IEC 60300-3-4

Edition 3.0 2021-10

PRE-RELEASE VERSION (FDIS)

colour inside

Dependability management –
Part 3-4: Application guide – Specification of dependability requirements

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 03.100.40; 03.120.01

56/1932/FDIS

FINAL DRAFT INTERNATIONAL STANDARD (FDIS)

PROJECT NUMBER:	
IEC 60300-3-4 ED3	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2021-10-08	**2021-11-19**
SUPERSEDES DOCUMENTS:	
56/1891/CDV, 56/1913A/RVC	

IEC TC 56 : DEPENDABILITY	
SECRETARIAT: United Kingdom	SECRETARY: Mr Amit Patel
OF INTEREST TO THE FOLLOWING COMMITTEES:	HORIZONTAL STANDARD: ☐
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Final Draft International Standard (FDIS) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is a draft distributed for approval. It may not be referred to as an International Standard until published as such.

In addition to their evaluation as being acceptable for industrial, technological, commercial and user purposes, Final Draft International Standards may on occasion have to be considered in the light of their potential to become standards to which reference may be made in national regulations.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Dependability management - Part 3-4: Application guide - Specification of dependability requirements

PROPOSED STABILITY DATE: 2023

NOTE FROM TC/SC OFFICERS:

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 8
2 Normative references 8
3 Terms and definitions 8
4 Specifying dependability 10
4.1 Description of dependability specification 10
4.2 Principles 13
4.3 Benefits 15
5 Derivation of dependability requirements 15
5.1 General 15
5.2 Define stakeholder needs and expectations 17
5.3 Develop supporting documentation 18
5.4 Derive dependability requirements 19
5.5 Justify the measures used for the dependability requirements 33
5.6 Complete dependability specification 34
5.7 Review dependability specification 34
Annex A (informative) Discussion on useful life 35
A.1 General 35
A.2 Factors that determine useful life 35
A.3 Specification of useful life of non-repairable items (components) 36
Annex B (informative) Process for prioritizing dependability attributes 38
Annex C (informative) Development of a dependability specification for a home security system 40
C.1 Define stakeholder needs and expectations 40
C.2 Develop supporting documentation 40
C.3 Derive the dependability requirements 45
C.4 Complete dependability specification 46
Annex D (informative) Influencing factors for dependability specification 48
D.1 Examples of constraints on system dependability 48
D.2 Type of system operation 48
D.3 Criticality of operation 49
D.4 Determining relevant influencing factors for the evaluation of system functions 52
Bibliography 54

Figure 1 – High level process for derivation of dependability requirements in the specification 16
Figure 2 – What are we trying to achieve? 18
Figure 3 – What do we need to manage? 22
Figure 4 – What constraints are there? 22
Figure 5 – Assurance considerations 23
Figure 6 – Reliability requirements 27
Figure 7 – Maintainability requirements 29

Figure 8 – Supportability requirements....31
Figure 9 – Availability requirements....33
Figure B.1 – Process for prioritizing attributes....39
Figure C.1 – System configuration for normal mode of operation....44
Figure C.2 – System configuration for panic mode of operation....44
Figure C.3 – System configuration for security service mode of operation....45

Table B.1 – Questions for prioritizing dependability attributes....38
Table D.1 – Examples of influencing factors under each influencing condition....52
Table D.2 – Relationship of system properties with influencing conditions....53

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Specification of dependability requirements

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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.

IEC 60300-3-4 has been prepared by IEC technical committee 56: Dependability. It is an International Standard.

This third edition cancels and replaces the second edition published in 2007. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) consistency with the other of the six core IEC dependability standards;
b) a process for defining requirements has been included;
c) the definitions and language used have been made consistent with other system related standards.

The text of this International Standard is based on the following documents:

Draft	Report on voting
56/XX/FDIS	56/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Dependability is the ability to perform as and when required. A dependable item is one where there is justified confidence that it operates as desired and satisfies agreed stakeholder expectations.

