local effects is to provide a basis for evaluating compensating provisions and for recommending corrective actions.

NOTE 2 End effects

End effects define the effect that the analysed failure mode has on the operation, function, or status of the product under investigation and its interfaces, such that it allows integration into the next higher level FMEA.

<9> Severity classification

a. The FMEA worksheet shall contain the severity classification category assigned to each failure mode according to the worst potential end effect of the failure (see clause 4.1 and 4.2).

<10> Failure detection method - Observable symptoms

a. The FMEA worksheet shall identify the failure detection method and the observable symptoms.

NOTE The failure detection means include telemetry (exact label), visual or audible warning devices, sensing instrumentation, other unique indications (e.g. the failure effect itself), or none.

<11> Compensating provisions

a. The FMEA worksheet shall identify the existing compensating provisions, such as design provisions or operator actions, which circumvent or mitigate the effect of the failure.

NOTE 1 Design provisions

Compensating provisions are considered design provisions when they feature a design that nullifies the effects of a malfunction or failure, control, or deactivate product items to halt generation or propagation of failure effects, or activate backup or standby items. Design compensating provisions include:

- redundant items or alternative modes of operation that allow continued and safe operation, and
- safety or relief devices which allow effective operation or limit the failure effects.

NOTE 2 Operator actions

Compensating provisions are considered operator actions when the operator circumvents or mitigates the effect of the postulated failure mode.

<12> Recommendations

a. Recommendations for corrective actions shall be noted. Each recommendation shall have a non-ambiguous identifier for tracking purpose.

<13> Remarks

a. The FMEA worksheet shall contain any pertinent remarks relevant to and clarifying any other column in the worksheet line.

B.2.2 Example of FMEA worksheet

Figure B-1 gives an example of FMEA worksheet.

Failure Modes and Effects Analysis (FMEA)											
Product:			**System:**				**Subsystem:**			**Equipment:**	
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Recommendations	Remarks

Figure B-1: Example of FMEA worksheet

Annex C (normative)
FMECA worksheet – DRD

C.1 DRD identification

C.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement Annex A.2.1<14>a.

C.1.2 Purpose and objective

The purpose of the FMECA worksheet is to document the analysis performed in a tabular form.

C.2 Expected response

C.2.1 Scope and content

<1> General

a. The FMECA worksheet shall provide the data elements identified in FMEA worksheet of Annex B.2.1.

<2> Severity number

a. The FMECA worksheet shall contain the severity number (SN) assigned to each assumed failure mode.

NOTE The SNs applied at the different severity categories are given in Table 5-1.

<3> Failure mode probability

a. The FMECA worksheet shall contain an assessment of the probability of occurrence of the assumed failure mode and the relevant probability number (PN)

NOTE The PNs applied at the different probability levels are given in Table 5-2.

<4> Criticality number

a. The FMECA worksheet shall contain a criticality number (CN) assigned to each assumed failure mode, as per 5.2n.

C.2.2 Example of FMECA worksheets

Figure C-1 and Figure C-2 give examples of FMECA worksheets.

Failure Modes Effects and Criticality Analysis (FMECA)														
Product:			**System:**			**Subsystem:**					**Equipment:**			
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity classification	Failure detection method/ observable symptoms	Compensating provisions	Severity Number SN	Probability and PN	Criticality Number CN	Recommendations	Remarks

Figure C-1: Example 1 of FMECA worksheet

Failure Modes Effects and Criticality Analysis (FMECA)			
Product:	System:	Subsystem:	Equipment:
Id. Number:	Item/block:		
Function:			
Failure mode:			
Failure cause:			
Mission phase/Operational mode:			
Failure effects: a. Local effects b. End effects			
Severity classification			
Failure detection method/Observable symptoms			
Compensating provisions:			
Severity Number SN:	Probability and PN:	Criticality Number CN:	
Recommendations:			
Remarks:			

Figure C-2: Example 2 of FMECA worksheet

Annex D (normative)
HSIA form - DRD

D.1 DRD identification

D.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement 7.2h.

