**ECSS-Q-30-02A**
7 September 2001


# Space product assurance

## Failure modes, effects and criticality analysis (FMECA)

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

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

ISSN: 1028-396X

Price: € 20

Printed in The Netherlands

# Foreword

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

The formulation of this Standard takes into account the existing ISO 9000 family of documents.

This Standard has been prepared by the ECSS Working Group Q-30-02, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

*(This page is intentionally left blank)*

# Contents

## Figures



## Tables

# Introduction

The failure modes, effects analysis or failure modes effects and criticality analysis (FMEA/FMECA) process, provided it is a timely, iterative activity, is an effective tool in the decision making process. 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 subclause of this Standard.

The FMEA/FMECA can be initiated at any level of integration depending on the information available and the requirements of a programme. 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 design 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 FMEA/FMECAs and provide outputs to be passed to lower level analysts. After performing the required lower level FMEA/FMECAs, their integration leads to the updating and refinement of the system FMEA/FMECA in an iterative manner.

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.

*(This page is intentionally left blank)*

# 1

# Scope

## 1.1 General

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

This Standard defines the principles and requirements that shall be adhered to with regard to failure modes, effects and criticality analysis (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 FMECA to systematically evaluate and document the potential impact of each failure (functional, hardware, or process) on product operation and mission success, personnel and product safety, maintainability and maintenance requirements.

Recommended forms and formats are identified in this Standard.

## 1.2 Applicability

This Standard applies to all elements of space projects where failure modes, effects and criticality analyses are part of the dependability programme.

Application specific integrated circuits (ASICs), integrated circuits, and software are treated as "black boxes". 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 FMECA.

## 1.3 Tailoring

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-00-03, 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.

NOTE Tailoring is a process by which individual requirements or specifications, standards and related documents are evaluated and made applicable to a specific project by selection, and in some exceptional cases, modification of existing or addition of new requirements.

# 2

# Normative references

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

| | |
|---|---|
| ECSS-P-001 | Glossary of terms |
| ECSS-Q-30 | Space product assurance — Dependability |
| ECSS-Q-40 | Space product assurance — Safety |
| ECSS-M-30 | Space project management — Project phasing and planning |

*(This page is intentionally left blank)*

# 3

# Terms, definitions and abbreviated terms

## 3.1 Terms and definitions

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

**3.1.1**
**active redundancy**
that redundancy wherein all means for performing a required function are intended to operate simultaneously
[IEC 60050-191]

**3.1.2**
**area analysis**
study of man-product or man-machine interfaces with respect to the area where the work is performed

**3.1.3**
**black box**
representation of an item whereby its internal composition is not essential to understand its function, and only its interface characteristics are considered

**3.1.4**
**cold redundancy**
term used to indicate a standby redundancy where the redundant means is not powered, and thus to allow the differentiation of failure rates (on or off)

**3.1.5**
**criticality**
combined measure of the severity of a failure mode and its probability of occurrence

**3.1.6**
**design FMEA/FMECA**
FMEA/FMECA in which a product design is analysed and item failure modes and effects on the product operation are examined

NOTE A design FMEA/FMECA is performed as functional FMEA/FMECA or hardware FMEA/FMECA.

**3.1.7**
**failure propagation**
any 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

**3.1.8**
**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. The potential failure modes are classified according to their severity
[IEC 60050-191]

**3.1.9**
**failure mode, effects and criticality analysis (FMECA)**
FMEA extended to classify potential failure modes according to their criticality
[IEC 60050-191]

**3.1.10**
**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.

**3.1.11**
**functional FMEA/FMECA**
FMEA/FMECA in which the functions, rather than the items used in their implementation, are analysed

**3.1.12**
**hardware FMEA/FMECA**
FMEA/FMECA in which the hardware used in the implementation of the product functions is analysed

**3.1.13**
**hardware-software interaction analysis**
analysis to verify that the software is specified to react to hardware failures as required

**3.1.14**
**hot redundancy**
term used to indicate a standby redundancy where the redundant means is powered

NOTE An active redundancy is always hot.

**3.1.15**
**leak before burst**
fracture mechanics design concept in which it is shown that any initial defect grows through the wall of a pressurized system and causes leakage prior to burst (catastrophic failure) at maximum design pressure (MDP)
[ECSS-E-30-01]

**3.1.16**
**process FMEA/FMECA**
FMEA/FMECA in which the processes (such as manufacturing, assembling and integration, pre-launch operations) are analysed, as well as the effects of their potential failures

**3.1.17**
**protection device**
device designated to perform a specific protective function
[adapted from "protection equipment" in IEC 60050-191]

**3.1.18**
**redundancy**
in an item, the existence of more than one means for performing a required function
[IEC 60050-191]

**3.1.19**
**severity**
measure of the worst potential consequences of a failure mode

**3.1.20**
**single point failure**
failure of an item which results in the unrecoverable failure of the analysed product

**3.1.21**
**standby redundancy**
that redundancy wherein a part of the means for performing a required function is intended to operate, while the remaining part(s) of the means are inoperative until needed
[IEC 60050-191]

## 3.2 Abbreviated terms

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

| Abbreviation | Meaning |
|---|---|
| **ASIC** | application specific integrated circuit |
| **CDR** | critical design review |
| **CIL** | critical item list |
| **CN** | criticality number |
| **DN** | detection number |
| **ECSS** | European Cooperation for Space Standardization |
| **EEE** | electrical, electronic and 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 |
| **HSIA** | hardware-software interaction analysis |
| **H/W** | hardware |
| **Mil-HDBK** | military handbook |
| **NPRD** | nonelectronic parts reliability data |
| **ORU** | orbital replaceable unit |
| **PCB** | printed circuit board |
| **PN** | probability (of occurrence) number |
| **RAMS** | reliability, availability, maintainability and safety |
| **RB** | requirements baseline |
| **RBD** | reliability block diagram |
| **SN** | severity number |
| **SOW** | statement of work |
| **S/W** | software |
| **Td** | detection time |
| **Tp** | propagation time |
| **Tr** | recovery time |
| **TS** | technical specification |

# 4

# Design FMEA/FMECA requirements

## 4.1 General requirements

a. The design FMEA/FMECA shall be initiated as an integral part of the early design process and shall be updated to reflect design changes.

b. The FMEA/FMECA results shall be used to update the product requirements and to drive its design along the project life cycle.

