SLOVENSKI STANDARD
SIST EN 62347:2008

01-januar-2008

Napotki za specifikacije sistemske zagotovljivosti (IEC 62347:2006)

Guidance on system dependability specifications

Anleitung zur Spezifikation der Zuverlässigkeit von Systemen

Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes

Ta slovenski standard je istoveten z: **EN 62347:2007**

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 62347:2008 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62347

March 2007

ICS 03.120.01

English version

Guidance on system dependability specifications
(IEC 62347:2006)

Lignes directrices
pour les spécifications de sûreté
de fonctionnement des systèmes
(CEI 62347:2006)

Anleitung zur Spezifikation
der Zuverlässigkeit von Systemen
(IEC 62347:2006)

This European Standard was approved by CENELEC on 2007-03-01. 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: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 62347:2007 E

Foreword

The text of document 56/1138/FDIS, future edition 1 of IEC 62347, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62347 on 2007-03-01.

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)	2007-12-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2010-03-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 62347:2006 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 60300-1	NOTE	Harmonized as EN 60300-1:2003 (not modified).
IEC 60300-2	NOTE	Harmonized as EN 60300-2:2004 (not modified).
IEC 61069	NOTE	Harmonized in EN 61069 series (not modified).
IEC 61069-1	NOTE	Harmonized as EN 61069-1:1993 (not modified).
ISO 9000	NOTE	Harmonized as EN ISO 9000:2005 (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 60050-191	-[1)]	International Electrotechnical Vocabulary (IEV) - Chapter 191: Dependability and quality of service	-	-
ISO/IEC 15288	-[1)]	Systems engineering - System life cycle processes	-	-

[1)] Undated reference.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62347

Première édition
First edition
2006-11

Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes

Guidance on system dependability specifications

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE V

Pour prix, voir catalogue en vigueur
For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDANCE ON SYSTEM DEPENDABILITY SPECIFICATIONS

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 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 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 62347 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1138/FDIS	56/1161/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 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

A system is a physical and/or virtual entity. It is necessary sometimes to define a system's boundary so that it can be distinguished or separated from other systems. A system interacts with its surroundings or environment to fulfil a specific need or purpose, or to achieve a defined objective. This is accomplished through the interaction of the system's elements representing the necessary functions designed to meet the intended objective. Determining the functions needed to meet a specific objective represents the process of developing a system specification. Detailed system design begins only after the functions have been identified.

Systems may vary in their complexity structurally and functionally. A system can consist of hardware, software, and human elements, or a combination of any of these elements to perform the necessary functions. A system consisting of a single function can be a product, such as a television set or a software program for lighting controls. A system performing multiple functions can be a home theatre system or an aircraft. Individual systems with defined boundaries can be joined together to form a complex set of interacting systems such as a power distribution network or an internet protocol service.

System specification establishes the envelope and boundary for the system. System structure is often hierarchical linking subsystems and interacting systems. System specification is applicable to all systems under the generic definition of system irrespective of its hierarchy. It does not replace or substitute for use a product specification, which provides specific details of the product requirements.

The dependability of a system infers that the system is perceived to be trustworthy and has the ability to provide service upon demand as desirable performance attributes. Such performance attributes can be achieved through the incorporation of dependability into the functions. Dependability implies the awareness of user confidence acquired through prior experience of the system with reliable performance results in meeting user expectations.

This International Standard provides the rationale on the importance of dependability in system specification by functions. It presents a procedure for determining system dependability requirements. For generic system operation, the process of determining the functions needed to meet system dependability objective is described. For specific system operation, the concept of an operating profile is introduced to establish the requirements of functions in an environment relevant to the specific system operation. This International Standard is based on the system model and categorization of functions established in the IEC 61069 series. Relevant technical processes for the definition and analysis of system requirements are adopted from ISO/IEC 15288. The procedural steps and processes for determining system dependability requirements are presented with applicable examples. IEC 60300-1 and IEC 60300-2 are used to guide dependability management. This International Standard extends the dependability specification process to address functions as a prerequisite for system design. It complements IEC 60300-3-4 in specification of dependability requirements for products and equipment. The technical process for engineering dependability into systems is described in IEC 60300-3-15.

GUIDANCE ON SYSTEM DEPENDABILITY SPECIFICATIONS

1 Scope

This International Standard gives guidance on the preparation of system dependability specifications. It provides a process for system evaluation and presents a procedure for determining system dependability requirements.

This International Standard is not intended for certification or to perform conformity assessment for contractual purposes. It is not intended to change any rights or obligations provided by applicable statutory or regulatory requirements.

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 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

ISO/IEC 15288, *Systems engineering – System life cycle processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050(191) and the following apply.

3.1
system
set of interrelated or interacting elements

[ISO 9000:2005, 3.2.1]

NOTE 1 In the context of dependability, a system will have:

- a defined purpose expressed in terms of intended functions;
- stated conditions of operation/use; and
- defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

[IEC 60300-1, 3.6]

NOTE 3 For some systems, such as Information Technology products, data is an important part of the system elements.

3.2
operating profile
complete set of tasks to achieve a specific system objective

NOTE An operating profile is the sequence of 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.

3.3
function
elementary operation performed by the system which, combined with other elementary operations (system functions), enables the system to perform a task

[IEC 61069-1, definition 2.2.5]

NOTE For some systems, information and data are important parts of the system elements.

3.4
element
combination of components that form the basic building block to perform a distinct function

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

3.5
influencing condition
condition set forth by external influencing elements and/or other factors that interact with and affect system performance

NOTE Influencing conditions may also include regulations and constraints.

4 Concepts dealing with system dependability

4.1 Understanding the system

4.1.1 Purpose and objective

A system is designed for a purpose. A system must have a defined objective to achieve its purpose. The purpose of a home theatre system is to provide cinema-like entertainment in a home environment. The objectives may include users' perception of a clear picture vision and superb sound quality, reliability and safety in operation, and ease of installation and upgrade. A system may have a specific objective to perform a dedicated task, such as an aircraft carrying cargo to reach a delivery target. The objectives of a system may include the completion of a sequence of tasks, such as delivering different payloads to different destinations. Defining the system to meet its generic or specific objectives is an important prerequisite of specifying the system requirements.

A system with multiple functions and complex operating scenario often involves external interacting systems to achieve its objectives. A system may also evolve with time, resulting from enhancements of its performance capability, to sustain service demands in operation and for market competition.

4.1.2 System properties and characteristics

A system has a set of properties specifically assigned, selected or designed into the system to meet its intended objectives. Specific system properties are used to develop the needed functions to perform the tasks. These properties represent the special features or attributes inherent in the system. They may be categorized in major groupings as defined in IEC 61069 series. Under each group is a set of characteristics relevant to and dominant in that group. The functions are derived from those system properties by means of interacting elements within the system. The interacting elements are designed to provide specific characteristics capable of delivering the system functions and to carry out the tasks once these functions can be realized. System characteristics may be qualitative or quantitative. Figure 1 shows an example of the system characteristics grouped under various system properties.