

Software dependability through the software life-cycle processes — Application guide

ICS 35.080

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 61713:2000 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology, 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 committee 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 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, the IEC title page, pages 2 to 34, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the Management Systems Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 October 2000

© BSI 10-2000

ISBN 0 580 36480 1

Amendments issued since publication

Amd. No.	Date	Comments

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
61713**

Première édition
First edition
2000-06

**Sûreté de fonctionnement des logiciels
pendant leurs processus de cycle de vie –
Guide d'application**

**Software dependability through
the software life-cycle processes –
Application guide**



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CONTENTS

	Page
FOREWORD	3
INTRODUCTION	4
Clause	
1 Scope	5
2 Normative references	5
3 Definitions	6
4 Software life-cycle processes	10
5 Dependability activities in the primary software processes	11
5.1 Acquisition process	11
5.2 Supply process	15
5.3 Development process	17
5.4 Operation process	23
5.5 Maintenance process	26
6 Dependability activities in the supporting software processes	29
7 Dependability activities in the organizational software life-cycle processes	29
Annex A (informative) Association of software life-cycle processes with dependability programme elements and tasks	32
Annex B (informative) Interaction of users with primary software life-cycle processes	33
Bibliography	34

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SOFTWARE DEPENDABILITY THROUGH THE SOFTWARE LIFE-CYCLE PROCESSES – APPLICATION GUIDE

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 specifications, 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 61713 has been prepared by IEC technical committee 56: Dependability

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

FDIS	Report on voting
56/685/FDIS	56/690/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 3.

Annexes A and B are for information only.

The committee has decided that the contents of this publication will remain unchanged until 2003. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

Dependability is the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. IEC 60300-2 provides guidance on the elements and tasks to be included in a comprehensive dependability programme. More detailed guidance on the software aspects of a dependability programme is contained in IEC 60300-3-6. This International Standard is intended to support IEC 60300-3-6 by providing guidance on the achievement of software dependability in the context of software life-cycle processes which form the basis for many software standards. This guide identifies software life-cycle process activities that will help achieve dependable software (i.e. software that reliably performs according to requirements). A full description of the software life-cycle processes and the framework they provide to represent the software life cycle from software acquisition through to software maintenance is provided in ISO/IEC 12207.

The software activities are related to the various software life-cycle processes. A software life cycle process is a set of planned activities, including requirement specifications, performed to achieve the stated objective of a software project. This guide will facilitate the identification and implementation of those life-cycle activities that have a bearing on software dependability.

SOFTWARE DEPENDABILITY THROUGH THE SOFTWARE LIFE-CYCLE PROCESSES – APPLICATION GUIDE

1 Scope

This International Standard provides guidance on those aspects of software life-cycle activities that have a bearing on the achievement of dependable software. The software life-cycle activities are defined in the context of software life-cycle processes. This guide is intended to be used to support IEC 60300-3-6.

The software life-cycle activities identified can be part of a dependability programme for a system or in relation to a product containing software. The activities identified will help achieve software that is reliable and maintainable and help ensure that appropriate maintenance support will be provided. The activities can be applicable throughout the entire software life cycle or be limited to a subset of the software life-cycle processes depending upon the users of the software. The relationship between the users of the software and the software life-cycle processes is shown in annex B. They are grouped according to the various individual software life-cycle processes that represent the overall software life-cycle as defined in ISO/IEC 12207.

Emphasis is placed on the dependability requirements and activities applicable in the primary software life-cycle processes.

This guide can be used by acquirers, suppliers, developers, operators or maintainers of software. In addition to software and dependability specialists, this guide is intended for use by project managers, quality practitioners and other project participants who develop or use systems or products containing software.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

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

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

IEC 60300-3-6:1997, *Dependability management – Part 3: Application guide – Section 6: Software aspects of dependability*

IEC 61160, *Formal design review*

ISO/IEC 12207, *Information technology – Software life cycle processes*

ISO 8402, *Quality management and quality assurance – Vocabulary*

3 Definitions

For the purpose of this International Standard, the terms and definitions of IEC 60050(191), ISO/IEC 12207 and ISO 8402 apply together with the following.

3.1

dependability

collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. [IEV 191-02-03]

NOTE Software dependability will be described in terms of software reliability, software maintainability and software maintenance support.

3.2

dependability function

term used to describe an individual aspect of the software dependability requirement specification. The dependability function can describe reliability, maintainability or maintenance support-related dependability requirements

3.3

maintenance release

product release which is carried out for corrective maintenance rather than to provide enhanced functionality

3.4

software reliability

probability that no fault in any software element of a system will be activated in a given time interval in the operation of the system under given conditions

3.5

software maintainability

ease with which a detected fault in a software element of a system can be corrected

3.6

software maintenance support

ability of an organization, under given conditions, to provide upon demand the resources required to maintain a software element of a system, under a given maintenance policy

NOTE The given conditions are related to the software element itself and to the conditions under which it is used and maintained.

[IEV 191-02-08, modified]

To assist understanding of this standard, the following definitions of terms used in ISO/IEC 12207 are repeated here.

3.7

acquirer

organization that acquires or procures a system, software product or software service from a supplier

NOTE The acquirer could be one of the following: buyer, customer, owner, user, purchaser.