   The analysis provides an essential contribution to the development of the product architecture and to the definition of the test and operation procedure.

c. The analysis shall be used to identify critical items and to provide recommendations for corrective action.

   Critical items are defined in subclause 4.4.

d. The FMEA/FMECA shall also be used to define special test considerations, preventative maintenance actions, operational constraints, useful life, and other pertinent information and activities necessary to minimize failure risk.

e. For all critical items all recommended actions which result from the FMEA/FMECA shall be evaluated and formally dispositioned by appropriate implementation or if the decision is for no action, a documented rationale is recorded.

f. The following discrete steps shall be used in performing the analysis:

   1. Define the product (i.e. function or hardware) to be analysed. Complete product definition includes identification of interface functions, expected performance, product restraints and failure definitions. Functional descriptions of the product shall include all tasks to be performed for each mission, mission phase and operational mode. When required the functional analysis shall be used as input for product definition.
   2. Prepare functional and reliability block diagrams which illustrate the operation, interrelationships and interdependencies of the items which constitute the product. All product interfaces shall be indicated.
   3. 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.
   4. Evaluate each failure mode in terms of the worst potential consequences and assign a severity category.

5. Assess the probability of occurrence of each identified failure mode and assign a criticality category (step limited to the FMECA).
6. Identify failure detection methods and existing compensating provisions for each failure mode.
7. Identify for all critical items corrective design or other actions (such as operator actions) required 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. Record all critical items into a dedicated table which shall be an input to the overall project critical item list (CIL).

   A failure effect severity list (FESL) should be prepared according to subclause 4.7.1.

## 4.2 Severity categories

a. A severity category classification shall be assigned to each identified failure mode analysed. Severity categories are assigned without consideration of existing compensating provisions to provide a qualitative measure of the worst potential consequences resulting from item failure. The number identifying the severity category shall be followed by a suffix in the following cases:

   1. The suffix S shall be used to indicate safety impacts.
   2. The suffix R shall be used to indicate redundancy.

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

b. The severity categories that shall be applied at the different levels of analysis are given in Table 1.

   The customer may tailor these severity categories to suit his or her individual programme.

   The evaluation of the severity of consequences at lower levels is limited to the interfaces of the analysed product. The consequences are then reassessed by the upper level analysts.

c. Criteria for mission loss (e.g. loss of one or more essential mission objectives), mission degradation, functionality loss and functionality degradation shall be defined by the customer.

## 4.3 Criticality ranking (only for FMECA)

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. The SN shall be consistent with the severity category assigned to the failure mode. The existence of redundancy does not affect the severity classification and therefore relevant severity number. The highest numbers shall indicate the most severe categories.

c. The SNs shown in Table 2 shall be used.

**Table 1: Severity categories applied at the different levels of analysis**

| SYSTEM LEVEL FMEA/FMECA | |
|---|---|
| **Severity category** | **Failure effect** |
| Catastrophic 1S | • Loss of life, life threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system.<br>• Loss of launch site facilities.<br>• Long-term detrimental environmental effects. |
| Catastrophic 1 | • Loss of system. |
| Critical 2S | • Temporary disabling but not life threatening injury, or temporary occupational illness.<br>• Loss of, or major damage to other flight systems, major flight elements, or ground facilities.<br>• Loss of, or major damage to public or private property.<br>• Short-term detrimental environmental effects. |
| Critical 2 | • Loss of mission. |
| Major 3 | • Mission degradation. |
| Negligible 4 | • Any other effect. |
| **SUBSYSTEM/ASSEMBLY/EQUIPMENT LEVEL FMEA/FMECA** | |
| **Severity category** | **Failure effect** |
| Catastrophic 1S | • Loss of life, life threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system.<br>• Loss of launch site facilities.<br>• Long-term detrimental environmental effects. |
| Catastrophic 1 | • Propagation of failure to other subsystems/assemblies/equipment. |
| Critical 2S | • Temporary disabling but not life threatening injury, or temporary occupational illness.<br>• Loss of, or major damage to other flight systems, major flight elements, or ground facilities.<br>• Loss of, or major damage to public or private property.<br>• Short-term detrimental environmental effects. |
| Critical 2 | • Loss of functionality. |
| Major 3 | • Degradation of functionality. |
| Negligible 4 | • Any other effect. |

**Table 2: Severity numbers applied at the different severity categories**

| **Severity category** | | **SN** |
|---|---|---|
| 1S, 1 | catastrophic | 4 |
| 2S, 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.

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

e. The **qualitative approach** shall be used if specific failure rate data are not available.

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. Each level shall be identified by a probability number (PN), i.e. the probability of occurrence.

For system level FMECA the probability of occurrence levels, limits of the levels and relevant PNs are as shown in Table 3.

**Table 3: Probability levels, limits and numbers (for system)**

| Level | Limits | PN |
|---|---|---|
| Probable | P > 10E-2 | 4 |
| Occasional | 10E-4 < P ≤ 10E-2 | 3 |
| Remote | 10E-5 < P ≤ 10E-4 | 2 |
| Extremely remote | P ≤ 10E-5 | 1 |

The customer may tailor the probability levels to the individual programme through specific requirements.

For lower level FMECAs the customer shall allocate the probability limits to be consistent with the above table.

f. When required by the SOW the **quantitative approach** shall be used when specific failure rates and probability of occurrence data are available. Data sources shall be listed. They shall be the same as those used for the other dependability analyses performed for the programme.

g. The failure probabilities shall be ranked as above and relevant entry (the PN) listed in the FMECA worksheet column.

h. 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. It shall be calculated as the product of the ranking assigned to each factor:

$$CN = SN \times PN$$

i. 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.

## 4.4 Identification of critical items

An item shall be considered a critical item if the failure mode is classified as:

a. from FMEA: severity categories 1S, 1, 2S, and 2;

b. from FMECA: CN ≥ 8.

The severity or criticality classification defining a failure mode as critical may be tailored according to programme specific needs.