D.1.2 Purpose and objective

The purpose of the HSIA form is to document the analysis performed in a tabular form.

The HSIA check list is an aid for performing the analysis, see Annex I.

D.2 Expected response

D.2.1 Scope and content

<1> Subsystem or equipment

a. The HSIA form shall contain the identification of subsystem or equipment submitted to HSIA.

<2> HSIA sheet number

a. The HSIA form shall contain the HSIA running sheet number.

<3> FMEA/FMECA reference

a. The HSIA form shall contain the identification of the reference number of the failure mode in the design FMEA/FMECA.

<4> Failure mode

a. The HSIA form shall contain a summary of failure mode description.

<5> RB/TS reference

a. The HSIA form shall contain a reference to the software specification used for the HSIA (number, issue).

<6> Identification of parameters used to trigger the software

a. The HSIA form shall contain identification of the information processed by the software to notify the presence of the failure or initiate an isolation or corrective action in response.

b. The HSIA form shall contain the identification of corresponding health signal (health signal = result of comparison between detected and reference values).

<7> RB/TS requirement number for S/W triggering

a. The HSIA form shall contain the requirement number in the RB/TS corresponding to the information at D.2.1<6>.

<8> Description of software (S/W) action

a. The HSIA form shall contain a summary of the actions specified in RB/TS which are provided to negate the effects of or isolate the failure (isolation/recovery).

<9> RB/TS requirement number for S/W action

a. The HSIA form shall contain the requirement number in the RB/TS corresponding to the information at D.2.1<8>.

<10> Description of the effect of the S/W action on the product functionality

a. The HSIA form shall contain a summary of the effects of the actions taken by S/W (as described in RB/TS) on the functions of the product and on interfacing items.

<11> Identified adverse effects on hardware (H/W)

a. The HSIA form shall contain a description of any identified adverse effect.

NOTE Examples of adverse effects are overstress of H/W, or failure propagation.

<12> Assessment of the S/W action

a. The HSIA form shall contain an assessment of the S/W action.

NOTE The answer “yes” summarizes that the S/W action on the product functionality is conforming to the FDIR requirements (where

applicable) and the S/W action is acceptable for the product functioning.
In case of answer "no", recommendations are reported in D.2.1<13>.

<13> Recommendations

a. The HSIA form shall contain recommendations in case of insufficient S/W actions or in case of adverse effect on H/W.

<14> Remarks:

a. The HSIA form shall contain any additional remark where relevant.

D.2.2 Example of HSIA form

Figure D-1 gives an example of HSIA form.

HARDWARE-SOFTWARE INTERACTION ANALYSIS (HSIA)	
1. Subsystem/Equipment:	2. HSIA sheet number:
3. FMEA/FMECA reference:	4. Failure mode:
5. RB/TS reference:	
6. Identification of parameters used to trigger the S/W action:	7. RB/TS requirement number for S/W triggering:
8. Description of S/W action:	9. RB/TS requirement number for S/W action:
10. Description of the effects of the S/W action on the H/W:	11. Identified adverse effect on H/W
12. Assessment of S/W action: Is the S/W action as expected? yes/no	
13. Recommendations:	
14. Remarks	

Figure D-1: Example of HSIA form

D.2.3 HSIA integrated in FMEA/FMECA worksheet

a. In case the HSIA is provided inside the FMEA/FMECA, the FMEA/FMECA worksheet shall be completed as follows:

1. add S/W Specification reference in the Reference document;
2. in each completed column: for each failure mode where software is involved enter “S/W”;
3. local/end effect: add points 10 and 11 of HSIA form;
4. failure detection: add points 6 and 7 of HSIA form;
5. recovery or compensation: add points 8 and 9 of HSIA form;
6. recommendation: add points 12 and 13 of HSIA form.

Annex E (normative)
Process FMECA report – DRD

E.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement 8.3a.

