

Guidance on system dependability specifications

The European Standard EN 62347:2007 has the status of a
British Standard

ICS 03.120.01

National foreword

This British Standard is the UK implementation of EN 62347:2007. It is identical to IEC 62347:2006.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 September 2007

© BSI 2007

ISBN 978 0 580 54164 3

Amendments issued since publication

Amd. No.	Date	Comments

**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

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.

CONTENTS

INTRODUCTION.....	4
1 Scope.....	5
2 Normative references	5
3 Terms and definitions	5
4 Concepts dealing with system dependability.....	6
4.1 Understanding the system	6
4.2 System life cycle	8
4.3 System operation	10
4.4 System operating profile.....	10
4.5 Dependability requirements	11
5 Procedure for specifying system dependability	13
5.1 System specification process	13
5.2 System dependability specification process.....	13
5.3 Determining dependability values	14
5.4 Procedural steps for determining system dependability requirements	15
Annex A (informative) Evaluation of dependability characteristics	19
Annex B (informative) An example on developing a system dependability specification – A home security system	26
Annex ZA (normative) Normative references to international publications with their corresponding European publications.....	35
Bibliography.....	34
Figure 1 – An example of system properties and related characteristics.....	7
Figure 2 – Overview of system life cycle stages	9
Figure 3 – Relationships of system operating profile and scenario in system operation	11
Figure 4 – Overview of system specification process	14
Figure 5 – Steps for determining system dependability requirements	16
Figure B.1 – System configuration for normal mode of operation.....	30
Figure B.2 – System configuration for panic mode of operation.....	31
Figure B.3 – System configuration for security service mode of operation	31
Table A.1 – Examples of influencing factors under each influencing condition.....	24
Table A.2 – Relationship of system properties with influencing conditions.....	25

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

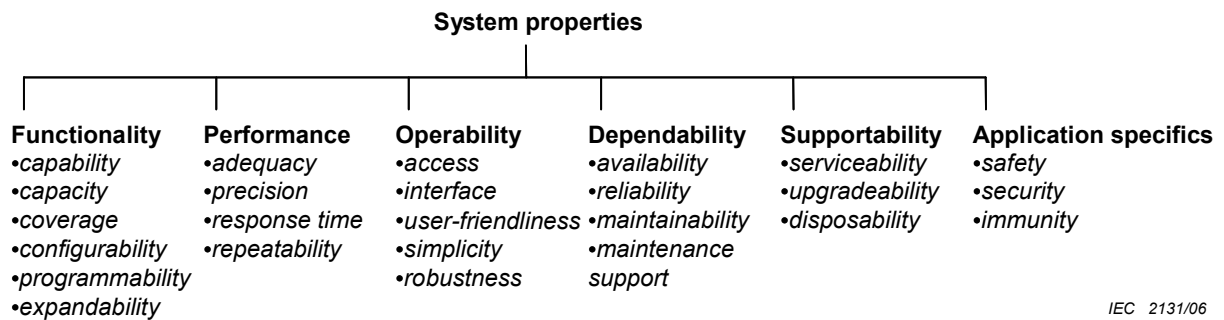
4.1.1 Purpose and objective

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.



- NOTES**
- Functionality:** the extent to which the processing, monitoring and control functions are provided.
- Performance:** the extent to which the provided functions can be executed under defined operational and environmental conditions.
- Operability:** the extent to which information can be effectively communicated via the human interfaces and established protocols.
- Dependability:** the extent to which the system can be relied upon to perform its intended functions under defined operational and environmental conditions at a given instant of time or over a given time interval.
- Supportability:** the extent to which the system can be supported and maintained for continual operation.
- Application specifics:** the extent to which the system can be designed for risk avoidance and risk containment, such as security operational measures.