Dependability has many attributes, but is usually characterized in terms of reliability, maintainability, and supportability, and the derived characteristic of availability. Dependability also includes the performance characteristics such as durability, testability and restorability as well as security and integrity, particularly in relation to software-based systems.

Dependability is an important attribute that affects the value items generate. Consequently, relevant dependability attributes should be defined and specified in addition to functional performance requirements and physical attributes. Whilst mainly addressing system and equipment level dependability, many of the techniques described in the various dependability related IEC standards may also be applied to products or at the component level. The term "item" is used throughout this document to mean an individual part, component, device, functional unit, off-the-shelf (OTS) equipment, subsystem, or system. The item may consist of hardware, software, people or any combination thereof (see IEC 60050-192). In order to refer to a specific kind of "item", terms like component, OTS, product or large open system are used.

Dependability attributes may be specified for an individual system or product (for example, a vehicle) and/or a group of similar systems or products (for example, a fleet of similar vehicles).

Dependability attributes may be specified using either quantitative and/or qualitative measures. In order to assess the values of some of the dependability attributes achieved, statistical methods may be necessary.

The levels of reliability, maintainability, supportability and availability achieved by an item depend on the conditions under which it is realized, utilized, maintained and supported and also on the life profile of the system. The requirements in the dependability specification, should also define the following:

- conditions under which the item is stored, transported, realized and utilized;
- life profile and expected useful life;
- maintenance policies;
- available support.

Dependability attributes may be specified, along with other performance characteristics, in various ways depending on the situation. In a basic project context where an acquirer obtains an item from a supplier, three main types are:

1) specifications written by the supplier;
2) specifications written by the acquirer;
3) specifications mutually agreed or written by the supplier and the acquirer.

The guidance in this document is applicable to all three types of specifications and may be adapted to other situations as needed.

This document provides guidance for writing dependability requirements in specifications, together with a means of assuring the achievement of those requirements.

This document is one of the six "top level" interrelated dependability standards that provide managers and technical personnel with guidance on how to effectively plan and implement dependability activities. As such, this document should be used in conjunction with:

- IEC 60300-1 [1][1], which highlights the importance and benefits of managing dependability. It gives guidance on dependability activities and how to integrate them into an existing management system and life cycle processes;
- IEC 60300-3-1 [2], IEC 60300-3-10 [3], IEC 60300-3-14 [4] and IEC 60300-3-17 [5] which provide guidance on how to identify and apply appropriate analysis and assurance techniques for reliability, maintainability (and maintenance), supportability (and support) and availability respectively.

[1] Numbers in square brackets refer to the bibliography

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Specification of dependability requirements

1 Scope

This part of IEC 60300 gives guidance on specifying dependability requirements and collating these requirements in a specification, together with a list of the means of assuring the achievement of the dependability requirements.

The guidance provided includes:

- specifying quantitative and qualitative reliability, maintainability, supportability and availability requirements;
- advising acquirers on how to ensure that the requirements can be fulfilled by suppliers;
- advising suppliers to help them meet the acquirer's requirements.

Other obligations, such as legislation and governmental regulations, can also place requirements on items, in addition to any requirements derived in accordance with this document.

Whilst mainly addressing system and equipment level dependability, many of the techniques described in the various dependability related IEC standards can also be applied to products or at the component level. The term "item" is used throughout this document.

This guidance is given in a basic project context where an acquirer obtains an item from a supplier. It can be modified and adapted to other situations as needed.

NOTE 1 This document does not directly consider safety and environment specifications although much of the guidance in this document could also be applied to them.

NOTE 2 This document does not cover items with special multi-stakeholder long-term arrangements (e.g. services provided through Public-Private Partnership procurements) and how dependability is specified in such arrangements.

NOTE 3 The guidance in this document can be applied to some aspects of the specification of requirements relating to software but specific guidance can be found in IEC 62628 [6] and the different parts of the IEC 61508 series [7].

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60050-192, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability* (available at http://www.electropedia.org)