## 4.5 Level of analysis

The level of analysis to which failure modes shall be assessed shall be down to the level agreed between the contractor and the next higher level customer. The agreed level of analysis shall be in conformance with the following:

a. All failure modes leading to consequences with severity category 1S, 1, 2S, and 2 at system level shall be analysed down to a level to identify all single point failures.

b. If the relevant items are protected by a protection device the effectiveness of such device shall be verified.

c. All failure modes leading to consequences with severity category 1SR, 1R, 2SR, and 2R at system level shall be analysed down to a level to ensure that the redundancy is effective.

## 4.6 Detailed requirements

a. All mission phases and related operational modes shall be addressed by the FMEA/FMECA.

b. Combinations of failures shall not be considered except in the following cases:

   1. Where a single item failure is non-detectable (e.g. due to the existence of an active redundancy or a protection device) the analysis shall be extended to determine the effects of additional failure(s), occurring in the relevant redundancy or protected item, which in combination with the first hidden failure can lead to catastrophic or critical consequences (at system level).

   2. The failure of emergency, caution and warning devices shall be analysed in combination with failures whose occurrence is monitored by these devices.

c. 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) for each operational phase or operational mode in which the item is used.

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

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

f. ASICs, integrated circuits, and software shall be treated as “black boxes”. These items can be split into more than one black box.

g. Software reactions to hardware failures shall be addressed by the hardware-software interaction analysis (HSIA).

   Human errors shall be highlighted where human performance is a significant contributor to mission success or safety. In such cases the FMEA/FMECA should invoke the requirement for the performance of a human error effects analysis and a task analysis.

h. The time between the occurrence of the failure and the manifestation of the irreversible consequences (propagation time, Tp) shall be estimated for catastrophic and critical failure consequences.

i. The time between the occurrence of a failure and the detection of the failure through the observable symptoms (detection time,Td) shall be estimated for catastrophic and critical failure consequences.

j. The maximum time available from the observation of the failure to the completion of recovery action (recovery time, Tr) shall be estimated for catastrophic and critical failure consequences.

k. Failures for which $Td + Tr \geq Tp$ shall be identified as time critical failures.

l. In the late project phases, when the physical layout of the equipment and subsystems is defined, additional product design aspects, which were not considered in the FMECAs of the early phases, shall be included in the hardware FMECA.

For electronic equipment and or subsystems, typical additional product design aspects are:

- failure modes resulting from the location of the components, such as failure propagation due to components being mounted too close to each other (e.g. heat transfer, capacitance);
- failure modes resulting from wiring layout, such as inadequate connector pins allocation (e.g. redundant paths on adjacent pins), solder joints and PCB conductive tracks;
- failure possibility due to unintentional exchange of components during assembly, e.g. mix-up of connectors;
- failure modes resulting from multi-application of individual components, e.g. use of one integrated circuit for two redundant paths;
- failure modes which can result in: contamination, explosion, high temperature, vibration, shock, or chemical attack;
- failure modes due to inadequate grounding or shielding;
- failure modes associated with the use of dissimilar metals.

Table 4 shows examples of check-list items that should be used for electronic equipment or subsystems.

**Table 4: Example of a product design failure modes check-list for electronic equipment or subsystems**

| Design failure modes | yes/no |
|---|---|
| Short circuit of adjacent connector pins. | |
| 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). | |

## 4.7 FMEA/FMECA report

### 4.7.1 Contents

The results of the FMEA/FMECA shall be documented in a report containing:

a. Cover sheet – title of the analysis and unique reference number, issue, revision and date, contractor sign-off date, and the names and signatures of the analyst(s) and the approval authority.

b. Introduction – concise statements on the objectives of the analysis including definition of the level of the analysis.

c. Design – definition of the status of the design of the product under analysis by reference to a configuration document. 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.

d. Product – a narrative description of the product functions and performance and of each lower level function considered in the analysis to provide an understanding of the analysis. Functional partition in the design between hardware and software, including a reference to the corresponding HSIA shall be addressed.

e. 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. 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.

f. Incomplete design – description and listing of any incomplete design areas.

g. Ground rules and assumptions – description of the ground rules adopted for the analysis (including list of items omitted from the analysis) and all the assumptions made regarding, for example, mission phases and times, operational modes, environmental conditions and failure criteria.

h. Failure detection or isolation criteria – describe the FDIR policy and criteria including reference to relevant documents and to telemetry measurement lists.

i. Reference documents – list the documents, including subcontractors analyses, used in the preparation of the FMEA/FMECA.

j. Acronyms and abbreviations – a list of acronyms, abbreviations and definitions of special terms used.

k. Results and recommendations – conclusions and recommendations based upon the detailed analysis presented by the FMEA/FMECA worksheets.

l. Critical items – list all the critical items identified. Item identification and cross-reference with FMEA/FMECA worksheets shall be provided.

m. Failure effect summary – a summary of the failure effects leading to consequences listed in severity category 1 and 2 and identify all relevant failure modes. Item identification and cross-reference with FMEA/FMECA worksheets shall be provided.

n. Status on recommendations – provide visibility on status of recommendations from previous issues of the analysis, stating whether implemented or not (in this case rationale shall be provided) and referencing, for example, the appropriate action item list and minutes of meeting.

o. FMEA/FMECA worksheets.

### 4.7.2 Worksheet

a. The documentation of the FMEA/FMECA shall be accomplished by completing the columns of the customer-approved worksheet.

   An example of FMEA worksheet is shown in Figure 1. Two examples of FMECA worksheets are shown in Figures 2 and 3. These worksheets should be used, but they are not mandatory.

b. Each FMEA/FMECA worksheet shall include in the header basic information including:

   1. The identity of the project of which the product under analysis is part (the project phase should also be identified).
   2. The identity of the product (hardware or function).
   3. The identity of corresponding equipment, subsystem, and system (as applicable).
   4. The identity of the analyst(s) who performed the analysis and of the approval authority.
   5. The identification of the analysis (i.e. document reference number, issue and date, number of pages).

   The mission phase or operational mode may also be identified in the header.

c. The FMEA/FMECA worksheet shall provide the following data elements:

   1. **Identification number**

      The identification number shall be assigned for traceability purposes.

   2. **Item/block**

      The name of the item or function being analysed shall be listed.

      The block of the reliability block diagram that is applicable to the analysis entry shall be identified.

   3. **Function**

      A concise statement of the function performed by the item shall be listed.

   4. **Failure mode**

      All potential failure modes of the item or function under analysis shall be identified and described.

