

STN	Zabezpečovanie výrobkov kozmického programu Spôľahlivosť	STN EN 16602-30 31 0542
------------	---	---

Space product assurance - Dependability

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 10/18

Obsahuje: EN 16602-30:2018

127405

EUROPEAN STANDARD**EN 16602-30****NORME EUROPÉENNE****EUROPÄISCHE NORM**

April 2018

ICS 49.140

English version

Space product assurance - DependabilityAssurance 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

European Foreword	6
1 Scope	7
2 Normative references	8
3 Terms, definitions and abbreviated terms	9
3.1 Terms from other standards.....	9
3.2 Terms specific to the present standard	9
3.3 Abbreviated terms.....	10
3.4 Nomenclature	11
4 Dependability programme	12
4.1 General.....	12
4.2 Organization	12
4.3 Dependability programme plan	12
4.4 Dependability risk assessment and control	13
4.5 Dependability critical items	13
4.6 Design reviews	14
4.7 Dependability Lessons learnt.....	14
4.8 Progress reporting	14
4.9 Documentation	14
5 Dependability engineering	15
5.1 Integration of dependability in the project.....	15
5.2 Dependability requirements in technical specification	15
5.3 Dependability design criteria.....	16
5.3.1 General.....	16
5.3.2 Consequences	16
5.3.3 Failure tolerance	17
5.3.4 Design approach.....	18
5.4 Criticality classification.....	19
5.4.1 Classification of critical functions, hardware and operations.....	19
5.4.2 Assignment of software criticality category	20
5.5 Involvement in testing process.....	21

5.6	Involvement in operational aspects.....	21
5.7	Dependability recommendations.....	22
6	Dependability analyses.....	23
6.1	Identification and classification of undesirable events.....	23
6.2	Assessment of failure scenarios.....	23
6.3	Dependability analyses and the project life cycle.....	23
6.4	Dependability analyses - methods.....	24
6.4.1	General.....	24
6.4.2	Reliability analyses.....	25
6.4.3	Maintainability analyses.....	28
6.4.4	Availability analysis.....	28
6.5	Dependability Critical Items Criteria.....	29
7	Dependability testing, demonstration and data collection.....	30
7.1	Reliability testing and demonstration.....	30
7.2	Availability testing and demonstration.....	30
7.3	Maintainability demonstration.....	30
7.4	Dependability data collection and dependability performance monitoring.....	31
8	Pre-tailoring matrix per product types.....	32
Annex A (informative)	Relationship between dependability activities and project phases.....	41
A.1	Mission analysis / Needs identification phase (phase 0).....	41
A.2	Feasibility phase (phase A).....	41
A.3	Preliminary definition phase (phase B).....	41
A.4	Detailed definition and production/ground qualification testing phases (phase C/D).....	42
A.5	Utilization phase (phase E).....	42
A.6	Disposal phase (phase F).....	43
Annex B (informative)	Dependability documents delivery per review.....	44
Annex C (normative)	Dependability plan - DRD.....	47
C.1	DRD identification.....	47
C.1.1	Requirement identification and source document.....	47
C.1.2	Purpose and objective.....	47
C.2	Expected response.....	47
C.2.1	Scope and content.....	47
C.2.2	Special remarks.....	48

EN 16602-30:2018 (E)

Annex D (normative) Contingency analysis – DRD	49
D.1 DRD identification	49
D.1.1 Requirement identification and source document	49
D.1.2 Purpose and objective	49
D.2 Expected response	49
D.2.1 Scope and content	49
D.2.2 Special remarks	49
Annex E (normative) Reliability prediction – DRD	51
E.1 DRD identification	51
E.1.1 Requirement identification and source document	51
E.1.2 Purpose and objective	51
E.2 Expected response	52
E.2.1 Scope and content	52
E.2.2 Special remarks	52
Annex F (normative) Failure Detection Identification and Recovery Analysis – DRD	53
F.1 DRD identification	53
F.1.1 Requirement identification and source document	53
F.1.2 Purpose and objective	53
F.2 Expected response	53
F.2.1 Scope and content	53
F.2.2 Special remarks	54
Annex G (normative) Zonal analysis – DRD	55
G.1 DRD identification	55
G.1.1 Requirement identification and source document	55
G.1.2 Purpose and objective	55
G.2 Expected response	55
G.2.1 Scope and content	55
G.2.2 Special remarks	55
Annex H (normative) Maintainability analysis – DRD	56
H.1 DRD identification	56
H.1.1 Requirement identification and source document	56
H.1.2 Purpose and objective	56
H.2 Expected response	56
H.2.1 Scope and content	56
H.2.2 Special remarks	57

Annex I (normative) Common-cause analysis – DRD	58
I.1 DRD identification	58
I.1.1 Requirement identification and source document	58
I.1.2 Purpose and objective	58
I.2 Expected response	58
I.2.1 Scope and content	58
I.2.2 Special remarks	58
Annex J (normative) Worst Case Analysis – DRD	59
J.1 DRD identification	59
J.1.1 Requirement identification and source document	59
J.1.2 Purpose and objective	59
J.2 Expected response	59
J.2.1 Scope and content	59
J.2.2 Special remarks	59
Annex K <<deleted>>	61
Annex L (informative) Common-cause check lists	62
Bibliography	65
 Tables	
Table 5-1: Severity categories	17
Table 5-2: Criticality of functions	19
Table 5-3: Criticality category assignment for software products vs. function criticality	20
Table 8-1: Definitions of the columns of Table 8-2	33
Table 8-2: Pre-Tailoring matrix per “Space product types”	34
Table B-1 : Dependability deliverable documents per project review	45
Table L-1 : Common cause check list example for design	62
Table L-2 : Common cause check list example for design (continued)	63
Table L-3 : Common cause check list example for environment	64
Table L-4 : Common cause check list example for unexpected operations	64

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

koniec náhľadu – text ďalej pokračuje v platenej verzii STN