SLOVENSKI STANDARD
SIST EN 62741:2015

01-september-2015

Vodilo za predstavitev zahtev za zagotovljivost - Primer zagotovljivosti

Guide to the demonstration of dependability requirements - The dependability case

Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen - Der Zuverlässigkeitsnachweis

Démonstration des exigences de sûreté de fonctionnement - Argumentaire dans le cadre de la sûreté de fonctionnement

Ta slovenski standard je istoveten z: EN 62741:2015

ICS:

03.120.01	Kakovost na splošno	Quality in general
21.020	Značilnosti in načrtovanje strojev, aparatov, opreme	Characteristics and design of machines, apparatus, equipment

SIST EN 62741:2015 **en**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 62741

March 2015

ICS 21.020; 03.120.01

English Version

Demonstration of dependability requirements - The dependability case (IEC 62741:2015)

Démonstration des exigences de sûreté de fonctionnement - Argumentaire dans le cadre de la sûreté de fonctionnement
(IEC 62741:2015)

Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen - Der Zuverlässigkeitsnachweis
(IEC 62741:2015)

This European Standard was approved by CENELEC on 2015-03-24. 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 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 CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62741:2015 E

Foreword

The text of document 56/1591/FDIS, future edition 1 of IEC 62741, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62741:2015.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-12-24
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2018-03-24

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62741:2015 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-1	NOTE	Harmonized as EN 60300-3-1.
IEC 60300-3-4	NOTE	Harmonized as EN 60300-3-4.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 62347	NOTE	Harmonized as EN 62347.
IEC/ISO 31010	NOTE	Harmonized as EN 31010.
IEC 62198	NOTE	Harmonized as EN 62198.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60050-192	-	International electrotechnical vocabulary - Part 192: Dependability	-	-
IEC 60300-1	-	Dependability management -- Part 1: Guidance for management and application	EN 60300-1	-
ISO 31000	-	Risk management - Principles and guidelines	-	-

IEC 62741

Edition 1.0 2015-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Demonstration of dependability requirements – The dependability case

Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01; 21.020

ISBN 978-2-8322-2247-8

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62741 has been prepared by IEC technical committee 56: Dependability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1591/FDIS	56/1609/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Dependability is the ability to perform as and when required. Acceptable levels of dependability are therefore essential for continued performance and optimized life cycle costs.

In order to achieve dependability of a system, dependability requirements should be established, the risks of not meeting them identified and a suitable set of activities developed to meet and demonstrate the requirements and manage the risks. A dependability case provides a convenient and convincing means of recording the output of these activities in a single location and presenting an argument, supported by evidence, that risks have been treated and that the necessary dependability has been or will be achieved and will continue to be achieved over time. It serves as the main means of communication on dependability among customers, suppliers and other stakeholders and promotes cooperation among them. This is essential for dependability achievement and providing assurance as part of the customer/supplier relationship.

Preparing a dependability case can also improve dependability through the actions taken to prepare and develop the argument within the dependability case. It can improve the cost effectiveness of a dependability programme because if an activity does not provide evidence to support the case, this may indicate that the activity is not necessary.

The activities required for the achievement of dependability depend on the nature and development state of the system and are likely to vary significantly from one project to another.

Throughout this International Standard, the term "dependability" includes all aspects of reliability, availability, maintainability and supportability, as well as other attributes such as usability, testability and durability. In addition, dependability of a system includes all aspects of that system, including components, processes, hardware, software and the interfaces between them.

This standard is intended as guidance: the guidelines are not prescriptive in nature, they are generic, they should be tailored to the specific objectives and are not exhaustive.

This standard does not address safety or the environment.

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

1 Scope

This International Standard gives guidance on the content and application of a dependability case and establishes general principles for the preparation of a dependability case.

This standard is written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement. The methods provided in this standard may be modified and adapted to other situations as needed.

The dependability case is normally produced by the customer and supplier but can also be used and updated by other organizations. For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly where they use the system for a different purpose.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* [1]

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in IEC 60050-192, as well as the following, apply.

3.1 Terms and definitions

3.1.1
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

3.1.2
evidence framework
structure identifying what evidence will be/has been produced and when

[1] To be published.

