

© Copyright SEK. Reproduction in any form without permission is prohibited.

Tillförlitlighetsverksamhet – Del 3-4: Riktlinjer – Anvisning för specificering av tillförlitlighetskrav

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

Som svensk standard gäller europastandarden EN 60300-3-4:2008. Den svenska standarden innehåller den officiella engelska språkversionen av EN 60300-3-4:2008.

Nationellt förord

Europastandarden EN 60300-3-4:2008

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 60300-3-4, Second edition, 2007 - Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements**

utarbetad inom International Electrotechnical Commission, IEC.

Denna standard kompletterar SS-EN 62347.

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPEAN STANDARD

EN 60300-3-4

NORME EUROPÉENNE

EUROPÄISCHE NORM

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)

This European Standard was approved by CENELEC on 2007-12-01. 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

© 2008 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 60300-3-4:2008 E

SEK Svensk Elstandard

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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	9
4 General considerations for dependability specifications	9
4.1 The need for dependability	9
4.2 Requirements and goals	11
4.3 Systems	11
4.4 Demonstration of achievement of requirements	13
4.4.1 Concept.....	13
4.4.2 Activities.....	14
4.5 Contracting for dependability.....	15
4.6 Types of specification.....	16
4.7 Derivation of dependability specifications	17
5 Dependability management	18
6 Availability.....	19
6.1 General.....	19
6.1.1 Choice of dependability characteristic.....	19
6.1.2 Relationship between availability, reliability and maintainability	19
6.2 Availability specifications.....	20
6.2.1 Quantitative requirements.....	20
6.2.2 Qualitative requirements.....	20
6.3 Provision of availability verification and validation	20
6.3.1 General	20
6.3.2 Verification and validation by testing.....	21
6.3.3 Verification and validation by analysis	21
7 Reliability	21
7.1 General.....	21
7.2 Reliability specification	22
7.2.1 Quantitative requirements.....	22
7.2.2 Qualitative requirements.....	23
7.3 Reliability verification and validation.....	24
7.3.1 General	24
7.3.2 Verification and validation by testing.....	24
7.3.3 Verification and validation by analysis	25
8 Maintainability	25
8.1 General.....	25
8.2 Maintainability specification.....	25
8.2.1 Quantitative requirements.....	25
8.2.2 Qualitative requirements.....	26
8.3 Maintainability verification and validation.....	26
9 Maintenance support	27
9.1 General.....	27
9.2 Maintenance support specification.....	27

9.2.1	Quantitative requirements.....	27
9.2.2	Qualitative requirements.....	28
9.3	Maintenance support verification and validation	28
Annex A (informative)	Reference standards for verification and validation techniques.....	29
Annex B (informative)	Examples of reliability, maintainability, maintenance support and availability requirements	31
Bibliography.....		33
Figure 1 – Relationship between cost and reliability.....		10
Figure 2 – System elements.....		12
Table A.1 – Techniques for dependability verification and validation through testing.....		29
Table A.2 – Techniques for dependability verification and validation through analysis.....		30

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*