Figure 1 – Example of system properties and related characteristics

4.1.3 Influencing conditions

In order to determine which functions have the selected characteristics appropriate to achieving a specific objective, it is necessary to define the conditions that the system is capable of withstanding or meeting the demands and duration of the assigned tasks. The following areas of influence or domains affecting the system should be considered:

- task requirements imposed on the system;
- human interface with the system;
- process involved with system operation;
- environment to which the system is exposed;
- support services available for the system;
- utilities needed to operate the system;
- external interacting systems;
- constraints and regulations.

A system dependability specification cannot be completed in isolation. It requires the input of detailed information at the system planning stage to determine how the system is intended to perform for the entire duration of its defined life. This effort is essential to permit identification and selection of dependability and other relevant characteristics, and justification for design trade-off and system optimization.

4.1.4 Influencing factors

Each influencing condition can be affected by various factors influencing the status of its condition. For example, the task requirements imposed on the system could be influenced by factors associated with the nature and duration of the task; the system environment could be influenced by the temperature and humidity of the system ambience. Influencing factors are not equal to the extent of their influence. Some factors are more prominent or dominant in the extent of their influence while others may have less influence or be negligible.

Annex A provides typical examples of influencing factors on system functions to serve as criteria for evaluation of system dependability characteristics.

4.1.5 Relationships of system properties with influencing conditions

Establishing the relationships of system properties with influencing conditions can help identify the relevance and criticality of a specific external condition influencing the design of a function. The identification process will lead to the selection of specific properties and associated characteristics that are needed for the function. The selected characteristics are not exclusive to a specific function. The same characteristics may be needed in the design of other functions. The importance of these characteristics is determined by an iterative process for evaluation and design trade-off. The results derived from this evaluation can help determine the system configuration and establish the appropriate system boundaries in meeting the intended objective. The relevant information and data captured in this evaluation process will form the basis for specifying the important characteristics in the design of system functions.

The relationships of system properties with influencing conditions can be used as guidance for evaluation of system functions. The identification of functions is presented in Annex A to facilitate determination of relevant dependability characteristics.

4.1.6 Realization of system functions

A system can consist of any combination of hardware, software, and human elements. System functions can be realized by means of using hardware and/or software in their construction. Some functions may involve human intervention to achieve their assigned tasks. For new system development, system functions can be realized through engineering design and production as described in IEC 60300-3-15 (under consideration). Sometimes it may be more economical or expedient to modify an existing design or to utilize a commercial-off-the-shelf (COTS) product to serve as the needed function. Evolving systems often require additional functions for performance capability enhancement and removal of obsolete functions. In such a case, the engineering effort would have to deal with legacy issues as described in Annex A.

4.2 System life cycle

A system, irrespective of its size and complexity, follows a life cycle progression from its initial conception through to its eventual retirement. A system life cycle is generally represented by a sequence of discrete stages. Each system life cycle stage can be further represented by sub-stages to facilitate planning, operation and support. A typical system life cycle can consist of the following identifiable stages as shown in Figure 2.

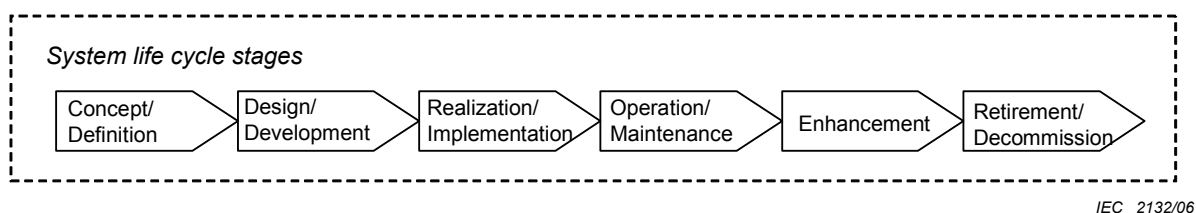


Figure 2 – Overview of system life cycle stages

The objective of each life cycle stage is presented as follows:

- *Concept/definition*: to identify system requirements and develop system specifications.
- *Design/development*: to conduct preliminary design and develop viable system functions to meet performance objectives.
- *Realization/implementation*: to produce, out-source or acquire the system elements in hardware and software forms for assembly of subsystems suitable for human interactions as needed in system operation.
- *Operation/maintenance*: to engage the system for provision of operational service and to sustain the prescribed level of system performance capability.
- *Enhancement*: to improve the system performance with additional features.
- *Retirement/decommission*: to end the existence of the system entity.

