# Dependability management -- Part 3-4: Application guide - Guide to the specification of dependability requirements

Dependability management -- Part 3-4: Application guide - Guide to the specification of dependability requirements

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

| | |
|---|---|
| Käesolev Eesti standard EVS-EN 60300-3-4:2008 sisaldab Euroopa standardi EN 60300-3-4:2008 ingliskeelset teksti. | This Estonian standard EVS-EN 60300-3-4:2008 consists of the English text of the European standard EN 60300-3-4:2008. |
| Standard on kinnitatud Eesti Standardikeskuse 20.02.2008 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas. | This standard is ratified with the order of Estonian Centre for Standardisation dated 20.02.2008 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation. |
| Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 11.01.2008. | Date of Availability of the European standard text 11.01.2008. |
| Standard on kättesaadav Eesti standardiorganisatsioonist. | The standard is available from Estonian standardisation organisation. |



**ICS** 03.100.40, 03.120.01

**Võtmesõnad:**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN 60300-3-4

January 2008

ICS 03.100.40; 03.120.01

English version

# Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements

(IEC 60300-3-4:2007)

Gestion de la sûreté de fonctionnement - Partie 3-4: Guide d'application - Spécification d'exigences de sûreté de fonctionnement (CEI 60300-3-4:2007)

Zuverlässigkeitsmanagement - Teil 3-4: Anwendungsleitfaden - Anleitung zum Festlegen von Zuverlässigkeitsforderungen (IEC 60300-3-4:2007)



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 60300-3-4:2008 E

## Foreword

The text of document 56/1212/FDIS, future edition 2 of IEC 60300-3-4, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 60300-3-4 on 2007-12-01.

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) | 2008-09-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2010-12-01 |

Annex ZA has been added by CENELEC.

———————

## Endorsement notice

The text of the International Standard IEC 60300-3-4:2007 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 60812 | NOTE | Harmonized as EN 60812:2006 (not modified). |
| IEC 61165 | NOTE | Harmonized as EN 61165:2006 (not modified). |
| IEC 61508-1 | NOTE | Harmonized as EN 61508-1:2001 (not modified). |
| IEC 61508-2 | NOTE | Harmonized as EN 61508-2:2001 (not modified). |
| IEC 61508-3 | NOTE | Harmonized as EN 61508-3:2001 (not modified). |
| IEC 61508-4 | NOTE | Harmonized as EN 61508-4:2001 (not modified). |
| IEC 61508-5 | NOTE | Harmonized as EN 61508-5:2001 (not modified). |
| IEC 61508-6 | NOTE | Harmonized as EN 61508-6:2001 (not modified). |
| IEC 61508-7 | NOTE | Harmonized as EN 61508-7:2001 (not modified). |
| IEC 61709 | NOTE | Harmonized as EN 61709:1998 (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 | – | – |
| IEC 60300-1 | – [1)] | Dependability management - Part 1: Dependability management systems | EN 60300-1 | 2003 [2)] |
| IEC 60300-2 | – [1)] | Dependability management - Part 2: Guidelines for dependability management | EN 60300-2 | 2004 [2)] |
| IEC 60300-3-1 | – [1)] | Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology | EN 60300-3-1 | 2004 [2)] |
| IEC 60300-3-2 | – [1)] | Dependability management - Part 3-2: Application guide - Collection of dependability data from the field | EN 60300-3-2 | 2005 [2)] |
| IEC 60300-3-3 | – [1)] | Dependability management - Part 3-3: Application guide - Life cycle costing | EN 60300-3-3 | 2004 [2)] |
| IEC 60300-3-5 | – [1)] | Dependability management - Part 3-5: Application guide - Reliability test conditions and statistical test principles | – | – |
| IEC 60300-3-10 | – [1)] | Dependability management - Part 3-10: Application guide - Maintainability | – | – |
| IEC 60300-3-12 | – [1)] | Dependability management - Part 3-12: Application guide - Integrated logistic support | EN 60300-3-12 | 2004 [2)] |
| IEC 60300-3-14 | – [1)] | Dependability management - Part 3-14: Application guide - Maintenance and maintenance support | EN 60300-3-14 | 2004 [2)] |

[1)] Undated reference.

[2)] Valid edition at date of issue.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC 60605-4 | – [1)] | Equipment reliability testing - Part 4: Statistical procedures for exponential distribution - Point estimates, confidence intervals, prediction intervals and tolerance intervals | – | – |
| IEC 60605-6 | – [1)] | Equipment reliability testing - Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity | – | – |
| IEC 60706-2 | – [1)] | Maintainability of equipment - Part 2: Maintainability requirements and studies during the design and development phase | EN 60706-2 | 2006 [2)] |
| IEC 60706-3 | – [1)] | Maintainability of equipment - Part 3: Verification and collection, analysis and presentation of data | EN 60706-3 | 2006 [2)] |
| IEC 60706-5 | – [1)] | Maintainability of equipment - Part 5: Testability and diagnostic testing | EN 60706-5 | 2007 [2)] |
| IEC 61014 | – [1)] | Programmes for reliability growth | EN 61014 | 2003 [2)] |
| IEC 61025 | – [1)] | Fault Tree Analysis (FTA) | EN 61025 | 2007 [2)] |
| IEC 61070 | – [1)] | Compliance test procedures for steady-state availability | – | – |
| IEC 61078 | – [1)] | Analysis techniques for dependability - Reliability block diagram and Boolean methods | EN 61078 | 2006 [2)] |
| IEC 61123 | – [1)] | Reliability testing - Compliance test plans for success ratio | – | – |
| IEC 61124 | – [1)] | Reliability testing - Compliance tests for constant failure rate and constant failure intensity | EN 61124 | 2006 [2)] |
| IEC 61160 | – [1)] | Design review | EN 61160 | 2005 [2)] |
| IEC 61164 | – [1)] | Reliability growth - Statistical test and estimation methods | EN 61164 | 2004 [2)] |
| IEC 61508 | Series | Functional safety of electrical/electronic/programmable electronic safety-related systems | EN 61508 | Series |
| IEC 61649 | – [1)] | Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data | – | – |
| IEC 61703 | – [1)] | Mathematical expressions for reliability, availability, maintainability and maintenance support terms | EN 61703 | 2002 [2)] |
| IEC 61710 | – [1)] | Power law model - Goodness-of-fit tests and estimation methods | – | – |
| IEC 61713 | – [1)] | Software dependability through the software life-cycle processes - Application guide | – | – |

