

DIN EN 16602-30-02

ICS 49.140

**Raumfahrtproduktsicherung –
Fehlermöglichkeits-, Einfluss-(und Kritikalitäts-)Analyse
(FMEA/FMECA);
Englische Fassung EN 16602-30-02:2014**

Space product assurance –
Failure modes, effects (and criticality) analysis (FMEA/FMECA);
English version EN 16602-30-02:2014

Assurance produit des projets spatiaux –
Analyse des modes de defaillance, de leurs effets (et de leur criticite) (AMDE/AMDEC);
Version anglaise EN 16602-30-02:2014

Gesamtumfang 77 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (EN 16602-30-02:2014) wurde vom Technischen Komitee CEN/CLC/TC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-10-01 AA „Interoperabilität von Informations-, Kommunikations- und Navigationssystemen“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Dieses Dokument (EN 16602-30-02:2014) basiert auf ECSS-Q-ST-30-02C.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von EN 16602-30-02:2014.

Dieses Dokument wurde speziell zur Behandlung von Raumfahrtsystemen erarbeitet und hat daher Vorrang vor jeglicher Europäischer Norm, da es denselben Anwendungsbereich hat, jedoch über einen größeren Geltungsbereich (z. B. Luft- und Raumfahrt) verfügt.

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

3 Begriffe und Abkürzungen

3.1 Begriffe aus anderen Normen

Für die Anwendung dieses Dokuments gelten die Begriffe nach ECSS-S-ST-00-01.

Für die Anwendung dieses Dokuments gilt zudem die folgende Benennung nach ECSS-E-ST-32-02:

Leck vor dem Bersten

3.2 Für diese Norm spezifische Begriffe

3.2.1

aktive Redundanz

funktionsbeteiligte Redundanz

alle für die Ausführung einer geforderten Funktion notwendigen Komponenten sind simultan aktiv

[QUELLE: IEC 60050-191]

3.2.2

Bereichsanalyse

Untersuchung der Schnittstellen Mensch-Produkt oder Mensch-Maschine in dem Bereich, in dem Arbeiten durchgeführt werden

3.2.3

Kritikalität

Kritizität

Kombination des Maßes für die Schwere der Folgen eines potenziellen Fehlers mit der Wahrscheinlichkeit des Fehlerauftretens

3.2.4

End-Auswirkung

bei Betätigung und Funktion einer Einheit oder für den Zustand des untersuchten Produkts und seiner Schnittstellen eine Folge einer mutmaßlichen Fehlermöglichkeit

3.2.5

Fehlerursache

angenommene Ursache, die einer bestimmten Fehlermöglichkeit zuzuordnen ist

3.2.6

Fehlereinfluss

bei Betätigung und Funktion einer Einheit oder für den Zustand der Einheit eine Folge einer mutmaßlichen Fehlermöglichkeit

3.2.7

Fehlerausbreitung

physikalisches oder logisches, durch einen Fehler innerhalb eines Produkts verursachtes Ereignis, das zu einem oder mehreren weiteren Fehler(n) des Produkts außerhalb der Grenzen des betrachteten Produkts führen kann

3.2.8

Fehlermöglichkeits- und Einflussanalyse (FMEA)

Analyse, durch die jede potenzielle Fehlermöglichkeit in einem Produkt (oder in einer Funktion oder in einem Prozess) untersucht wird, um die Auswirkungen zu bestimmen

ANMERKUNG Die potenziellen Fehlermöglichkeiten werden nach der Bedeutung (Schwere) ihrer Folgen klassifiziert.

[QUELLE: IEC 60050-191]

3.2.9

Fehlermöglichkeits-, Einfluss- und Kritikalitäts-Analyse (FMECA)

FMEA, die zur Klassifizierung potenzieller Fehlermöglichkeiten nach ihrer Kritikalität erweitert ist

[QUELLE: IEC 60050-191]

3.2.10

Funktionsbeschreibung

narrative Beschreibung der analysierten Produktfunktionen und aller Funktionen auf einer niedrigeren Ebene in einer so ausreichenden Ausführlichkeit, dass das Verständnis für das Produkt und für die Analyse gegeben ist

ANMERKUNG In die Funktionsbeschreibung werden für alle funktionellen Baugruppen Darstellungen ihrer Funktion (z. B. Funktionsbäume, Funktions-Blockdiagramme und Funktionsmatrizen) auf einer Ebene einbezogen, die der Ausführlichkeit der Analyse und der Ausgereiftheit der Konstruktion entspricht.