E.1.2 Purpose and objective

The purpose of the Process FMECA report is to document the analysis performed.

E.2 Expected response

E.2.1 Scope and content

<1> Cover sheet

a. The Process FMECA report shall contain the title of the analysis and reference number, issue, revision and date, supplier sign-off date, and the names and signatures of the analyst(s) and the approval authority.

<2> Documents

a. The Process FMECA report shall list the applicable and reference documents, including applicable procedure, design reference, lower level supplier analyses, used in the preparation of the process FMECA.

<3> Description of the analysed process

a. The Process FMECA report shall describe the analysed process.

<4> Process FMECA worksheets

a. The Process FMECA report shall contain the Process FMECA worksheets in accordance with Annex F.

<5> List of recommendations for improvement

a. The Process FMECA report shall list recommendations for improvement.

<6> Follow-on actions

a. The Process FMECA report shall include follow-on action to be presented to the project team responsible for final decisions.

NOTE 1 The follow-on actions (references for implementation, rejection, or analysis of alternative recommendations) apply to the updates of the report.

NOTE 2 In the case where company "CONFIDENTIAL" processes are documented, the report can be split into:

- a summary report including recommendations and unacceptable points (to be submitted to the customer);
- the detailed process FMECA worksheets (company confidential).

NOTE 3 See also clause 8.6 about "Follow-on actions".

E.2.2 Special remarks

None

Annex F (normative)
Process FMECA worksheet – DRD

F.1.1 Requirement identification and source document

This DRD is called from ECSS-Q-ST-30-02, requirement 8.3b and Annex E.2.1<4>a.

F.1.2 Purpose and objective

The purpose of the Process FMECA worksheet is to document the analysis performed in a tabular form.

F.2 Expected response

F.2.1 Scope and content

<1> Worksheet header

a. The Process FMECA worksheet shall identify the:

1. Analysed process,
2. System, subsystem, and equipment.

<2> Identification number

a. The Process FMECA worksheet shall contain the identification number for traceability purpose.

<3> Item

a. The Process FMECA worksheet shall contain the identification of the individual process step.

<4> Description

a. The Process FMECA worksheet shall contain the description of the process step.

<5> Failure mode/failure cause

a. The Process FMECA worksheet shall contain the description of the assumed process step failure mode together with its causes.

<6> Failure effects

a. Depending on the process analyzed and on the purpose of the analysis, the Process FMECA worksheet shall contain the description of all possible effects of the assumed failure modes on:

1. Safety,
2. Product (i.e. final result of the process),
3. Process,
4. Programmatic

   NOTE For example, impact on costs schedule.

5. Others, if any

   NOTE For example, company image.

<7> Detection means

a. The Process FMECA worksheet shall contain the description of the existing means and methods by which the effects can be detected.

<8> Existing preventive or compensatory provisions

a. The Process FMECA worksheet shall contain the description of the existing preventive or compensatory provisions to prevent the failure mode, to reduce its effects, or to reduce its probability of occurrence.

<9> Severity

a. The Process FMECA worksheet shall contain the identification of the severity of failure effect by assigning a severity number (SN) according to a table agreed with the customer.

<10> Occurrence

a. The Process FMECA worksheet shall contain the identification of the probability of occurrence of the failure mode by assigning a probability number (PN) according to a table agreed with the customer.

<11> Detection

a. The Process FMECA worksheet shall contain the Identification of the probability of detection of the failure mode by assigning a detection number (DN) according to a table agreed with the customer.

<12> Criticality

a. The Process FMECA worksheet shall contain the criticality number (CN).

<13> Recommendations and remarks

a. The Process FMECA worksheet shall contain a description of the recommended preventive or compensatory provisions to eliminate the failure mode, to reduce its effects, to reduce its probability of occurrence, or to improve its detectability, as well as any additional information being useful.

F.2.2 Example of Process FMECA worksheet

An example of a Process FMECA worksheet is given in Figure F-1.