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC 62198 | – [1)] | Project risk management - Application guidelines | – | – |
| IEC 62308 | – [1)] | Equipment reliability - Reliability assessment methods | EN 62308 | 2006 [2)] |
| IEC 62347 | – [1)] | Guidance on system dependability specifications | EN 62347 | 2007 [2)] |

# CONTENTS

# INTRODUCTION

In many systems, reliability, maintainability and availability are essential performance characteristics. These characteristics, together with maintenance support performance, are known collectively as dependability.

In systems where any of the dependability characteristics are important, it is necessary that these characteristics should be defined and specified in the same way as other system characteristics such as technical performance, dimensions and mass.

The levels of reliability, maintainability, availability and maintenance support performance achieved by a system depend on the conditions under which the system is used and also on the mission profile of the system. When requirements for dependability characteristics are specified, it is necessary to define the conditions of storage, transportation, installation and use that will be applied to the system. It may be important to take account not only of the conditions under which the system will operate, but also of the maintenance policy and organization for maintenance support of the system.

In order to assess the values of the dependability characteristics achieved, it is necessary to use statistical methods.

Dependability characteristics may be specified, like other performance characteristics, in three different ways:

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

This standard is applicable to all three types of specification.

This standard complements IEC 62347 which deals with the definitions of systems and their constituent elements and how to define these so that the dependability requirements of each element can be specified using this standard. The premise of IEC 62347 is to identify system requirements by functions from a system engineering perspective. It provides a process for transforming the purchaser's view on system applications into a technical view for engineering the system. IEC 62347 emphasises architectural and functional design for realisation of functions with appropriate selection of hardware, software and human elements to achieve the system dependability requirements relevant to the purchaser's needs.

# DEPENDABILITY MANAGEMENT –

# Part 3-4: Application guide – Guide to the specification of dependability requirements



## 1 Scope

This part of IEC 60300 gives guidance on specifying the required dependability characteristics in specifications, together with specifications of procedures and criteria for verification and validation.

The guidance provided includes the following:

– advice on specifying quantitative and qualitative reliability, maintainability, availability and maintenance support requirements;

– advice to purchasers of a system on how to ensure that the specified requirements will be fulfilled by suppliers;

– advice to suppliers to help them to meet purchaser requirements.

Other documents, such as legislation and governmental regulation may also place requirements on systems and these should be applied in addition to any specifications derived in accordance with this standard.

NOTE 1 Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of IEC 60300 may also be applied to products, items or at the component level. The term system is used throughout this standard.

NOTE 2 This standard does not give guidance on the management of dependability programmes or on the various activities necessary to fulfil stated availability, reliability, maintainability and maintenance support requirements. For this general guidance, see other standards.

NOTE 3 Safety and environment specifications are not directly considered in this guide. However, much of the guidance in this standard could also be applied to safety or environmental specification.

NOTE 4 Specifications for the dependability of a service are not considered in this guide. This includes the provision of a service such as those provided through Public-Private Partnership procurements.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the reference 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.*

IEC 60300-1, *Dependability management systems – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60706-5, *Maintainability of equipment – Part 5: Diagnostic testing*

IEC 61014, *Programmes for reliability growth*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61070, *Compliance test procedures for steady-state availability*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*

IEC 61160, *Design review*

IEC 61164, *Reliability growth – Statistical test and estimation methods*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61649, *Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data*

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61713, *Software dependability through the software life cycle processes – Application guide*

IEC 62198, *Project risk management – Application guidelines*

IEC 62308, *Equipment Reliability – Reliability assessment methods*

IEC 62347, *Guidance on system dependability specifications*

## 3 Terms and definitions

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

NOTE Definitions of “dependability”, “availability (performance)”, “reliability (performance)”, “maintainability (performance)”, “maintenance support”, “failure”, “fault”, “item”, “time to failure”, and “operating time between failures” are given in IEC 60050-191.

**3.1**
**verification**
confirmation, through provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005, definition 3.8.4 modified]

NOTE 1 In the context of this standard, verification is the activity of demonstrating for each phase of the relevant life cycle, by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

NOTE 2 Example verification activities include:

– reviews on outputs (documents from all phases of the life cycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

– design reviews;

– tests and analysis performed on the designed systems to ensure that they perform according to their specification;

– integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together.

**3.2**
**validation**
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[ISO 9000:2005, definition 3.8.5 modified]

NOTE Validation is the activity of demonstrating that the system under consideration, before or after installation, meets in all respects the requirements specification for that system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software requirements specification.

## 4 General considerations for dependability specifications

### 4.1 The need for dependability

All systems exhibit some level of dependability, however often they might fail or require maintenance. However, if a system fails too often it might not be available to perform when required or it might cost too much to maintain. In addition, systems that fail repeatedly will get a bad reputation with the user and are unlikely to be bought again once a replacement is