3.8

acquisition

process of obtaining a system, software product or software service

3.9

agreement

definition of terms and conditions under which a working relationship will be conducted

3.10

audit

conducted by an authorized person for the purpose of providing an independent assessment of software products and processes in order to assess compliance with requirements

3.11

baseline

formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle

3.12

configuration item

entity within a configuration that satisfies an end-use function and that can be uniquely identified at a given reference point

3.13

contract

binding agreement between two parties, especially enforceable by law, or a similar internal agreement wholly within an organization, for the supply of software service or for the supply, development, production, operation, or maintenance of a software product

3.14

developer

organization that performs development activities (including requirements analysis, design, testing through acceptance) during the software life-cycle process

3.15

evaluation

systematic determination of the extent to which an entity meets its specified criteria

3.16

firmware

combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control

3.17

life-cycle model

framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use

3.18

maintainer

organization that performs maintenance activities

3.19

monitoring

examination of the status of the activities of a supplier and of their results by the acquirer or a third party

3.20

non-deliverable item

hardware or software product that is not required to be delivered under the contract but may be employed in the development of a software product

3.21

off-the-shelf product

product that is already developed and available, usable either "as is" or with modification

3.22

operator

organization that operates the system

3.23

process

set of timely ordered and interrelated activities, which transform inputs into outputs

NOTE The term "activities" covers use of resources.

3.24

qualification

process of demonstrating whether an entity is capable of fulfilling specified requirements

3.25

qualification requirement

set of criteria or conditions that have to be met in order to qualify a software product as complying with its specifications and being ready for use in its target environment

3.26

qualification testing

testing, conducted by the developer and witnessed by the acquirer (as appropriate), to demonstrate that a software product meets its specifications and is ready for use in its target environment

3.27

quality assurance

all the planned and systematic activities implemented within the quality system, and demonstrated as needed, to provide adequate confidence that an entity will fulfil requirements for quality

NOTE 1 There are both internal and external purposes for quality assurance:

- a) internal quality assurance: within an organization, quality assurance provides confidence to management;
- b) external quality assurance: in contractual situations, quality assurance provides confidence to the customer or others.

NOTE 2 Some quality control and quality assurance actions are interrelated.

NOTE 3 Unless requirements for quality fully reflect the needs of the user, quality assurance may not provide adequate confidence.

3.28

release

particular version of a configuration item that is made available for a specific purpose (for example, test release)

3.29
request for proposal
tender

document used by the acquirer as the means to announce its intention to potential bidders to acquire a specified system, software product or software service

3.30
retirement

withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system

3.31
security

protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them

3.32
software product

set of computer programs, procedures, and possibly associated documentation and data

3.33
software service

performance of activities, work, or duties connected with a software product, such as its development, maintenance and operation

3.34
software unit

separately compilable piece of code

3.35
statement of work

document used by the acquirer as the means to describe and specify the tasks to be performed under the contract

3.36
supplier

organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract

NOTE 1 The term "supplier" is synonymous with contractor, producer, seller or vendor.

NOTE 2 The acquirer may designate a part of its organization as supplier.

3.37
system

integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective

3.38
test coverage

extent to which the test cases test the requirements for the system or software product

3.39
testability

extent to which an objective and feasible test can be designed to determine whether a requirement is met

3.40

user

individual or organization that uses the operational system to perform a specific function

NOTE The user may perform other roles, such as acquirer, developer, or maintainer.

3.41

validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 In design and development, validation concerns the process of examining a product to determine conformity with user needs.

NOTE 2 Validation is normally performed on the final product under defined operating conditions. It may be necessary in earlier stages.

NOTE 3 "Validated" is used to designate the corresponding status.

NOTE 4 Multiple validations may be carried out if there are different intended uses.

3.42

verification

confirmation by examination and provision of objective evidence that specified requirements have been fulfilled

NOTE 1 In design and development, verification concerns the process of examining the result of a given activity to determine conformity with the stated requirements for that activity.

NOTE 2 "Verified" is used to designate the corresponding status.

3.43

version

identified instance of an item

NOTE Modification to a version of a software product, resulting in a new version, requires configuration management action.

4 Software life-cycle processes

A software life-cycle process is a set of planned activities or tasks necessary to achieve a stated objective of a software project. There are three groups of processes: primary, supporting and organizational, involving activities relating to a software product from its conception to its retirement.

The five primary processes provide guidance to acquirers, suppliers, developers, operators and maintainers of systems or products containing software.

The eight supporting life-cycle processes support another process and can be used with the five primary processes. The supporting processes are documentation, configuration management, quality assurance, verification, validation, joint review, audit and problem resolution.

The four organizational processes can be used by the major parties or primary processes depending upon the organizational or project needs. The organizational processes are management, infrastructure, improvement and training. Details of the software life-cycle processes and their use are given in ISO/IEC 12207.

The relationships of the software life-cycle processes with the dependability programme elements and tasks described in IEC 60300-2, as they relate to products containing software, is described in IEC 60300-2. Cross-references are made to specific subclauses of IEC 60300-2 in annex A.