SLOVENSKI STANDARD
SIST EN 60300-3-15:2010

01-februar-2010

Upravljanje zagotovljivosti - 3-15. del: Napotki za tehnično načrtovanje sistema zagotovljivosti (IEC 60300-3-15:2009)

Dependability management - Part 3-15: Guidance to engineering of system dependability (IEC 60300-3-15:2009)

Zuverlässigkeitsmanagement - Teil 3-15: Anwendungsleitfaden - Technische Realisierung der Systemzuverlässigkeit (IEC 60300-3-15:2009)

Gestion de la sûreté de fonctionnement - Partie 3-15: Guide d'application - Ingénierie de la sûreté de fonctionnement des systèmes (CEI 60300-3-15:2009)

Ta slovenski standard je istoveten z: **EN 60300-3-15:2009**

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 60300-3-15:2010 **en,fr**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60300-3-15

December 2009

ICS 03.120.01

English version

Dependability management - Part 3-15: Application guide - Engineering of system dependability

(IEC 60300-3-15:2009)

Gestion de la sûreté de fonctionnement - Partie 3-15: Guide d'application - Ingénierie de la sûreté de fonctionnement des systèmes
(CEI 60300-3-15:2009)

Zuverlässigkeitsmanagement - Teil 3-15: Anwendungsleitfaden - Technische Realisierung der Systemzuverlässigkeit
(IEC 60300-3-15:2009)

This European Standard was approved by CENELEC on 2009-10-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

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

CENELEC

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 60300-3-15:2009 E

Foreword

The text of document 56/1315/FDIS, future edition 1 of IEC 60300-3-15, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 60300-3-15 on 2009-10-01

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2010-07-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2012-10-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 60300-3-15:2009 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:

[1] IEC 61069-1	NOTE	Harmonized as EN 61069-1:1993 (not modified).
[2] IEC 62347	NOTE	Harmonized as EN 62347:2007 (not modified).
[7] IEC 60300-3-1	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
[9] IEC 61508	NOTE	Harmonized in EN 61508 series (not modified).
[10] IEC 61508-1	NOTE	Harmonized as EN 61508-1:2001 (not modified).
[12] IEC 61014	NOTE	Harmonized as EN 61014:2003 (not modified).
[13] IEC 61164	NOTE	Harmonized as EN 61164:2004 (not modified).
[14] ISO 10007	NOTE	Harmonized as EN ISO 10007:1996 (not modified).
[16] IEC 60300-3-11	NOTE	Harmonized as EN 60300-3-11:2009 (not modified).
[17] IEC 60300-3-12	NOTE	Harmonized as EN 60300-3-12:2004 (not modified).
[22] IEC 60721	NOTE	Harmonized in EN 60721 series (not modified).
IEC 60300-3-4	NOTE	Harmonized as EN 60300-3-4:2008 (not modified).
IEC 60812	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61025	NOTE	Harmonized as EN 61025:2007 (not modified).
IEC 61078	NOTE	Harmonized as EN 61078:2006 (not modified).
IEC 61508-7	NOTE	Harmonized as EN 61508-7:2001 (not modified).
IEC 61709	NOTE	Harmonized as EN 61709:1998 (not modified).
IEC 62308	NOTE	Harmonized as EN 62308:2006 (not modified).
ISO 13407	NOTE	Harmonized as EN ISO 13407:1999 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

Publication	Year	Title	EN/HD	Year
IEC 60300-1	-[1)]	Dependability management - Part 1: Dependability management systems	EN 60300-1	2003[2)]
IEC 60300-2	-[1)]	Dependability management - Part 2: Guidelines for dependability management	EN 60300-2	2004[2)]

[1)] Undated reference.

[2)] Valid edition at date of issue.

IEC 60300-3-15

Edition 1.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Dependability management –
Part 3-15: Application guide – Engineering of system dependability**

**Gestion de la sûreté de fonctionnement –
Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 03.120.01

ISBN 2-8318-1048-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

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 should be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability should 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 should not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-15 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1315/FDIS	56/1321/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.

A list of all parts of the IEC 60300 series, under the general title *Dependability management*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site 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

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

– process,

– achievement,

– assessment, and

– measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

2 Normative references

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

IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
system
set of interrelated items considered as a whole for a defined purpose, separated from other items

NOTE 1 A system is generally defined with the view of performing a definite function.

NOTE 2 The system is considered to be bound by an imaginary surface that intersects the links between the system and the environment and the other external systems.

NOTE 3 External resources (i.e. outside the system boundary) may be required for the system to operate.

NOTE 4 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

3.2
subsystem
system that is part of a more complex system

3.3
operating profile
complete set of tasks to achieve a specific system objective

NOTE 1 Configurations and operating scenarios form part of the mode of system operation.