3.2.11

Funktions-FMEA

FMEA, bei der die Funktionen und nicht die bei ihrer Durchführung verwendeten Einheiten analysiert werden

3.2.12

Funktions-FMECA

FMECA, bei der die Funktionen und nicht die bei ihrer Durchführung verwendeten Einheiten analysiert werden

3.2.13

Hardware-FMEA

FMEA, bei der die Hardware analysiert wird, die bei Durchführung der Produktfunktionen verwendet wird

3.2.14

Hardware-FMECA

FMECA, bei der die Hardware analysiert wird, die bei Durchführung der Produktfunktionen verwendet wird

3.2.15

Hardware/Software-Interaktionsanalyse

Analyse um zu verifizieren, ob die Software so festgelegt ist, dass die geforderte Reaktion auf Hardwarefehler erfolgt

3.2.16

Prozess-FMECA

FMECA, bei der die Prozesse unter Einbeziehung der Auswirkungen ihrer potenziellen Fehler analysiert werden

ANMERKUNG Unter Prozessen sind zu verstehen z. B. der Herstellungsprozess, der Montageprozess und der Integrationsprozess, die Operationen vor dem Start.

3.2.17

Schutzgerät

Gerät, das so ausgelegt ist, dass es eine bestimmte Schutzfunktion erfüllt

[angepasst aus IEC 60050-191 für „Schutzeinrichtung“]

English version

Space product assurance - Failure modes, effects (and criticality) analysis (FMEA/FMECA)

Assurance produit des projets spatiaux - Analyse des modes de défaillance, de leurs effets (et de leur criticité) (AMDE/AMDEC)

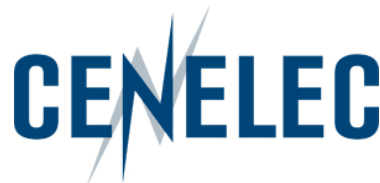
Raumfahrtproduktsicherung - Fehlermöglichkeits-, Einfluss- (und Kritikalitäts-) Analyse (FMEA/FMECA)

This European Standard was approved by CEN on 6 April 2014.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



CEN-CENELEC Management Centre:
Avenue Marnix 17, B-1000 Brussels

Table of contents

Foreword	5
Introduction.....	6
1 Scope.....	8
2 Normative references	9
3 Terms, definitions and abbreviated terms.....	10
3.1 Terms from other standards.....	10
3.2 Terms specific to the present standard	10
3.3 Abbreviated terms.....	12
4 FMEA requirements.....	13
4.1 General requirements	13
4.2 Severity categories	14
4.3 Identification of critical items	16
4.4 Level of analysis	16
4.5 Integration requirements	16
4.6 Detailed requirements.....	19
4.7 FMEA report	20
5 FMECA requirements	21
5.1 General requirements	21
5.2 Criticality ranking	21
5.3 Identification of critical items	23
5.4 FMECA report.....	23
6 FMEA/FMECA implementation requirements.....	24
6.1 General requirements	24
6.2 Phase 0: Mission analysis or requirements identification	24
6.3 Phase A: Feasibility	24
6.4 Phase B: Preliminary definition	25
6.5 Phase C: Detailed definition.....	27
6.6 Phase D: Production or ground qualification testing.....	30

6.7	Phase E: Utilization.....	30
6.8	Phase F: Disposal.....	30
7	Hardware-software interaction analysis (HSIA)	31
7.1	Overview	31
7.2	Technical requirements	31
7.3	Implementation requirements	32
8	Process FMECA.....	33
8.1	Purpose and objective	33
8.2	Selection of processes and inputs required	33
8.3	General process FMECA requirements	34
8.4	Identification of critical process steps.....	36
8.5	Recommendations for improvement	36
8.6	Follow-on actions.....	36
8.6.1	General	36
8.6.2	In case 1:	37
8.6.3	In case 2:	37
8.6.4	In case 3:	37
Annex A	(normative) FMEA/FMECA report – DRD.....	38
Annex B	(normative) FMEA worksheet – DRD	41
Annex C	(normative) FMECA worksheet – DRD	46
Annex D	(normative) HSIA form - DRD	50
Annex E	(normative) Process FMECA report – DRD	54
Annex F	(normative) Process FMECA worksheet – DRD	56
Annex G	(informative) Parts failure modes (space environment)	60
Annex H	(informative) Product design failure modes check list.....	71
Annex I	(informative) HSIA check list	72
Bibliography		73

Figures

Figure 4-1:	Graphical representation of integration requirements	18
Figure B-1 :	Example of FMEA worksheet	45
Figure C-1 :	Example 1 of FMECA worksheet	48
Figure C-2 :	Example 2 of FMECA worksheet	49

Figure D-1 : Example of HSIA form	52
Figure F-1 : Example of process FMECA	59
Figure G-1 : Two open contacts (relay stuck in intermediate position)	70
Figure G-2 : Two contacts in opposite positions	70
Figure G-3 : Short circuit between fix contacts	70
Figure I-1 : Example of HSIA check-list	72

Tables

Table 4-1: Severity of consequences.....	15
Table 5-1: Severity Numbers (SN) applied at the different severity categories with associated severity level	22
Table 5-2: Example of probability levels, limits and numbers.....	22
Table 5-3: Criticality matrix	23
Table 8-1: Example of Severity numbers (SN) for severity of failure effects.....	35
Table 8-2: Probability numbers (PN) for probability of occurrence	35
Table 8-3: Detection numbers (DN) for probability of detection.....	35
Table G-1 : Example of parts failure modes.....	60
Table G-2 : Example of relay failure modes.....	69
Table H-1 : Example of a product design failure modes check-list for electromechanical electrical equipment or assembly or subsystems.....	71

Foreword

This document (EN 16602-30-02:2014) has been prepared by Technical Committee CEN/CLC/TC 5 "Space", the secretariat of which is held by DIN.