   5. **Failure cause**

      The most probable cause associated with the assumed failure mode shall be identified and described. Since a failure mode can have more than one cause, all potential independent causes for each failure mode shall be identified and described. The failure cause should not be identified when components are analysed (equipment level FMEA/ FMECA).

   6. **Mission phase/Operational mode**

      A concise statement of the mission phase and operational mode in which the failure is assumed to occur. These elements may 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.

7. **Failure effects**

   The consequences of each assumed failure mode shall be identified and recorded at the following levels:

   (a) 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 shall be 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.

   (b) End effects

   End effects define the effect that the assumed failure mode has on the operation, function, or status of the product under investigation and its interfaces. The data shall be detailed to allow integration into the next higher level FMEA/FMECA.

8. **Severity classification**

   A severity classification category shall be assigned to each failure mode according to the worst potential end effect of the failure (see subclause 4.2).

9. **Failure detection method - Observable symptoms**

   A description by which occurrence of the failure mode is detected or observed shall be recorded. The failure detection means, such as visual or audible warning devices, sensing instrumentation, other unique indications (e.g. the failure effect itself), or none, shall be identified.

10. **Compensating provisions**

    The existing compensating provisions, such as design provisions or operator actions, which circumvent or mitigate the effect of the failure shall be identified, evaluated and recorded.

    (a) 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.

    (b) Operator actions

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

11. **Severity number** (only for FMECA)

    A severity number (SN) shall be given to each assumed failure mode. The SN shall be consistent with the severity category assigned to the failure mode (see subclause 4.3).

12. **Failure mode probability** (only for FMECA)

    An assessment of the probability of occurrence of the assumed failure mode shall be made and a relevant PN given (see subclause 4.3).

13. **Criticality number** (only for FMECA)

    A criticality number (CN) shall be given to each assumed failure mode. The CN shall be derived from the severity of the failure effects and the probability of the failure mode occurrence. It shall be calculated as the product of the rankings assigned to each factor (see subclause 4.3).

14. **Corrective actions**

    Corrective actions shall be defined for all critical items as defined in subclause 4.4. All actions shall be entered into an action item list which ensures control of a follow-up until the action is closed. If a catastrophic or critical failure mode cannot be eliminated, justification shall be provided showing that all reasonable actions have been implemented which allow the acceptance of the design. The rationale for acceptance of these failure modes, including design features, tests and inspections accomplished and historical information on the design or a similar design, shall be documented.

15. **Remarks**

    Any pertinent remarks relevant to and clarifying any other column in the worksheet line shall be noted.

| FAILURE MODES AND EFFECTS ANALYSIS (FMEA) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Product:<br>Project/Phase:<br>System/Subsystem/Equipment: | | | | | Prepared by:<br>Approved by:<br>Date: | | | Document reference:<br>Issue:<br>Page of | | | |
| Ident. number | Item/ block | Function | Failure mode | Failure cause | Mission phase/ Op. mode | Failure effects a. Local effects b. End effects | Severity | Failure detection method/ observable symptoms | Compensation provisions | Correction actions | Remarks |
| | | | | | | | | | | | |

**Figure 1: FMEA worksheet**

| FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS (FMECA) | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Product:<br>Project/Phase:<br>System/Subsystem/Equip-ment: | | | | | Prepared by:<br>Approved by:<br>Date: | | | | Document reference:<br>Issue:<br>Page of | | | | | |
| Ident. number | Item/ block | Function | Failure mode | Failure cause | Mission phase/ Op. mode | Failure effects a. Local effects b. End effects | Severity | Failure detection method/ observable symptoms | Compensation provisions | Severity Number SN | Probability and PN | Criticality Number CN | Correction actions | Remarks |
| | | | | | | | | | | | | | | |

**Figure 2: FMECA worksheet (example 1)**

| FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS (FMECA) | | | |
|---|---|---|---|
| Product: | System: | Prepared by: | Document ref.: |
| Project: | Subsystem: | Approved by: | Issue: |
| Phase: | Equipment: | Date: | Page of |
| Id. Number: | Item/block: | | |
| Function: | | | |
| Failure mode: | | | |
| Failure cause: | | | |
| Mission phase/Operational mode: | | | |
| Failure effects: a. Local effects<br>b. End effects | | | |
| Severity: | | | |
| Probability and PN: | | SN: | CN: |
| Failure detection method/Observable symptoms: | | | |
| Compensating provisions: | | | |
| Corrective actions: | | | |
| Remarks: | | | |

**Figure 3: FMECA worksheet (example 2)**

## 4.8 Implementation requirements

### 4.8.1 General requirements

This subclause establishes requirements concerning the implementation of FMEA/FMECA in each project phase.

For the project phase definition refer to ECSS-M-30.

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

   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.

   The means of recording shall be agreed by the customer. On request these records shall be made available to the customer.

### 4.8.2 Phase 0: Mission analysis or requirements identification

The FMEA/FMECA process need not be applied during Phase 0.

### 4.8.3 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.

   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:
   - The mission requirements. In particular the dependability and safety requirements shall be considered.
   - The design documentation of the different product concepts identified in phase 0.
   - The hierarchical decomposition of the product functions. The function decomposition is generally derived from the functional analysis.

c. The FMEA/FMECA shall be performed to provide the following results:
   - evaluation of the conformance of each design concept function to the system dependability and safety requirements;
   - identification of the features (e.g. functional redundancies or inhibits, possible alternative implementations) to be implemented for each analysed function in order to meet the system dependability and safety requirements.

### 4.8.4 Phase B: Preliminary definition

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

b. Rationale for selection of the approach shall be provided. The following criteria shall be considered in the selection:
   - available design data;
   - product complexity and level of integration;
   - criticality of the product or function;
   - segregation of function.

c. The FMEA/FMECA shall:
   - support the trade-offs from the dependability and safety point of view;

- 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 (e.g. system or subsystem specification and performance specification). In particular the dependability and safety requirements shall be considered.
   3. The current hierarchical decomposition of the system functions. The function decomposition is generally derived from the functional analysis.
   4. The design of the product architecture (e.g. 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 orbital replaceable unit (ORU) definition.
   7. When available, FMEA/FMECAs performed at lower integration level.
   8. Item failure rates from databases agreed by the customer.

e. The FMEA/FMECA shall be performed to provide the following results:
   1. List of dependability and safety requirements to be allocated to the product and lower levels for implementing the prevention and compensation methods and for avoiding the single point failures.
   2. Input to safety analyses: identification of hazardous consequences due to failures at lower levels and relevant identified prevention and compensation methods.
   3. Where applicable, input to maintainability analyses, e.g. identification of ORU for meeting the dependability and safety requirements.
   4. Input to software criticality analysis, e.g. identification of function failure consequences to be used as support in defining the effects of functional software failures.
   5. Input to the critical function list or critical item list, e.g. identification of the critical items as defined in subclause 4.4.
   6. Input for developing the FDIR system.