Process Failure Modes, Effects and Criticality Analysis (FMECA)											
Analysed process:				**System:**			**Subsystem:**				**Equipment:**
Ident. number	Item	Description	Failure mode/ Failure cause	Failure effects: a) safety b) product c) process d) programmatic e) others	Detection means	Existing preventive or compensatory provisions	Severity SN	Occurrence PN	Detection DN	Criticality CN	Recommendations and remarks

Figure F-1: Example of process FMECA

Annex G (informative)
Parts failure modes (space environment)

Table G-1: Example of parts failure modes

01. CAPACITORS (family/group 01 xx)		
Type	Failure modes	Remarks
01 01 ceramic 01 02 ceramic chip 01 04 tantalum non-solid 01 06 glass 01 07 mica 01 09 aluminium solid 01 10 feedthrough 01 11 semiconductor	OC SC S/C with structure (only for feedtrough)	
01 03 tantalum solid	OC SC Current Leakage	Depending on leakage value, final effect can be either short circuit or open circuit (in case of over heating and burst) In particular for CMS tantalum capacitor open circuit condition after short circuit to be considered. Because of explosion risk as a result of low ohmic failure case, redundant solid tantalum capacitors are segregated in such a way that the product resulting from the explosion of the nominal part does not affect the redundant part
01 05 plastic metallized	OC SC (epsilon)	For self-healing capacitor (typical PM94, PM96, PM90, …) the short circuit is considered in the FMEA/FMECA (for traceability aspects). The minimum self-healing energy is indicated in the FMEA/FMECA.
02. CONNECTORS (family/group 02 xx)		
Type	Failure modes	Remarks
02 01 circular 02 02 rectangular 02 03 printed circuit board 02 05 RF coaxial 02 06 glassfibre 02 07 microminiature	Any single pin OC Connector disconnection (1)	(1): The number of critical connectors (i.e. the demating of which has critical effects on the mission) is minimized by design. A specific analysis is performed for identifying critical connectors. Connector disconnection is considered as a not credible failure in flight providing a locking device exists and verification of

02 08 RF filter 02 09 rack and panel		locking is performed during AIT. An appropriate justification is provided.

03. PIEZO-ELECTRIC DEVICES (family/group 03 xx)

Type	Failure modes	Remarks
03 01 crystal resonator	OC (no clock signal) Frequency drift	- drift means over the worst case range specified - the worst effect with regard to the device function is assessed

04. DIODES (family/group 04 xx)

Type	Failure modes	Remarks
04 01 switching 04 02 rectifier 04 03 voltage regulator 04 04 voltage reference/zener 04 05 RF/microwave schottky (Si) 04 06 pin 04 07 hot carrier 04 08 transient suppression 04 09 tunnel 04 10 high voltage rectifier 04 11 microwave varactor (GaAs) 04 12 step recovery 04 13 RF/microwave varactor (Si) 04 14 current regulator 04 15 microwave schottky (GaAs) 04 16 RF/microwave pin 04 17 microwave gunn (GaAs)	Any single pin OC SC Any single terminal SC to structure	Terminal means pin or component case (if any) It is important to consider SC between terminal and structure according to technology for diodes directly mounted on the structure

05. FILTERS (family/group 05 xx)

Type	Failure modes	Remarks
05 01 feedthrough 05 02 diplexers	Any single pin OC SC Any single terminal SC to structure	It is important to consider SC between terminal and structure according to technology

06. FUSES (family/group 06 xx)

Type	Failure modes	Remarks
06 01 all	OC	Glass fuses are generally forbidden with the exception of wire link fuses

07. INDUCTORS (family/group 07 xx)

Type	Failure modes	Remarks
07 01 RF coil 07 02 cores 07 03 chip	OC SC between terminals SC between turns Any single terminal SC to core or structure	SC between terminals or turns to be considered except where specific provisions other than enamel are taken (e.g. specifically insulated wire, kapton layer or specific design rules) It is important to consider SC between terminal and core or structure according to technology for inductors mounted directly on the structure Breaking of the magnetic core is assimilated to SC and is considered except where specific provisions are taken (e.g. potting)