3.1.3
off-the-shelf
OTS
non-developmental item of supply that is both commercial and sold in substantial quantities in the commercial marketplace

Note 1 to entry: Sometimes referred to as COTS (commercial off-the-shelf) or MOTS (modified off-the-shelf).

3.1.4
customer
party which orders or specifies the item, including the dependability requirements

Note 1 to entry: This could be an organization, sponsor, department, company or an individual and can change through the life cycle.

3.1.5
subsystem
part of a system, which is itself a system

3.1.6
supplier
party which supplies the item, which meets its dependability requirement

Note 1 to entry: This could be an organization, department, company or an individual and can change through the life cycle.

3.1.7
system <in dependability>
defined set of items that collectively fulfil a requirement

Note 1 to entry: A system is considered to have a defined real or abstract boundary.

Note 2 to entry: External resources (from outside the system boundary) may be required for the system to operate.

Note 3 to entry: A system structure may be hierarchical, e.g. system, subsystem, component, etc.

Note 4 to entry: Conditions of use and maintenance should be expressed or implied within the requirement.

3.2 Abbreviations

COTS	Commercial off-the-shelf
FEM	Finite element modelling
FMECA	Failure mode, effects and criticality analysis
FTA	Fault tree analysis
MOTS	Modified off-the-shelf
OTS	Off-the-shelf

4 Background to the dependability case

4.1 Principles and purpose

A dependability case provides a reasoned and traceable argument based on evidence that a system satisfies the requirements and will continue to do so over time. It demonstrates why certain activities have been undertaken and how they can be judged to be successful. For maximum effectiveness it should be initiated at the concept stage, revised progressively during a system life cycle and is typically summarized in dependability case reports at predefined milestones. It records progress in obtaining evidence that dependability requirements are met and remains with the system throughout its life cycle until retirement.

The dependability case is of the greatest benefit for high value, low quantity systems where direct evidence of dependability may be difficult or expensive to obtain. Since these systems are often highly complex, involve novel technologies and have wide-ranging stakeholders, an explicit argument is necessary in order to demonstrate their detailed dependability claims with suitable evidence.

4.2 Relationship between the dependability case and dependability plans

Effective management of dependability requires organizational arrangements to implement policy, activities implemented in dependability programmes and plans and processes for performance evaluation, assurance and review.

A dependability programme involves

a) dependability plans, that define the activities, techniques and resources required to achieve dependability,

b) methods for measurement and assessment,

c) assurance and review.

The objectives of a dependability plan include ensuring that

1) the dependability requirements of the customer are determined and demonstrated to be understood by both the customer and supplier,

2) activities are planned, agreed and implemented to satisfy and demonstrate the requirements and treat the risks of failure,

3) the customer is provided with assurance that the dependability requirements are being, or will be, satisfied and that uncertainty in the dependability decreases over the course of the plan.

The dependability case provides progressive assurance that dependability requirements are being or will be satisfied and that uncertainty in the dependability is decreasing. In addition, the case demonstrates that the activities in the plan achieve the requirements and treat the risks. This forms part of the argument and evidence for why the system is, or will be, dependable. The plan is usually based on standards and the organization’s experience in managing dependability and is tailored, taking into account factors such as the relevant life cycle stages, the organization’s context, resources available and the risks that need to be managed.

The dependability plan and dependability case are often developed concurrently as both include consideration of the risks of not meeting the requirements. However, the system might meet the dependability requirements but it might not be possible to demonstrate that these requirements have been met. This might be because there is no appropriate activity which can demonstrate that the requirements have been met, or the cost or time required to do so might be excessive. Therefore the dependability plan may also include activities specifically intended to treat the risks of not being able to demonstrate that the requirements have been met and these activities also provide evidence in the dependability case.

A register of risks produced as part of a dependability case should be coordinated with the risks identified as part of planning the dependability programme and with the project risk register. Activities proposed to treat the risks are included in the dependability plan and examined as sources of evidence that risks have been treated. As the dependability plan is implemented, the dependability case is populated with evidence of the successful implementation of the plan. This provides progressive assurance that requirements are being met. If sufficient evidence is not able to be obtained, then the dependability plan should be modified accordingly.

In a well managed project, the dependability plan and dependability case are fully integrated with overall project management. In such a project, the use of the dependability case does not incur an increase in overall workload, since the cost of constructing the case is recouped by