      For each hardware or function failure mode, the FMEA/FMECA shall identify as observable symptoms the telemetry parameters that are generated following the occurrence of the failure (e.g. warning signal, sensor information, equipment status and current and voltage monitors). When available as design information, the FMEA/FMECA shall provide the precise monitor in terms of acquisition channel name.

      The monitor lists, identified by the FMEA/FMECA for each failure mode, shall be provided as input for the FDIR development to allow the definition of algorithms, which can locate any occurred failure in front of the registered telemetry signals.
   7. Input to operation definition activity, e.g. identification of crew and system operations to be implemented to prevent or control critical dependability and safety events.

### 4.8.5 Phase C: Detailed definition

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

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

b. The FMEA/FMECA shall:

- Verify that the dependability and safety requirements, allocated to all of the project levels (system, subsystem and lower levels) in phase B, have been effectively and correctly implemented in the architecture.
- Verify the FDIR capabilities.

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 system functions as derived from the updated functional analysis.
4. The detailed system mission profile (definition of the mission phases or modes).
5. The detailed system architecture (design description, drawings, interfaces description).
6. The detailed description of hazard causes and hazard control implementation in the system architecture from the system safety analysis.
7. Definition of the system Orbital Replaceable Units from the maintenance analysis.
8. Item failure rate from databases (e.g. MIL-HDBK-217 F and Nonelectronic Parts Reliability Data - NPRD).
9. Definition of the crew and product operations.
10. Definition of the 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 (e.g. 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 impractical.
4. Input to safety analyses, e.g. identification of the implemented preventing or compensating methods for each identified hazardous consequence.
5. Input to the critical function list or critical item list, e.g. identification of the items (component or equipment) to be considered critical according to the provided criticality definition.
6. Input to the FDIR system definition activity for verifying the correct implementation. In particular, for each item (component or equipment) failure mode, the FMEA/FMECA shall list as observable symptoms the specific monitor parameters that allow the failure to be discovered, and

shall verify the capability of the recovery methods to control the failure consequences effectively.

Feedback to the FDIR development activity shall be provided in terms of:

— assurance of the corrective methods efficiency or proposal of alternative methods;

— identification of failure modes that are not monitored.

7. Input to operation definition activity, e.g. 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 applicable at the analysed integration level).

   EXAMPLE 1 List of failure modes with relevant effects and observable symptoms provided for generating test requirements and procedures.

   EXAMPLE 2 Identification of functional paths and redundancies that cannot be tested.

9. Input to user manual and operation procedures.

   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, checkout and mission use.

### 4.8.6 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.

### 4.8.7 Phase E: Utilization

The FMEA/FMECA performed at system level in phase C/D shall be utilized as support to in-flight diagnostic activities and shall be updated following in-flight contingencies in order to support the system maintenance and restoring.

### 4.8.8 Phase F: Disposal

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 (e.g. material, radiation) to define system disposal activities.

## 4.9 Integration requirements

This subclause establishes requirements concerning the integration of FMEA/FMECAs of different integration levels and of different project phases.

a. All FMEA/FMECAs of the lower level products shall be integrated into the FMEA/FMECA of the associated higher level product (see Figure 4).

b. The customer shall communicate to the contractor the information about the severity of failure modes at his level.

c. In his FMEA/FMECA the contractor shall consider the failure modes identified by his customer as failure effects.

d. All end effects of a lower level FMEA/FMECA shall become failure modes of the higher level FMEA/FMECA (see Figure 5).

e. All failure modes related to the end effect of a specific lower level FMEA/FMECA shall become failure causes of the associated failure mode of the higher level FMEA/FMECA (see Figure 5).

f. Additional failure modes shall be introduced at any level if missing from lower level FMEA/FMECAs.

g. All failure causes derived from lower level failure modes shall be checked if they are common causes of higher level failure modes integrated from different lower level FMEA/FMECAs.

h. The effect of operational and failure behaviour of specific parts or equipment (e.g. temperature, vibration, movement, power demand and heat flow) on other parts or equipment shall be assessed with regard to the physical layout of their mechanical, electrical and thermal interface.