NOTE 2 An operating profile is the sequence of required tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation.

3.4
function
elementary operation performed by the system which, when combined with other elementary operations (system functions), enables the system to perform a task

[IEC 61069-1 :1991, 2.2.5] [1][1]

3.5
element
combination of components that form the basic building block to perform a distinct function

NOTE 1 An element may comprise hardware, software, information and/or human components.

NOTE 2 For some systems, information and data are an important part of the system operations.

3.6
integrity
ability of a system to sustain its form, stability and robustness, and maintain its consistency in performance and use

4 System dependability engineering and applications

4.1 Overview of system dependability engineering

Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use. Dependability characteristics include availability and its inherent or external influencing factors, such as: reliability, fault tolerance, recoverability, integrity, security, maintainability, durability and maintenance support. The dependability of a system infers that the system is trustworthy and capable of performing the desirable service upon demand to satisfy user needs. The system objective, structure, properties, and influencing conditions affecting system dependability performance are described in IEC 62347 [2] which provides guidance for determination of relevant system functions for specifying system dependability.

There are four main aspects for engineering dependability into systems:

a) **dependability process** – establishes the technical processes for engineering dependability into systems. The process consists of a sequence of activities implemented at each respective life cycle stage to achieve specific dependability objectives in system performance. The dependability process shall be fully integrated into the design and management processes;

b) **dependability achievement** – implementation of the effective engineering effort and knowledge experience applied at appropriate system life cycle stages. The aim is for progressive accomplishment of dependability objectives of the constituent system functions suitable for subsystem realization and system integration (reliability growth);

c) **dependability assessment** – evaluates the dependability attributes and determines their effectiveness when implemented into systems. The process identifies the specific dependability attributes to meet project needs and provides the methodology and rationale on how these attributes can be determined;

d) **dependability measurement** – quantifies the dependability attributes for contracting, specification and assessment purposes. The process is to assign a quantitative value or number to designate a target entity representing a specific dependability characteristic.

---

1 Figures in square brackets refer to the bibliography.

The aim is to express a statement of intent in quantifiable terms to facilitate mutual understanding of the issue involved and to serve as basis for negotiation in reaching agreements.

4.2 System dependability attributes and performance characteristics

System dependability attributes are those specific dependability related features and time-dependent performance characteristics inherent in the system by design and construction. Some features, such as system performance characteristics can be quantified and measured. Other dependability features which are not quantifiable may present certain value or useful information pertinent to those attributes. These non-quantifiable features can be described in qualitative terms to establish its value for subjective dependability assessment. Both quantifiable and non-quantifiable features are important to describe the system dependability attributes. Examples of non-quantifiable features include product brand value, user friendly operation, and informative instructions. Examples of quantifiable performance characteristics include uptime duration, downtime frequency, mean-time-between-failures, and time for restoration from a degraded state back to normal system performance.

The main attributes of system dependability are as follows:

a) **availability**: the ability of the system to be in a state to perform a required function when a demand is placed upon the system. Availability performance is characterized in terms of measures such as percentage uptime for the duration of system performance operation upon demand; outage frequency and downtime duration;

b) **reliability**: the ability of the system to perform a required function for a given period of time under given conditions of use. Reliability performance is characterized in terms of measurements such as mean-time-between-failures and failure-free duration;

c) **maintainability**: the ability of the system to be restored to a state in which it can provide a required function following a failure, or retained in such an up-state, under given conditions of use and maintenance. Maintainability performance is characterized in terms of measurements such as mean-time-to-restore and recovery time;

d) **maintenance support**: ability of an organization to provide, when required, the resources required to maintain a system, under given conditions. Maintenance support performance is characterized in terms of measures such as utilization of maintenance resources, training needs, enabling tools and facilities, logistics delay time and turn-around time for spares provisioning.

There are other attributes related to dependability for specific system applications. They include but are not limited to:

e) **recoverability**: ability of a system to be restored to a state in which it can perform a required function following a failure without repair of hardware or software. It is characterized in terms of measurements such as mean-time-to-recover;

f) **testability**: ability of a system to be tested at designated maintenance levels for replace/repair action to determine fault coverage. It is characterized in terms of measurements such as percentage of test coverage;

g) **service accessibility**: ability of a service to be obtained within specified tolerances and other given conditions when requested by the user. It is characterized in terms of measurements such as probability of access to a service;

h) **service retainability**: ability of a service, once obtained, to continue to be provided under given conditions for a requested duration. It is characterized in terms of measurements such as probability of retention in time duration.

Recoverable performance is dependent on the design of system architecture, fault-tolerant and self-healing features incorporated into the system. Service performance is dependent on the properties of the system facilities, construction and infrastructure of resource deployment. The attributes of system performance in general are inherent in the system design. The performance attributes are derived from the capability of the system and the dependability feature of the system.