08. MICROCIRCUITS (family/group 08 xx)

Type	Failure modes	Remarks
08 10 microprocess/microcontrol/peripher 08 20 memory SRAM 08 21 memory DRAM 08 22 memory PROM 08 23 memory EPROM 08 24 memory EEPROM 08 29 memory others 08 30 programmable logic 08 40 ASIC technologies digital 08 41 ASIC technologies linear 08 42 ASIC technologies mixed analog/digital 08 50 linear operational amplifier 08 51 linear sample and hold amplifier 08 52 linear voltage regulator 08 53 linear voltage comparator 08 54 linear switching regulator 08 55 linear line driver 08 56 linear line receiver 08 57 linear timer 08 58 linear multiplier 08 59 linear switches 08 60 linear multiplexers/demultiplexer 08 61 linear analog to digital converter 08 62 linear digital to analog converter 08 69 linear other functions 08 80 logic families 08 90 other functions 08 95 microwave monolithic integrated circuits (MMIC)	Any single output SC to V+/V- Any single output stuck to 0/1 Any single output in high impedance Any single input SC to V+/V- Any single input SC to 0/1 OC of any single power supply V+ to V- SC SEP Any single functional failure Any single output SC to V+/V- Any single output stuck to 0/1 Any single output in high impedance Any single input SC to V+/V- Any single input SC to 0/1 OC of any single power supply V+ to V- SC SEP	OC of any single power supply including ground pin For complex IC's (ASIC, FPGA, µP,…), a functional FMEA/FMECA is performed taking into account the physical implementation . SEP effect analysis performed in the FMEA/FMECA is based on the output of the radiation analyses OC of any single power supply includes ground SEP effect analysis performed in the FMEA/FMECA is based on the output of the radiation analyses For linear integrated circuit SET worst case effect is considered when sensitivity identified trough radiation analyses (generally temporary effect)

09. RELAYS (family/group 09 xx)		
Type	Failure modes	Remarks
09 01 non latching 09 02 latching	Relay stuck in one position Coil Open Circuit 2 open contacts (relay stuck in intermediate position) 2 contacts in opposite position Short Circuit between fix contacts Short Circuit between coil and one contact (epsilon) Short Circuit between contact and structure (epsilon)	See details in Figure G-1, Figure G-2, Figure G-3 hereafter. Failure modes only applicable to electromechanical devices. For other devices performing same function (e.g. thermally actuated micro-machined relays), identify alternate possible failure modes and consider them according to the technology of the relay
10. RESISTORS (family/group 10 xx)		
Type	Failure modes	Remarks
10 01 metal oxide 10 05 composition 10 07 shunt 10 08 metal film 10 10 network (all) 10 11 heater, flexible	OC	For film network the open circuit of the common connection is considered
10 09 chip (all)	OC	No short circuit is considered possible for sizes 1206 or larger
10 02 wirewound precision (including surface mount) 10 03 wirewound chassis mounted	OC SC between terminals (epsilon)	
10 04 variable (trimmer)	OC SC between terminals	
11. THERMISTORS (family/group 11 xx)		
Type	Failure modes	Remarks
11 01 temperature compensating 11 02 temperature measuring 11 03 temperature sensor	OC SC between terminals Erroneous measurement	

12. TRANSISTORS (family/group 12 xx)

Type	Failure modes	Remarks
12 01 low power, NPN (< 2 W) 12 02 low power, PNP (> 2 W) 12 03 high power, NPN (< 2 W) 12 04 high power, PNP (> 2 W) 12 05 FET N channel 12 06 FET P channel 12 08 multiple 12 09 switching 12 10 RF/microwave NPN low power/low noise 12 11 RF/microwave PNP low power/low noise 12 12 RF/microwave FET N-channel/P-channel 12 13 RF/microwave bipolar power 12 14 RF/microwave FET power (Si) 12 15 microwave power (GaAs) 12 16 microwave low noise (GaAs) 12 17 chopper	Any single terminal OC SC between any two terminals	SC between terminal and structure are considered according to technology for transistors mounted directly on the structure For FET all failures causing over dissipation exceeding rated value is analysed (thermal risk failure propagation)