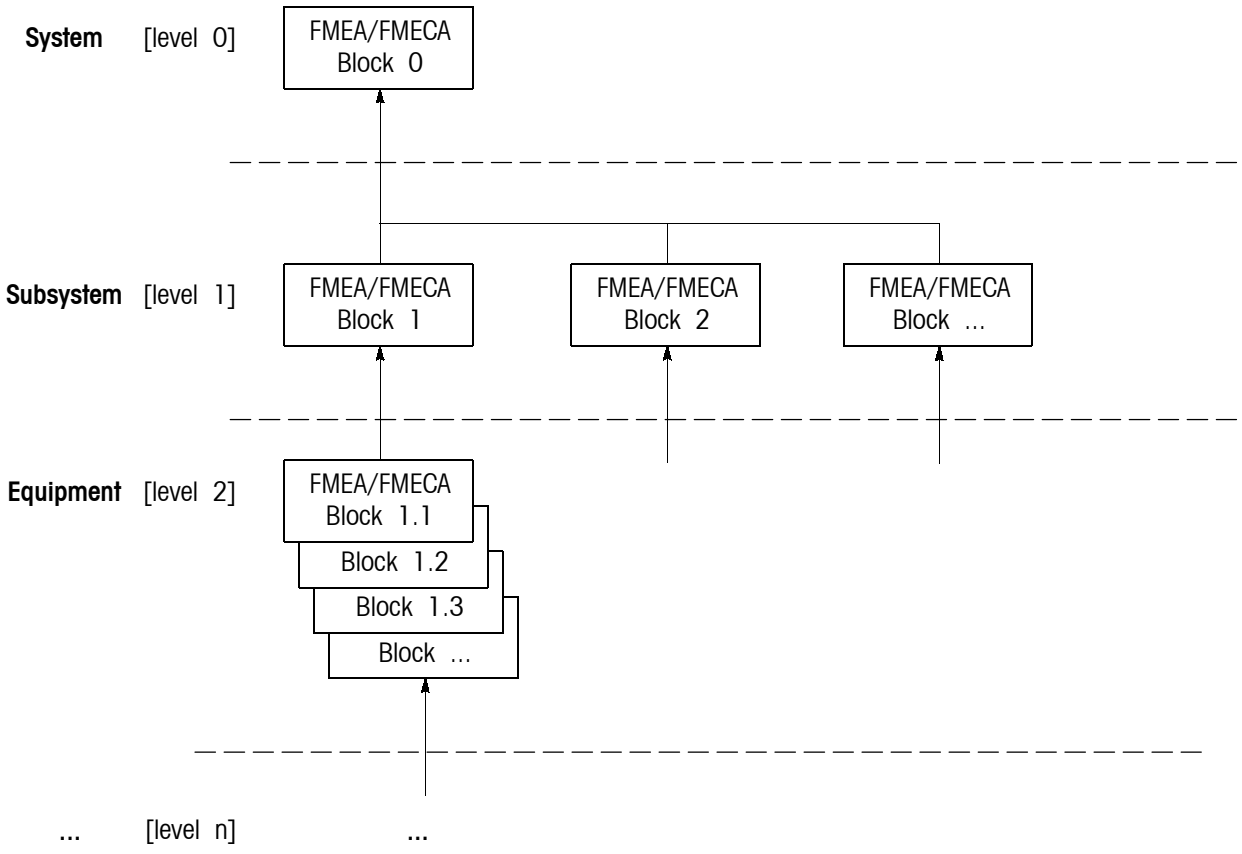


**Figure 4: Schematic of lower level FMEA/FMECAs products which integrate into the FMEA/FMECA of the associated higher level product**

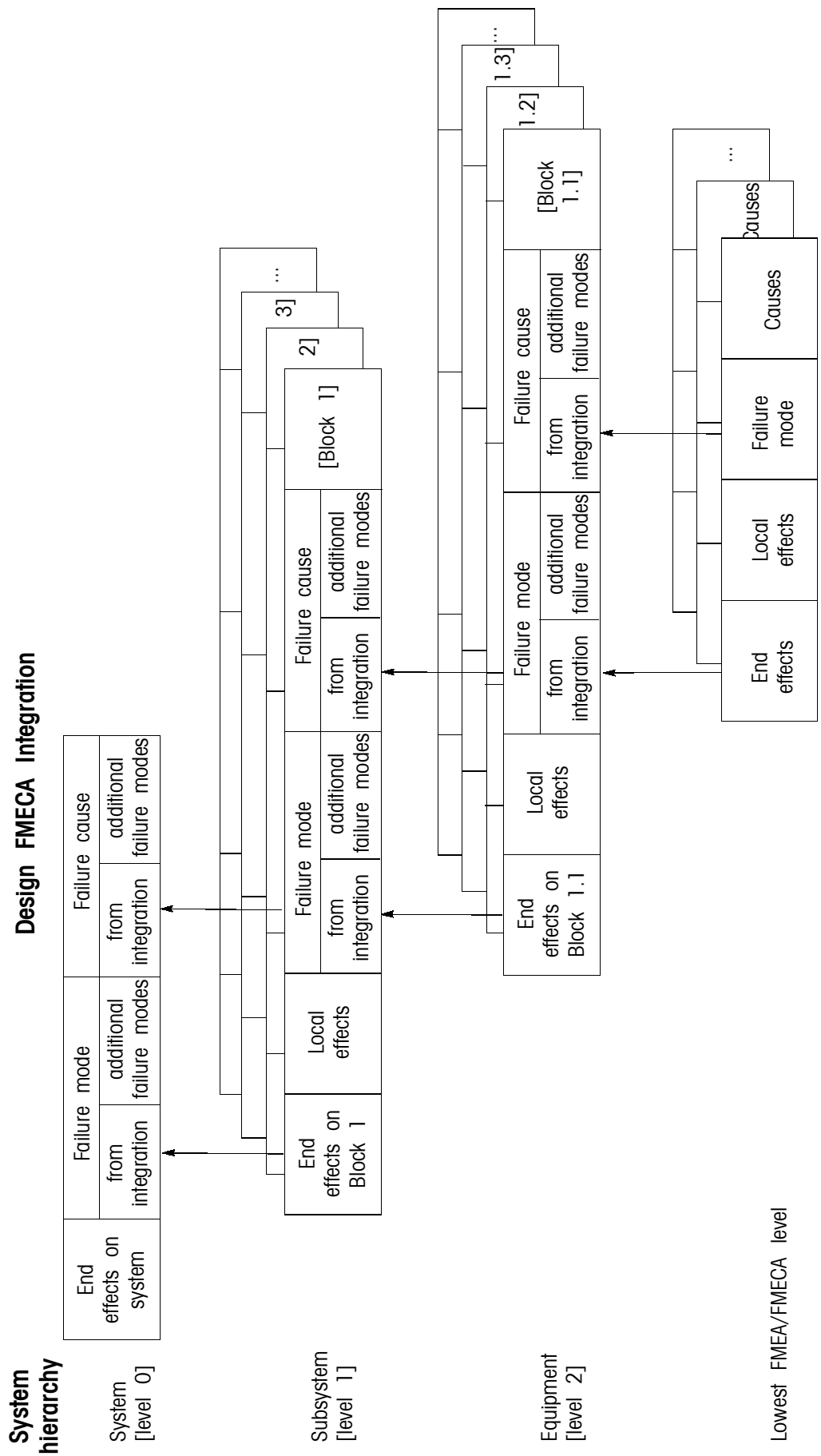


**Figure 5: Cause and effects of failure modes at different level FMEA/FMECAs**

## 4.10 Hardware-software interaction analysis (HSIA)

### 4.10.1 Purpose

HSIA is an activity to verify that software is specified to react to hardware failures as required.

