



NSAI
Standards

Irish Standard
I.S. EN 16602-30-02:2014

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

I.S. EN 16602-30-02:2014

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

EN 16602-30-02:2014

Published:

2014-09-17

*This document was published
under the authority of the NSAI
and comes into effect on:*

2014-10-04

ICS number:

49.140

NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

EUROPEAN STANDARD

EN 16602-30-02

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 2014

ICS 49.140

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)

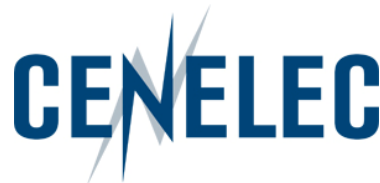
Raumfahrtproduktsicherung - Fehlermöglichkeits-, Einfluss- (und Kritikalitäts-) Analyse (FMEA/FMECA)

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

EN 16602-30-02:2014 (E)

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.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-