SLOVENSKI STANDARD
SIST EN 16602-30:2018

01-julij-2018

Zagotavljanje kakovosti proizvodov v vesoljski tehniki - Zagotovljivost

Space product assurance - Dependability

Raumfahrtproduktsicherung - Zuverlässigkeit

Assurance produit des projets spatiaux - Sûreté de fonctionnement

Ta slovenski standard je istoveten z: **EN 16602-30:2018**

ICS:

03.120.01	Kakovost na splošno	Quality in general
49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST EN 16602-30:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16602-30

April 2018

ICS 49.140

English version

Space product assurance - Dependability

Assurance produit des projets spatiaux - Sûreté de fonctionnement

Raumfahrtproduktsicherung - Zuverlässigkeit

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

Tables

European Foreword

This document (EN 16602-30:2018) has been prepared by Technical Committee CEN/CLC/JTC 5 “Space”, the secretariat of which is held by DIN (Germany).

This document (EN 16602-30:2018) originates from ECSS-Q-ST-30C 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 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 dependability assurance programme and the dependability requirements for space systems.

Dependability assurance is a continuous and iterative process throughout the project life cycle.

The ECSS dependability policy for space projects is applied by implementing a dependability assurance programme, which comprises:

- identification of all technical risks with respect to functional needs which can lead to non-compliance with dependability requirements,
- application of analysis and design methods to ensure that dependability targets are met,
- optimization of the overall cost and schedule by making sure that:
  - design rules, dependability analyses and risk reducing actions are tailored with respect to an appropriate severity categorisation,
  - risks reducing actions are implemented continuously since the early phase of a project and especially during the design phase.
- inputs to serial production activities.

The dependability requirements for functions implemented in software, and the interaction between hardware and software, are identified in this Standard.

NOTE 1 The requirements for the product assurance of software are defined in ECSS-Q-ST-80.

NOTE 2 The dependability assurance programme supports the project risk management process as described in ECSS-M-ST-80

This Standard applies to all European space projects. The provisions of this document apply to all project phases.

Depending of the product category, the application of this standard needs to be checked and if needed tailored. The pre-tailoring table in clause 8 contains the applicability of the requirements of this document and its annexes according to product type.

This standard may be tailored for the specific characteristics 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 16602-10	ECSS-Q-ST-10	Space product assurance —Product assurance management
EN 16602-10	ECSS-Q-ST-10-04	Space product assurance – Critical-item control
EN 16602-30-02	ECSS-Q-ST-30-02	Space product assurance – Failure modes, effects (and criticality) analysis (FMEA/FMECA)
EN 16602-30-11	ECSS-Q-ST-30-11	Space product assurance – Derating - EEE components

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, in particular for the following terms:

1. availability
2. failure
3. ground segment
4. hazard
5. launch segment
6. maintainability
7. reliability
8. risk
9. severity
10. single point failure
11. space segment
12. space system

3.2 Terms specific to the present standard

3.2.1 criticality

<CONTEXT: function, software, hardware, operation>

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 clause 5.4.

NOTE 2 This notion of criticality, applied to a function, 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 (see 3.2.2).

3.2.2 criticality

<CONTEXT: failure, failure mode>

classification of a failure or failure mode according to a combination of the severity of the consequences and its likelihood or probability of occurrence

NOTE 1 This notion of criticality, applied to a failure or failure mode, considers both the severity and likelihood or probability of occurrence, differently from the criticality of function or a software, hardware or operation, which considers only severity (see 3.2.1).

NOTE 2 The criticality of a failure or failure mode can be represented by a "criticality number" as defined in ECSS-Q-ST-30-02 (see also requirement 6.5a.2).

3.2.3 failure scenario

conditions and sequence of events, leading from the initial root cause, to an end failure

3.2.4 limited-life product

product with useful life duration or operating cycles limitation, prone to wear out, drift or degradation below the minimum required performance in less than the storage and mission time

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
DRD	Document Requirement Definition
DRL	Document Requirement List
EEE	electrical, electronic and electromechanical
FDIR	failure detection isolation and recovery
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FTA	fault tree analysis
HSIA	hardware-software interaction analysis
MTBF	mean time between failure
MTTR	mean time to repair
NRB	nonconformance review board
PA	product assurance
WCA	worst case analysis

3.4 Nomenclature

The following nomenclature applies throughout this document:

a. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.

b. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.

NOTE It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.

c. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.

d. The word “can” is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.

NOTE In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.

e. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

4
Dependability programme

4.1 General

a. The dependability assurance shall be implemented by means of a systematic process for specifying requirements for dependability and demonstrating that these requirements are achieved.

b. The dependability assurance process shall be in conformance with the dependability assurance programme plan for the project.

4.2 Organization

a. The supplier shall coordinate, implement and integrate the dependability programme management with the PA programme management.

4.3 Dependability programme plan

a. The supplier shall develop, maintain and implement a dependability plan for all project phases in conformance with the DRD in Annex C.

NOTE The plan can be included in the PA programme plan.

b. The plan shall address the dependability requirements applicable to the project.

c. The extent that dependability assurance is applied shall take account of the severity (as defined in Table 5-1) of the consequences of failures.

d. The establishment and implementation of the dependability programme plan shall be considered in conjunction with the safety aspects of the programme.

e. The Supplier shall ensure that any potential conflict between dependability and safety requirements are managed.

f. Responsibilities for carrying out all dependability tasks within each phase of the lifecycle shall be defined.

4.4 Dependability risk assessment and control

a. As part of the risk management process implemented on the project, the Dependability engineer shall be responsible for identifying and reporting dependability associated risks.

NOTE ECSS-M-ST-80 describes the risk management process.

b. Dependability risk analysis reduction and control shall include the following steps:

1. identification and classification of undesirable events according to the severity of their consequences;
2. analysis of failure scenarios, determination of related failure modes, failure origins or causes;
3. classification of the criticality of the functions and associated products according to the severity of relevant failure consequences;
4. definition of actions and recommendations for detailed risk assessment, risk elimination, or risk reduction and control to an acceptable level;
5. status of risk reduction and risk acceptance;
6. implementation of risk reduction;
7. verification of risk reduction and assessment of residual risks.

NOTE The process of risk identification and assessment implies both qualitative and quantitative approaches.

c. Risk reduction measures that are proposed for dependability shall be assessed at system level in order to select the optimum solution to reduce the system level risk.

4.5 Dependability critical items

a. Dependability critical items shall be identified by dependability analyses performed to support the risk reduction and control process performed on the project.

NOTE The criteria for identifying dependability critical items to be included in the Critical Items List are given in clause 6.5.

b. Dependability critical items, as part of the Critical Items List, shall be subject to risk assessment and critical items control in conformance with ECSS-Q-ST-10-04.

c. The control measures shall include:

1. a review of all design, manufacturing and test documentation related to critical functions, critical items and procedures;