

Dependability management —

Part 3: Application guide —

Section 6: Software aspects of dependability

ICS 29.020

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

National foreword

This British Standard reproduces verbatim IEC 60300-3-6:1997 and implements it as the UK national standard.

The UK participation in its preparation was entrusted by Technical Committee DS/1, Dependability and tetrotechnology, to Subcommittee DS/1/1, Dependability, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the CEI IEC title page, page ii, pages 1 to 18 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

This British Standard, having been prepared under the direction of the Management Systems Sector Board, was published under the authority of the Standards Board and comes into effect on 15 January 1998

© BSI 05-1999

ISBN 0 580 29414 5

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	ii
Introduction	1
1 Scope	2
2 Normative references	2
3 Definitions	2
4 Software aspects	2
5 Software life cycle phases and processes	3
6 Application of dependability programmes to products containing software	3
7 Tailoring of dependability programmes	10
Annex A (informative) Typical relationship of product life cycle phases and software life cycle phases	12
Annex B (informative) Selection of dependability programme elements	13
Annex C (informative) Software life cycle processes	14
Annex D (informative) Association of the software life cycle processes with the product life cycle phases	16
Annex E (informative) Cross-references between IEC 60300-2 and ISO 9000-3	17
Annex F (informative) Bibliography	18

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60300-3-6

Première édition
First edition
1997-11

Gestion de la sûreté de fonctionnement –

Partie 3:

Guide d'application –

**Section 6: Aspects logiciels de la sûreté
de fonctionnement**

Dependability management –

Part 3:

Application guide –

Section 6: Software aspects of dependability



Numéro de référence
Reference number
CEI/IEC 60300-3-6: 1997

Foreword

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-6 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/583/FDIS	56/600/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.

Annex A, Annex B, Annex C, Annex D, Annex E and Annex F are for information only.

Introduction

Dependability is the collective term describing the availability performance of a system or product. The availability performance is influenced by the reliability, maintainability and maintenance support performance factors. In many systems and products, reliability, maintainability, and availability rank amongst the dominant performance characteristics of importance to the users seeking cost-effective operation. Reliability and maintainability are performance characteristics inherent to the product design. Maintenance support is external to the product itself, and will affect the quality of service. Maintenance support performance reflects the ability of the maintenance organization to provide the necessary resources to sustain a level of maintenance support effort to achieve availability performance objectives.

A dependability programme must be tailored to the product for effective application. The dependability programme should form part of the overall project management programme for proper coordination with product development, manufacture, verification and deployment. Dependability programme elements and tasks should be consistent with the other support programmes such as quality management, configuration management, data collection etc.

The dependability management process includes project planning, specification, design analysis, verification and validation, implementation, evaluation, and data feedback of the product or service. Modern systems and products often contain software as a functional entity to achieve operational performance objectives. The software contained in the system or embedded in the product is subject to the dependability management process. This application guide addresses the software aspects of dependability. It provides specific guidance on the selection and application of relevant activities in dependability programmes associated with products containing software, or systems configured by software with hardware elements.

The availability performance of a product can be affected by hardware failures, software faults, or human errors. Product malfunction causing downtimes can be traceable to its internal design anomalies, or due to external interference including procedural errors. Product failures can arise from internal design faults relating to hardware or software problems. Failed hardware and worn-out parts can be identified and isolated, repaired or replaced to maintain the same level of product reliability. Unlike most physical hardware, software, once created in the form of codes or instructions, will not wear-out or deteriorate. Hence, some of the software processes may be different from those applicable for the hardware implementation. The intent of this application guide is to relate the software life cycle processes with the product life cycle phases within the dependability management framework.

Dependability management is defined in IEC 60300-1. Dependability programme elements and tasks are specified in IEC 60300-2. This application guide complements IEC 60300-2 in terms of dependability programme implementation of systems or products containing software. Emphasis is placed on the time-phase application of relevant software activities associated with the implementation of IEC 60300-2 as shown in Annex A. Annex B presents the selection of dependability programme elements associated with the software life cycle phases.

Efforts have been made to harmonize this application guide with ISO/IEC 12207 on software life cycle processes. An overview of the software life cycle processes is provided in Annex C. Cross-references are identified in Annex D to facilitate association of software life cycle processes with relevant dependability elements and product life cycle phases.

The relationship of dependability (IEC 60300 series of standards) and quality (ISO 9000 series of standards) is addressed in IEC 60300-1/ISO 9000-4 and will not be elaborated in this application guide. However, the guidelines contained in ISO 9000-3 for application of ISO 9001 to software should be noted in terms of quality factors influencing the dependability characteristics of software elements. Cross-references between IEC 60300-2 and ISO 9000-3 are shown in Annex E.

A bibliography is provided in Annex F for additional references to software aspects of dependability.

1 Scope

This application guide complements IEC 60300-2 and provides guidance for selection and application of dependability elements and tasks with respect to systems or products containing software.

This application guide is intended for use by project managers, contract administrators, product designers, software developers, dependability specialists, quality specialists, support personnel and system maintainers who contribute to the dependability of products or systems.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 60300-3. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this section of IEC 60300-3 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) — Chapter 191: Dependability and quality of service*.

IEC 60300-1/ISO 9000-4:1993, *Dependability management — Part 1: Dependability programme management*.

IEC 60300-2:1995, *Dependability management — Part 2: Dependability programme elements and tasks*.

IEC 61160:1992, *Formal design review*.
Amendment 1 (1994)

ISO 8402:1994, *Quality management and quality assurance — Vocabulary*.

3 Definitions

For the purpose of this section of IEC 60300-3, the terms and definitions of IEC 60050(191) and ISO 8402 apply.

4 Software aspects

The software aspects of dependability deal with the specific software issues in the establishment and implementation of a dependability programme for a system or product containing software. Emphasis is placed on achieving dependability in the product design and performance objectives in reliability, maintainability and maintenance support.

In the application of a dependability programme to a system or product, it is important to address the dependability issue from a system view point. A product is an entity which may contain hardware or software components or both. A system is an integrated composite entity, which may include the product, supply material, personnel, and related support facilities and services. The system environment defines the operating conditions and interactions of the system components. The availability performance of the system is measured or assessed to validate the achievement of stated dependability objectives in terms of reliability, maintainability, and maintenance support.

Dependability is a collective measure of the performances of a system in its actual state of application or use, with or without the operation of specific software functions which may form part of an integrated system.

It should be noted that software cannot function by itself but forms part of a system to provide specific application. Software is a medium for realization of a system performance objective. Software is characterized in particular by its application function, operating environment, size, language and complexity, installation and upgrade processes. The software aspects of dependability address the software components within a system in the context of dependability performance of the system. They do not address the quality of the software as a stand alone item. Software quality is described in ISO/IEC 9126 [1]¹⁾.

The software aspects of dependability are associated with the integrity of the software component in system operation. Integrity is an inherent design attribute associated with risk containment. Risk is an undesirable exposure or threat associated with the system operation. Risk is characterized by its probability of occurrence and its impact or consequence of the event outcome. The ability of a system and its software component to contain risk is dependent on the system architecture, fault tolerant design, and the degree of rigour in the application of relevant methods to the software. The integrity level is the assigned risk associated with the system operation which is to be contained. The relationship between dependability and integrity is closely linked by the criticality of software application associated with the assigned integrity levels when dealing with the software affecting system performance.

¹⁾ Figures in square brackets refer to the bibliography given in Annex F.