SLOVENSKI STANDARD
SIST EN 16602-40:2018

01-julij-2018

Nadomešča:
SIST EN ISO 14620-1:2004

Zagotavljanje kakovosti proizvodov v vesoljski tehniki - Varnost

Space product assurance - Safety

Raumfahrtsysteme - Sicherheit

Systèmes spatiaux - Sécurité

Ta slovenski standard je istoveten z: EN 16602-40:2018

ICS:

49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST EN 16602-40:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16602-40

April 2018

ICS 49.140

Supersedes EN ISO 14620-1:2002

English version

Space product assurance - Safety

Assurance produit des projets spatiaux - Sécurité

Raumfahrtsysteme - Sicherheit

This European Standard was approved by CEN on 18 September 2017.

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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Table of contents

Figures

Tables

European Foreword

This document (EN 16602-40:2018) has been prepared by Technical Committee CEN/CLC/JTC 5 “Space”, the secretariat of which is held by DIN (Germany).

This document (EN 16602-40:2018) originates from ECSS-Q-ST-40C Rev.1.

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of an identical text or by endorsement, at the latest by October 2018, and conflicting national standards shall be withdrawn at the latest by October 2018.

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 ISO 14620-1:2002.

The main changes with respect to EN ISO 14620-1:2002 are listed below:

- new EN number,
- Complete and thorough review with the focus on simplification and streamlining to improve clarity and consistency of requirements.
- Applicability guidelines to the different space systems has been defined (see applicability matrix provided in Annex E).
- System safety programme requirements reworked, i.e. the system safety programme supports the risk management process described in EN 16601-80 (based on ECSS-M-ST-80C).
- Space debris mitigation streamlined.
- Atmospheric re-entry addressed.
- Safety design principles reworked.
- Safety risk reduction and control updated.
- Safety analysis requirements and techniques updated.
- Common scheme for consequence severity classification used in EN 16602-30 and EN 16602-40 (based on ECSS-Q-ST-30C and ECSS-Q-ST-40C).
- Identification and control of safety-critical functions updated.
- Established link to EN 1602-10-04 “Critical-item control” (based on ECSS-Q-ST-10-04).
- Informative annex on European legislation and ‘CE’ marking added (Annex F).
- DRDs revisited and updated.
- Document reworked to be in compliance with ECSS standards drafting rules.

This document has been prepared under a standardization request 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 organisations 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1
Scope

This Standard defines the safety programme and the safety technical requirements aiming to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with European space systems.

This Standard is applicable to all European space projects.

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 16603-10	ECSS-E-ST-10	Space engineering – System engineering general requirements
EN 16603-32-01	ECSS-E-ST-32-01	Space engineering – Fracture control
EN 16603-32-10	ECSS-E-ST-32-10	Space engineering – Structural factors of safety for spaceflight hardware
EN 16603-40	ECSS-E-ST-40	Space engineering – Software general requirements
EN 16601-10	ECSS-M-ST-10	Space project management – Project planning and implementation
EN 16601-40	ECSS-M-ST-40	Space project management – Configuration and information management
EN 16601-80	ECSS-M-ST-80	Space project management – Risk management
EN 16602-10	ECSS-Q-ST-10	Space product assurance – Product assurance management
EN 16602-10-04	ECSS-Q-ST-10-04	Space product assurance – Critical-item control
EN 16602-20	ECSS-Q-ST-20	Space product assurance – Quality assurance
EN 16602-30	ECSS-Q-ST-30	Space product assurance – Dependability
EN 16602-60	ECSS-Q-ST-60	Space product assurance – Electrical, electronic and electromechanical (EEE) components
EN 16602-70	ECSS-Q-ST-70	Space product assurance – Materials, mechanical parts and processes
EN 16602-80	ECSS-Q-ST-80	Space product assurance – Software product assurance

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

a. For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply (see in clause 3.2 differences for "fail safe" and "system"), in particular for the following terms:

1. accident
2. failure
3. catastrophic
4. critical <CONTEXT: safety>
5. emergency
6. ground segment
7. hazard
8. hazardous event
9. inhibit
10. risk
11. safety
12. safing
13. severity
14. safety-critical function
15. space segment
16. system

3.2 Terms specific to the present standard

3.2.1 cause

action or condition by which a hazardous event is initiated (an initiating event)

NOTE 1 The cause can arise as the result of failure, human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).

NOTE 2 This definition is specific to this Standard, when used in the context of hazard analysis.

3.2.2 criticality

classification of a function or of a software, hardware or operation according to the severity of the consequences of its potential failures

NOTE 1 Refer to clauses 6.4.1 and 6.5.6.

NOTE 2 This notion of criticality, applied to a function or a software, hardware or operation, considers only severity, differently from the criticality of a failure or failure mode (or a risk), which also considers the likelihood or probability of occurrence.

3.2.3 fail safe

property of a system (or part of it), which prevents its failures from resulting in critical or catastrophic consequences

3.2.4 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

3.2.5 hazardous command

command that can remove an inhibit to a safety-critical function or activate a hazardous subsystem

3.2.6 hazard reduction

process of elimination or minimization and control of hazards

3.2.7 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.

3.2.8 operator error

failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator

3.2.9 safety approval authority

entity that defines or makes applicable, for a given project, detailed technical safety requirements, and reviews their implementation

3.2.10 safety audit

independent examination to determine whether the procedures specific to the safety requirements are implemented effectively and are suitable to achieve the specified objectives

3.2.11 safety risk

measure of the threat to safety posed by the hazard scenarios and their consequences

NOTE 1 Safety risk is always associated with a specific hazard scenario or a particular set of scenarios. The risk posed by a single scenario is called individual scenario risk. The risk posed by a set of scenarios with the same top consequence is called overall risk.

NOTE 2 The magnitude of a safety risk is a combination of the severity and the likelihood of the consequence.

3.2.12 safety status parameter

parameter that makes it possible to assess the status of an implemented hazard control

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
AR	acceptance review
CCB	configuration control board
CDR	critical design review
CE	Conformité Européenne
CRR	commissioning result review
EEE	electronic, electrical, electromechanical
ELR	end-of-life review
EMC	electro-magnetic compatibility
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FSDP	flight safety data package
FRR	flight readiness review
FTA	fault tree analysis
GSDP	ground safety data package
GSE	ground support equipment
IEC	International Electrotechnical Commission
LRR	launch readiness review
LVD	low voltage directive