### 4.10.2 Technical requirements

a. The HSIA shall be performed concurrently with the FMEA/FMECA for all hardware products involving software.

b. The HSIA shall consider all software which interacts with the hardware analysed in relevant FMEA/FMECA. The analysis shall be performed sufficiently early in the programme to influence the hardware design and the software requirements.

   Particular attention shall be paid to each failure mode of hardware which is:

   - involved in compensatory provisions (redundancy, protection);
   - controlled by software.

c. 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.
   For more details on RB and TS, see ECSS-E-40A annex A.2 and A.3.

d. The following information shall be considered for each failure mode:

   - Symptoms triggering the software action (parameters accounting for the failure mode). Refer to the RB or TS relevant section for justification.
   - Action of the software (failure isolation and recovery). Refer to the RB or TS relevant section for justification.
   - Effect of the software action on the product functionality (through induced possible sequence software-hardware effects).

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

   - inputs to the list of critical items (e.g. no or nonconforming software action and software action having adverse effects on hardware);
   - recommendations (e.g. hardware or software to be added or modified).

f. Nonconforming cases shall be identified and formally dispositioned.

g. The HSIA shall be documented by completing a form approved by the customer. The analysis may be provided in different formats:

   - Tabular form:
     each hardware failure mode is documented on a single table (see Figure 6).
   - Standard FMEA/FMECA worksheet:
     completed with the HSIA information (see Figure 1 and Figure 2) . Depending upon the specific case or application (e.g. not automatic or not continuously operating) the FMEA/FMECA considers separately software disabled and enabled in the following columns: effects, failure detection, recovery or compensation, severity or criticality.

h. The HSIA tabular form data elements that shall be provided are as follows:

   1. Subsystem or equipment: identification of subsystem or equipment submitted to HSIA.
   2. HSIA sheet number: HSIA running sheet number.
   3. FMEA/FMECA reference: identification of the reference number of the failure mode in the design FMEA/FMECA.
   4. Failure mode: summary of failure mode description.

5. TS/RB reference: reference to the software specification used for the HSIA (number, issue).
6. Identification of parameters used to trigger the software: identification of the information processed by the software to notify the presence of the failure or initiate an isolation or corrective action in response. Identification of corresponding health signal shall be added (health signal = result of comparison between detected and reference values).
7. TS/RB requirement number: requirement number in the TS/RB corresponding to the information at 4.10.2 h. 6.
8. Description of software (S/W) action: summary of the actions specified in TS/RB which are provided to negate the effects of or isolate the failure (isolation/recovery).
9. TS/RB requirement number: requirement number in the TS/RB corresponding to the information at 4.10.2 h. 8.
10. Description of the effect of the S/W action on the product functionality: summary of the effects of the actions taken by S/W (as described in TS/RB) on the functions of the product and on interfacing items.
11. Is there S/W action as specified?: the answer “yes” summarizes that the S/W action on the product functionality is conforming to the FDIR requirements for the product.
12. Identified adverse effects on hardware (H/W): description of any identified adverse effect (e.g. overstress of H/W, failure propagation).
13. Recommendations and remarks: recommendations in case of insufficient S/W actions or in case of adverse effect on H/W or any additional remark shall be recorded.

i. The FMEA/FMECA worksheet shall be completed as follows:

- in each completed column: for each failure mode where software is involved enter “S/W”;
- local/end effect: add point 10 of Figure 6;
- failure detection: add points 6 and 7 of Figure 6;
- recovery or compensation: add points 8 and 9 of Figure 6.

The HSIA can be performed with the aid of the check-list shown in Table 5. The questions may be tailored to the project.

j. Findings and recommendations arising from the HSIA shall be referenced in the applicable part of the FMEA/FMECA to maintain traceability.

| HARDWARE-SOFTWARE INTERACTION ANALYSIS (HSIA) | |
|---|---|
| 1. Subsystem/Equipment: | 2. HSIA sheet number: |
| 3. FMEA/FMECA reference: | 4. Failure mode: |
| 5. TS reference: | |
| 6. Identification of parameters used to trigger the S/W action: | 7. TS/RB requirement number: |
| 8. Description of S/W action: | 9. Reference to TS/RB section: |
| 10. Description of the effects of the S/W action on the H/W: | 11. Is there S/W action as specified? yes/no<br>12. Identified adverse effects |
| 13. Recommendations and remarks: | |

**Figure 6: HSIA tabular form**

**Table 5: HSIA check-list**

| HARDWARE-SOFTWARE INTERACTION ANALYSIS (HSIA) | | |
|---|---|---|
| Subsystem: | | FMECA number: |
| Item: | | Failure mode: |
| **No.** | **Question** | **yes/no** |
| 1a | Does the information provided to the on-board 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 on-board software can use to detect the failure? | |
| 1c | Are the answers to 1a and 1b consistent with the FMECA analysis of observable symptoms? | |
| 2a | Does the flight 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 cues, provided to signal 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: |
| 3. No S/W detection: | | 4. Detection during check-out: |
| 5. Accept rationale below: | | 6. Recommendations below: |
| 7. FMECA change recommended: | | |
| Comments: | | |

* circle number

# 5

# Process FMECA (Process risk analysis)

## 5.1 Purpose and objective

Process FMECA is the application of the FMECA methodology to processes. Its purpose is to identify potential weak points and to determine their effects on the product operation and the process itself.

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 weak points in processes or to reduce their criticality to an acceptable value. The process FMECA can be supported by analyses of the areas where the tasks are performed (area analysis).

## 5.2 Selection of processes and inputs required

Generally, this method is applied to the mission or safety critical processes as well as to processes which are critical from the programmatic point of view.

The inputs required 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).

## 5.3 Team and work organization

The analysis shall be performed by a small team including a member involved in the process to be analysed. The team should consist of an odd number of members to facilitate the decision process in the case of different opinions. One team member (e.g. RAMS engineer) coordinates the work of the team and chairs the meetings. He or she prepares the report and represents the team as its speaker.

The preparation for the meetings and the review of the necessary inputs should be performed by each team member individually, leading to a pre-selection of process steps (tasks) which are regarded as critical.