13. WIRES AND CABLES (family/group 13 xx)

Type	Failure modes	Remarks
13 01 low frequency 13 02 coaxial 13 03 fiber optic	OC SC	SC to be considered except in case of double insulation

14. TRANSFORMERS (family/group 14 xx)

Type	Failure modes	Remarks
14 01 power 14 02 signal	Any single terminal OC SC primary/secondary SC +/- primary SC +/- secondary SC between any two turns of any two coils Any single terminal SC to core or structure	SC between terminals or turns to be considered except where specific provisions other than enamel are taken (e.g. specifically insulated wire, kapton layer or specific design rules) SC between terminal and core or structure are considered according to technology for transformers mounted directly on the structure Breaking of the magnetic core is assimilated to SC and is considered except where specific provisions are taken (e.g. potting)

16. SWITCHES (family/group 16 xx)

Type	Failure modes	Remarks
16 01 standard DC/AC power toggle 16 02 circuit breaker 16 03 RF-switch 16 04 microswitch 16 05 reed switch	OC SC between terminals For RF Switch: - Fixed in original position - Failed in intermediate position	Failure modes considered are reported and justified along with a description of the component and of its application

18. OPTO-ELECTRONICS (family/group 18 xx)

Type	Failure modes	Remarks
18 01 optocoupler 18 03 phototransistor 18 06 charge couple device (CCD) 18 07 LCD display/screen	Diode OC Transistor OC SC between diode terminals SC between transistor terminals SC between any two diode and transistor terminals	SC between diode and transistor terminals are considered according to technology (epsilon for 3C91). This information should be contained in the optocoupler procurement specification. Radiation/aging effects leading to characteristics modifications (e.g. CTR/gain) and loss of performance should be considered when sensitivity identified through radiation analysis
18 02 LED 18 04 photo diode/sensor 18 05 laser diode	OC SC between terminals	

19. THYRISTORS (family/group 19 xx)

Type	Failure modes	Remarks
19 01 all	OC SC between any two terminals SC between any single terminal and structure	SC between terminal and structure are considered according to technology

20. THERMOSTAT (family/group 20 xx)

Type	Failure modes	Remarks
20 01 all	Blocked Open Blocked closed Commutation threshold drift SC between any single contact terminal and structure (epsilon)	It is important to consider SC between contact terminal and structure according to technology

23. LAMP (family/group 23 xx)

Type	Failure modes	Remarks
23 01 all	TBD	It is important to report the considered failure modes and justify them along with a description of the component and of its application

27. FIBEROPTIC COMPONENTS (family/group 27 xx)

Type	Failure modes	Remarks
27 01 fibre/cable 27 02 connector 27 03 isolator 27 04 switch	OC Transmission performance drift	

30. RF PASSIVE COMPONENTS (family/group 30 xx)

Type	Failure modes	Remarks
30 01 coaxial couplers 30 06 waveguide components 30 07 isolator/circulator 30 09 coaxial power dividers 30 10 coaxial attenuators/loads	- Open Circuit of an access or connection - Internal Short Circuit - Weld failure - Detuning - Deplating - Any other failure mode causing loss or degradation of performances	It is important to report the considered failure modes and justify them along with a description of the component and of its application

31. BATTERY (family/group 31 xx)

Type	Failure modes	Remarks
31 01 all	Cell OC SC between terminals of any single cell Cell rupture Cell leakage	

32. PYROTECHNICAL DEVICES (family/group 32 xx)

Type	Failure modes	Remarks
32 01 initiators 32 02 cutters	OC SC between terminals Any single terminal SC to structure	Failure modes considered are reported and justified along with a description of the component and of its application