This standard (EN 16602-30-02:2014) originates from ECSS-Q-ST-30-02C.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2015, and conflicting national standards shall be withdrawn at the latest by March 2015.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This document has been developed to cover specifically space systems and has therefore precedence over any EN covering the same scope but with a wider domain of applicability (e.g. : aerospace).

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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 constraints 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.

EN reference	Reference in text	Title
EN 16601-00-01	ECSS-S-ST-00-01	ECSS system – Glossary of terms
EN 16603-32-02	ECSS-E-ST-32-02	Space engineering – Structural design and verification of pressurized hardware
EN 16602-10-09	ECSS-Q-ST-10-09	Space product assurance – Nonconformance control system
EN 16602-30	ECSS-Q-ST-30	Space product assurance – Dependability

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.

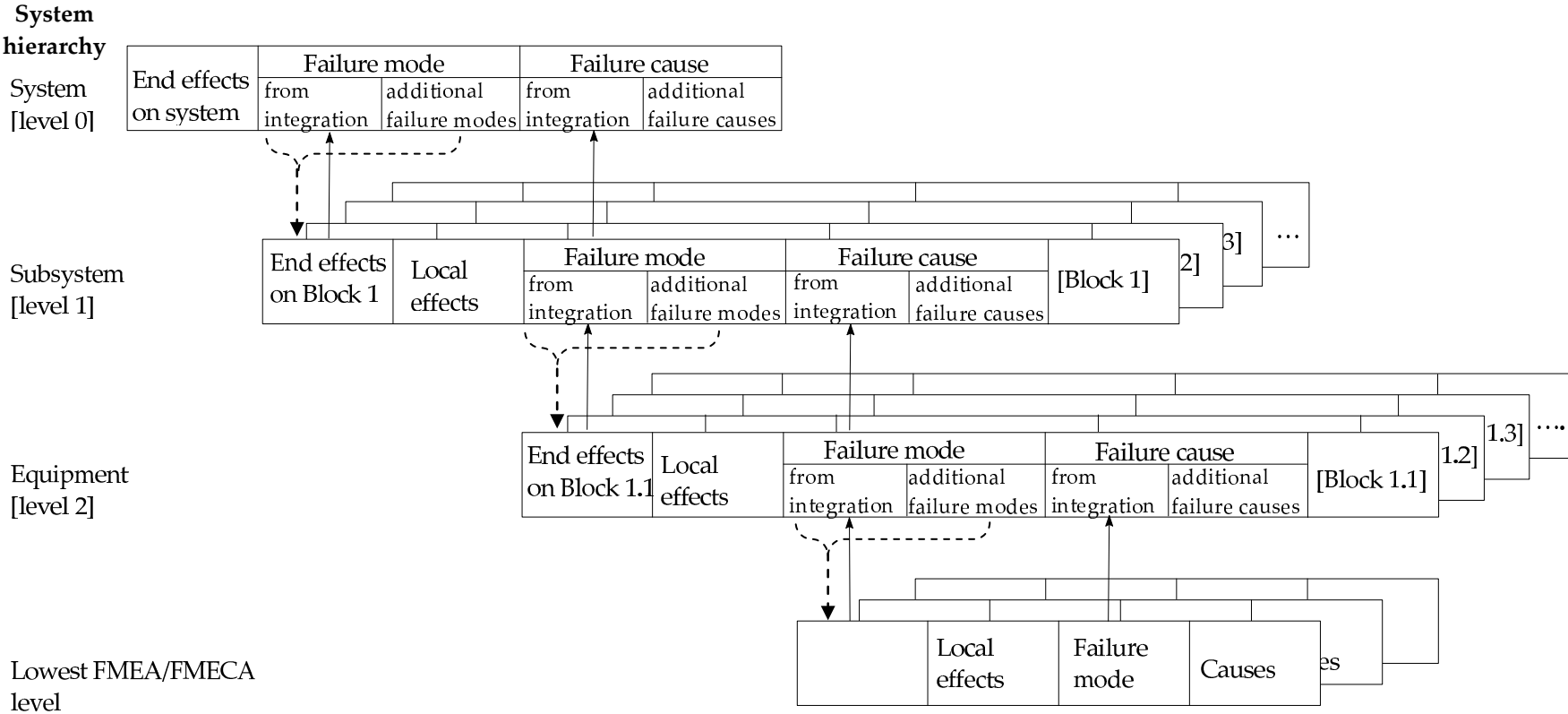
- f. Additional failure modes shall be introduced at any level if missing (as failure effects) from lower level FMEAs.
- g. At any level, additional failure causes, which can not be assessed at lower level as failure modes, shall be introduced into the FMEA.

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.