## 5.4 Method and worksheet

a. The potential weak points shall be evaluated by a (semi-quantitative) method as described in subclauses 5.5 and 5.6 in order to assess the resulting risk.

b. The documentation of the process FMECA shall be accomplished by completing the columns of the customer-approved worksheet. An example of worksheet is shown in Figure 7.

c. The following shall be identified in the worksheet header:
   - Project/subsystem/equipment;
   - Analysed process including the documentation reference of the applicable procedure;
   - Process FMECA documentation number and issue/revision status.

d. In the columns of the worksheet (see Figure 7), the analyst shall:

   1. **Identification number**

      Identify all process steps.

   2. **Item**

      Number the individual process steps.

   3. **Description**

      Describe the process step.

   4. **Failure mode/failure cause**

      Describe the assumed process step failure mode together with its causes.

   5. **Failure effects**

      1. the process, and
      2. the product involved.

      Describe all possible effects of the assumed failure modes on:

      — the process, and

      — the product involved.

   6. **Detection means**

      Describe the existing means and methods by which the effects can be detected.

   7. **Existing preventive or compensatory provisions**

      Describe the existing preventive or compensatory provisions to prevent the failure mode, to reduce its effects, or to reduce its probability of occurrence.

   8. **Severity**

      Identify the severity of a failure effect by assigning a severity number (SN) according to Table 6.

9. **Occurence**

   Identify the probability of occurrence of the failure mode by assigning a probability number (PN) according to the Table 7.

10. **Detection**

    Identify the probability of detection of the failure mode by assigning a detection number (DN) according to the Table 8.

11. **Criticality**

    Enter the criticality number (CN) by multiplying $SN \times PN \times DN$.

12. **Recommendations and remarks**

    Describe 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.

| Process Failure Modes, Effects and Criticality Analysis (FMECA) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Project/System/Subsystem/Equipment: | | | | Analysed process/Reference document: | | | Prepared by:<br>Approved by:<br>Date: | | | | Document ref.:<br>Issue:<br>Page of |
| Ident. number | Item | Description | Failure mode/ Failure cause | Failure effects:<br>1) process<br>2) product | Detection means | Existing preventive or compensatory provisions | Severity SN | Occurrence PN | Detection DN | Criticality CN | Recommendations and remarks |
| | | | | | | | | | | | |

**Figure 7: Process FMECA worksheet**

## 5.5 Determination of the criticality number (CN)

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:

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

The value of SN, PN, and DN are gained by votes of the team members (engineering judgement).

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 6: Severity numbers (SN) for severity of failure effects**

| SN | Definition |
|---|---|
| 4 | • Loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system.<br>• Loss of launch site facilities.<br>• Long-term detrimental environmental effects. |
| 3 | • Temporary disabling but not life-threatening injury, or temporary occupational illness.<br>• Loss of, or major damage to flight systems, major flight elements, or ground facilities.<br>• Loss of, or major damage to public or private property.<br>• Short-term detrimental environmental effects.<br>• Loss of system.<br>• Loss of mission. |
| 2 | • Mission degradation.<br>• Deterioration of the analysed process or of associated processes. |
| 1 | • Any other effect. |

**Table 7: Probability numbers (PN) for probability of occurrence**

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

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

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

## 5.6 Criticality acceptance criteria

The risk of a potential weak point is regarded as unacceptable and a recommendation for additional preventive or compensatory provisions shall be given if:

- the severity number SN ≥ 3
- the probability number PN = 4
- the detection number DN = 4
- the criticality number CN ≥ 12

Criticality acceptance criteria may be tailored to suit individual projects.

## 5.7 Recommendations for improvement

a. If the risk of a potential weak point is regarded as unacceptable (according to the criteria in subclause 5.6) a recommendation shall be given where feasible.

b. The failure mode 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. This shall be 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 subclause 5.6 are still not met, a second recommendation shall be 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. In this case ( e.g. because the severity of a failure effect cannot be modified) a justification for acceptability shall be given.

## 5.8 Reporting

A report shall be issued, containing as a minimum:

- a description of the analysed process (or reference to the appropriate documentation);
- the team members;
- the date and place of the meetings;
- the completed process FMECA worksheets;
- a list of recommendations for improvement;
- the follow-on actions.

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

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

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

## 5.9 Follow-on actions

All unacceptable weak points shall be compiled with the recommendations for improvement made in the process FMECA in the summary of the report and presented to the project team responsible for final decisions.

Decisions after consideration of the recommendations for improvement are:

(a) the recommendation shall be implemented, or

(b) the recommendation is rejected, or

(c) an alternative recommendation is made.

In the case of (a):

An actionee and a due date shall be entered for the implementation. The analysis result of the implementation shall be compared with the results leading to the original recommendation. In case of discrepancies, a clarification shall be entered and the relevant analysis steps shall be repeated. In case of no discrepancy, a close-out reference (e.g. the reference to the change notice) shall be entered.

In the case of (b):

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

The rationale is within the responsibility of the project.

In the case of (c):

An actionee and a due date shall be entered for the implementation of the alternative recommendation. The modified situation shall be treated on the same process FMECA worksheet to identify the improvements.

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

- acceptance according to (a), or
- rejection according to (b).

*(This page is intentionally left blank)*

# Bibliography

Informative documents are listed hereafter. They contain non-mandatory FMEA/FMECA requirements and validation information which are strongly recommended for use in order to achieve cost-efficient FMEA/FMECA assessments of space products.

| | |
|---|---|
| ECSS-E-30-01 | Space engineering — Fracture control |
| ECSS-E-40A | Space engineering — Software |
| IEC 60050-191 (1990-12) | International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service |
| IEC 60812 (1985-07) | International standard - Analysis techniques for system reliability - Procedure for Failure Mode and Effects Analysis (FMEA) |
| MIL-HDBK-217 F | Reliability prediction of electronic equipment |
| MIL-STD-1629A | Procedures for performing a Failure Mode, Effects and Criticality Analysis |
| NPRD | Non electronic parts reliability data |

*(This page is intentionally left blank)*

# ECSS Document Improvement Proposal

| 1. Document I.D. | 2. Document date | 3. Document title |
|---|---|---|
| ECSS-Q-30-02A | 7 September 2001 | Failure modes, effects and criticality analysis (FMECA) |

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

**5. Reason for recommendation**

**6. Originator of recommendation**

| Name: | Organization: | |
|---|---|---|
| Address: | Phone:<br>Fax:<br>e-mail: | **7. Date of submission:** |

**8. Send to ECSS Secretariat**

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

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

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

*(This page is intentionally left blank)*