40. HYBRIDS (family/group 40 xx)		
Type	Failure modes	Remarks
40 01 thick film 40 02 thin film	OC Any single functional failure	Failure modes of components when viewed as discrete parts
40 03 crystal oscillators	OC Frequency drift	
99. MISCELLANEOUS PARTS (family/group 99 xx)		
Type	Failure modes	Remarks
99 01 all	TBD	Failure modes considered are reported and justified along with a description of the component and of its application
Heater	OC, including heater delamination (for thermofoil) SC between terminals Any single terminal SC to structure SC between any two terminals of redundant lines	SC between terminal and structure are considered according to technology SC between redundant line terminals are considered according to technology SC between redundant lines at intermediate points not considered because of application of specific design rules. Specific design rules to be formulated or referred.
Heat pipe	Rupture Leakage Insufficient thermal transfer	
Solar Cell (Si or AsGa)	- Short Circuit - Open Circuit - Short Circuit of input or output with Structure	- Total or partial surface loss; low probability of occurrence - Depending on device technology
All pressurized element (tank, tubing, welded & screwed connections, filter, valve, regulator, pressure transducer, ...) Pressure transducer Filter Pyrotechnic valve, Electro valve (isolation)	- Rupture - External leakage - Incorrect measurement - Clogging - Insufficient filtering - Internal leakage - Stuck open / close - Untimely closed / opened	Failure mode to be confirmed by the supplier. The stuck open failure and leakage of both propellants have a very low probability of occurrence

Bi-propellant thruster valve	- Internal leakage - Stuck open / close - Asymmetric opening	
Pressure regulator	- High output pressure - Low output pressure	- Compared to normal pressure - Compared to normal pressure
Non-return valve	- Internal leakage - Stuck open / close	
Fill and Drain valve	- Rupture - External leakage	
Non Explosive Actuators	OC SC between terminals Any single terminal SC to structure	Failure modes considered are reported and justified along with a description of the component and of its application

The following table and figures identifies the failure modes, which are analysed for relays.

Table G-2: Example of relay failure modes

Failure modes	Mono-stable relays (type J412, T12, GP5 or equivalent)	Bi-stable relays (type J422, TL12, GP250 or equivalent)	Bi-stable relays (type EL210 or equivalent)	Bi-stable relays (type GP3 or equivalent)
Relay stuck in OFF position:				
- coil Open Circuit	A	A	A	A
- contact stuck OFF	A	A	A	A
Relay stuck in ON position:				
coil Open Circuit	N/a	A	A	A
contact stuck ON	A	A	A	A
Coil short circuit	N/A	N/A	N/A	N/A
2 open contacts (relay stuck in intermediate position)	N/A	A (2)	N/A	A (1)
2 contacts in opposite positions	A (1)	A (1)	N/A	A (1)
Short circuit between fix contacts	A (1)	A (1)	N/A	A (1)
Short circuit between coil and one contact	A (1)	A (1)	N/A	A (1)

(1): Negligible probability of occurrence. To be considered in the FMECA for traceability aspects.

(2) : Not applicable for GP250

A: applicable

N/A: not applicable

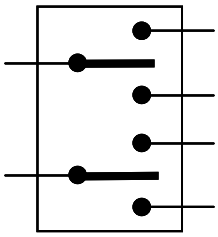


Figure G-1: Two open contacts (relay stuck in intermediate position)

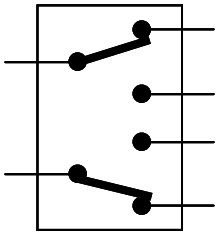


Figure G-2: Two contacts in opposite positions

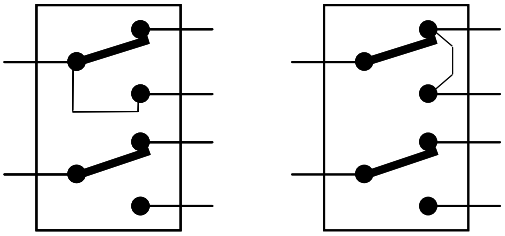


Figure G-3: Short circuit between fix contacts

Annex H (informative)
Product design failure modes check list

Table H-1: Example of a product design failure modes check-list for electromechanical electrical equipment or assembly or subsystems

