SLOVENSKI STANDARD
SIST EN 16602-40-02:2014

01-november-2014

Nadomešča:
SIST EN 14738:2004

Zagotavljanje varnih proizvodov v vesoljski tehniki - Analiza nevarnosti

Space product assurance - Hazard analysis

Raumfahrtproduktsicherung - Gefahrenanalyse

Assurance produit des projets spatiaux - Analyse de risques

Ta slovenski standard je istoveten z: **EN 16602-40-02:2014**

ICS:

03.100.40	Raziskave in razvoj	Research and development
49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST EN 16602-40-02:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16602-40-02

September 2014

ICS 49.140

Supersedes EN 14738:2004

English version

Space product assurance - Hazard analysis

Assurance produit des projets spatiaux - Analyse de risques

Raumfahrtproduktsicherung - Gefahrenanalyse

This European Standard was approved by CEN on 13 March 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 16602-40-02:2014) has been prepared by Technical Committee CEN/CLC/TC 5 “Space”, the secretariat of which is held by DIN.

This standard (EN 16602-40-02:2014) originates from ECSS-Q-ST-40-02C.

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 supersedes EN 14738:2004.

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

Safety analysis comprises hazard analysis, safety risk assessment and supporting analyses as defined in ECSS-Q-ST-40. The objective of safety analysis is to identify, assess, reduce, accept, and control safety hazards and the associated safety risks in a systematic, proactive, complete and cost effective manner, taking into account the project's technical and programmatic constraints. Safety analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases, and by changes to a given project baseline.

Hazard analysis comprises the identification classification and reduction of hazards. Hazard analysis can be implemented at each level of the customer-supplier network. Hazard analysis activities at lower level can contribute to system level safety analysis. System level safety analysis can determine lower level hazard analysis activities.

Hazard analysis interfaces with dependability analysis, in particular FMECA. Safety risk assessment interfaces with quantitative dependability analysis, in particular reliability analysis. Safety risk assessment contributes to project risk management. Ranking of safety risks according to their criticality for project success, allowing management to direct its attention to the essential safety issues, is part of the major objectives of risk management.

Safety risk assessment is further addressed in ECSS-Q-ST-40.

1
Scope

This Standard details the hazard analysis requirements of ECSS-Q-ST-40; it defines the principles, process, implementation, and requirements of hazard analysis.

It is applicable to all European space projects where during any project phase there exists the potential for hazards to personnel or the general public, space flight systems, ground support equipment, facilities, public or private property or the environment.

This standard may be tailored for the specific characteristics 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 16001-00-01	ECSS-S-ST-00-01	ECSS system — Glossary of terms
EN 16601-80	ECSS-M-ST-80	Space project management — Risk management
EN 16602-40	ECSS-Q-ST-40	Space product assurance — Safety

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, in particular for the following terms:

requirement

3.2 Terms specific to the present standard

3.2.1 consequence tree

set of hazard scenarios leading to the same safety consequence

3.2.2 detection time

time span between the occurrence of the initiator event and its detection through the observable symptoms

3.2.3 hazard

existing or potential condition of an item that can result in a mishap

NOTE 1 [ISO 14620 2]

NOTE 2 This condition can be associated with the design, fabrication, operation, or environment of the item, and has the potential for mishaps. [ISO 14620 2]

NOTE 3 Hazards are potential threats to the safety of a system. They are not events, but the prerequisite for the occurrence of hazard scenarios with their negative effects on safety in terms of the safety consequences.

3.2.4 hazard acceptance

decision to tolerate the consequences of the hazard scenarios when they occur

3.2.5 hazard analysis

systematic and iterative process of the identification, classification and reduction of hazards

3.2.6 hazard control

preventive or mitigation measure, associated to a hazard scenario, which is introduced into the system design and operation to avoid the events or to interrupt their propagation to consequence

3.2.7 hazard elimination

removal of a hazard from a particular hazard manifestation

3.2.8 hazard manifestation

presence of specific hazards in the technical design, operation and environment of a system

3.2.9 hazard minimization

substitution of a hazard in the hazard manifestation by another hazard of the same type but with a lower potential threat

NOTE For instance high toxicity to low toxicity.

3.2.10 hazard reduction

process of elimination or minimization and control of hazards

3.2.11 hazard scenario

sequence of events leading from the initial cause to the unwanted safety consequence

NOTE The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

3.2.12 hazard tree

set of hazard scenarios originating from the same set of hazard manifestations

3.2.13 hazardous

property of an item and its environment which provides the potential for mishaps

NOTE [ISO 14620 2]

3.2.14 observable symptoms

evidence that indicates that an undesirable event has occurred

NOTE Observable symptoms appear during the propagation time.

3.2.15 reaction time

time span between the detection and the occurrence of the consequence

NOTE This is the time span available for mitigating actions after detection of the occurrence of the initiator event.

3.2.16 residual hazard

hazard remaining after implementation of hazard reduction

3.2.17 resolved hazard

hazard that is reduced, the reduction verified and the hazard considered acceptable

NOTE Resolved hazards are submitted for formal acceptance.

3.2.18 scenario propagation time

time span between the occurrence of the initiator event and the occurrence of the consequence

3.2.19 severity of safety consequence

measure of the gravity of damage with respect to safety

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
CC&M	common cause and common failure mode analysis
DRD	document requirements definition
FMECA	failure modes, effects and criticality analysis
GSE	ground support equipment
NASA	National Aeronautics and Space Administration
OHA	operating hazard analysis
PHA	preliminary hazard analysis
SHA	system hazard analysis
SSHA	subsystem hazard analysis