SLOVENSKI STANDARD
SIST EN 16602-30-02:2014

01-november-2014

Zagotavljanje varnih proizvodov v vesoljski tehniki - Analiza načinov odpovedi ter njihovih učinkov (in kritičnosti) (FMEA/FMECA)

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

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

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

Ta slovenski standard je istoveten z: **EN 16602-30-02:2014**

ICS:

49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST EN 16602-30-02:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16602-30-02

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 defaillance, de leurs effets (et de leur criticite) (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

Figures

Tables

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 constrains of a space project in conformance with ECSS-S-ST-00.

2
Normative references

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

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

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

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

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

leak-before-burst

3.2 Terms specific to the present standard

3.2.1 active redundancy

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

[IEC 60050-191]

3.2.2 area analysis

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

3.2.3 criticality

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

3.2.4 end effect

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

3.2.5 failure cause

presumed causes associated to a given failure mode

3.2.6 failure effect

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

3.2.7 failure propagation

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

3.2.8 failure mode and effects analysis (FMEA)

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

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

[IEC 60050-191]

3.2.9 failure mode, effects and criticality analysis (FMECA)

FMEA extended to classify potential failure modes according to their criticality

[IEC 60050-191]

3.2.10 functional description

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

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

3.2.11 functional FMEA

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

3.2.12 functional FMECA

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

3.2.13 hardware FMEA

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

3.2.14 hardware FMECA

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

3.2.15 hardware-software interaction analysis

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

3.2.16 process FMECA

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

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

3.2.17 protection device

device designated to perform a specific protective function

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

3.3 Abbreviated terms

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

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

4
FMEA requirements

4.1 General requirements

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

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

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

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

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

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

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

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

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

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

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