Design failure modes	yes/no
Pin, wire sizing and PCB tracks not compatible with the over-current protection.	
Mis-mating of adjacent connectors.	
Connectors not used in flight configuration do not have flight qualified protection covers.	
Power supply lines and data lines mixed in the same connector or harness.	
Pyrotechnic lines and other lines mixed in the same connector or harness.	
More than one wire per crimped connection.	
Connectors not clearly labelled.	
Harness, connectors and tie points shared in common by otherwise redundant paths.	
Not every box or assembly has an external safety grounding stud.	
Vent hole sizing not adequate.	
Inadequate hermeticity for sealed devices.	
Box or assembly attachment foot and bolt are not freely accessible for the associated tools.	
PCB traces not properly derated.	
Excessive fan-out and fan-in between interfacing PCBs or components.	
Multiple functions performed by a single EEE part (e.g. redundant paths in one IC, a single multi-pole relay carrying redundant functions, redundancy paths integrated into a common multi-layer PCB).	
A sensing element is used in both control and monitoring.	
Adjacent parts not spaced enough to preclude short circuit, stray capacitance or excessive thermal conduction.	
Insufficient thermal isolation between redundant parts.	
Thermal coupling between high dissipation and heat sensitive elements.	
Hot spots.	
Not all conductive surfaces are grounded.	
Contact between metals with electrochemical potentials > 0,5 V.	
Telecommands and telemetries are mapped so their sets of addresses are separated by at least two bits (critical telecommands or telemetries).	

Annex I (informative)
HSIA check list

HARDWARE-SOFTWARE INTERACTION ANALYSIS (HSIA)		
Subsystem:	FMEA/FMECA number:	
Item:	Failure mode:	
No.	**Question**	**yes/no**
1a	Does the information provided to the software and its processing cause the presence of a failure to be passed to the software or initiate a corrective action in response?	
1b	If the answer to 1a is "no", does the hardware provide the information that the software can use to detect the failure?	
1c	Are the answers to 1a and 1b consistent with the FMEA/FMECA analysis of observable symptoms?	
2a	Does the software take action to negate the effects of the failure?	
2b	If the answer to 2a is "no", does the capability exist for the software to compensate for this failure mode?	
3	As a result of this failure mode, can the software cause the hardware to be overstressed, or induce another failure?	
4	Can this failure mode, in combination with software logic, adversely affect other functions?	
5	What are the failure tolerance characteristics of the design regarding this failure mode (take into account ground or crew intervention, or software compensation); how many failures can be tolerated? (1 2 3)*	
6	If ground or crew action is required to respond to this failure mode, is telemetry, or signal, provided to indicate the need for intervention?	
7	Is the response time limited by mission success factors?	
Change/Retention rationale summary		
1. No H/W or S/W issues:	2. H/W accepts risk:	
(crew or ground operators) (crew or ground operators) (crew or ground operators)	4. Detection during check-out:	
5. Acceptance rationale:	6. Recommendations:	
7. FMEA/FMECA change recommended:		
Comments:		

* circle number

Figure I-1: Example of HSIA check-list

Bibliography

ECSS-S-ST-00	ECSS System – Description, implementation and general requirements
ECSS-E-ST-40	Space engineering – Software general requirements
ECSS-M-ST-10	Space project management – Project planning and implementation
ECSS-M-ST-80	Space project management – Risk management
ECSS-Q-ST-10-04	Space product assurance – Critical-item control
ECSS-Q-ST-40	Space product assurance – Safety
IEC 60050-191 (1990-12)	International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service