
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**

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.



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

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document have to be withdrawn

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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	-	-

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

FOREWORD	4
INTRODUCTION	6
1 Scope	7
2 Normative references	7
3 Terms, definitions and abbreviations	7
3.1 Terms and definitions	7
3.2 Abbreviations	8
4 Background to the dependability case	8
4.1 Principles and purpose	8
4.2 Relationship between the dependability case and dependability plans	9
4.3 Progressive assurance of dependability	10
5 Principles of the dependability case	11
5.1 Description of the dependability case	11
5.2 Making claims in the dependability case	12
5.3 Using evidence in the dependability case	13
5.4 Evidence framework	14
5.5 Dependability case report	16
6 Development of the dependability case	16
6.1 General	16
6.2 Preparation of the dependability case	17
6.3 Concept stage	18
6.4 Development stage	19
6.5 Realization stage	19
6.6 Utilization stage	20
6.7 Enhancement stage	20
6.8 Retirement stage	20
7 Assessing the adequacy of evidence	21
Annex A (informative) Evidence framework	22
A.1 General	22
A.2 Abbreviations used only in this annex	23
Annex B (informative) General requirements for the dependability case report	40
B.1 General	40
B.2 Elements required for the dependability case report	40
B.3 Context and assumptions	40
B.3.1 Stakeholders	40
B.3.2 System description	41
B.3.3 Dependability requirements	41
B.3.4 Limitations on use	41
B.3.5 Assumptions	41
B.4 Risks	41
B.5 Dependability plan	42
B.6 The evidence framework	42
B.7 Body of evidence	42
B.8 Review of evidence to date	42
B.9 Dependability claims and argument	42

B.10 Conclusions and recommendations	42
Annex C (informative) Checklist of points for assessing the adequacy of evidence	44
Bibliography	45
Figure 1 – Illustration of progressive assurance process	11
Figure 2 – The development of claims	12
Figure 3 – Establishment and development of the evidence framework	15
Table A.1 – Evidence framework for system “X”	24
Table A.2 – Evidence framework for system Y	28

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.