The description of system life cycle stages in Figure 2 is viewed from a generic systems engineering perspective. There are other system life cycle descriptions. IEC 60300-2 describes the product life cycle phases from a project management view. ISO/IEC 15288 provides a similar system life cycle description from a software engineering view. Whereas there are some differences in the use of terms presented in these standards, their alignments are noticeable at the transition points of their respective system life cycle stages or project phases.

Each stage has its own specific objectives to be met by the system design process, such as limited access to maintenance during system operation, recyclable parts for ease of disposal. Each stage also requires different internal procedures and work instructions, as well as requiring different contractual conditions to be met. Defining system requirements and developing system solutions during concept/definition and design/development stages can affect subsequent stages in system operation/maintenance. Decisions made for system architecture and technology selection in system design can have an effect on production, system integration and enhancement efforts, and constraining the disposal process.

The time duration of a system life cycle is affected by various factors depending on the system type and application, the technology used, and the support provision. For example, the life cycle of a motor vehicle may last from 7 to 15 years due to mechanical wear and chassis deterioration, whereas a personal computer may have a life-span of less than 5 years due to technology obsolescence. The time duration for application is the useful life of the system.

4.3 System operation

The primary objective of a system design and application is aimed at achieving its intended performance during system operation. The operation stage of the system life cycle represents the useful life or service life of the system. During operation the system is monitored, maintained, and supported as needed to sustain operational objectives.

For most system operations, they follow a generic operating pattern of average usage reflecting the actual application. The functions during operation are needed to carry out the intended system performance all the time or to be available upon demand to meet performance requirements. In some cases, there is a warranty period representing a sub-stage during initial operation of the system. During guarantee and warranty periods, the system maintenance and support effort may be more intensive for business or contractual reasons than those normally applied after warranty for the remaining useful life of the system operation. Most commercially available systems, such as a motor vehicle or a home entertainment system, fit into this generic pattern for operation and maintenance.

However, there are systems designated for serving a dedicated operational objective where a specific operating profile will need to be established.

Degradation in system performance should be presented by a separate operation stage. Under normal system operation, degraded performance of system without affecting critical operation is tolerated up to a predetermined limit. For example, a few isolated outage incidents of subscriber lines of a telecommunications switching system due to infrequent lightning strikes in bad weather conditions is normally considered acceptable. The general public customers would tolerate such rare events subject to expedient restoration to full service within reasonable time. However, the occurrence of outages in such rare events still represents a degraded performance scenario. Degradation will have an effect on the quality of service provided by the system.

Emergency situations and responses should be treated as separate stages.

4.4 System operating profile

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. For example, the objective of a commercial aircraft flying from point A to point B is to deliver passenger service; an operating profile can be stated for the aircraft to perform the tasks of take-off, flight, and landing during its specific operation. Associated with each specific task, there are specific activities and conditions set forth for the aircraft to perform. Criteria are established at the completion or start of each task to determine its success before continuation or to abort further operation.

The tasks in an operating profile can only be achieved through the implementation of various functions designed into the system. From a system's operational perspective, some of the functions are critical that may demand incorporation of specific dependability requirements to achieve the designated tasks. Other functions may be non-critical; they may not be needed for those designated tasks. For example, the aircraft engines are critical functions to carry out the tasks of take-off, flight, and landing. However, the landing gears are only used during take-off and landing. The landing gear function is not needed during flight. An analysis of the system operating profile may help determine the application needs and duty cycles of specific functions during operation. Figure 3 shows the relationships of operating profile and operating scenario in system operation to the system life cycle stages.