

**Dependability management - Part 3-15: Application
guide - Engineering of system dependability**

This document is a preview generated by EVS

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 60300-3-15:2010 sisaldab Euroopa standardi EN 60300-3-15:2009 ingliskeelset teksti.

Standard on kinnitatud Eesti Standardikeskuse 28.02.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 04.12.2009.

Standard on kättesaadav Eesti standardiorganisatsioonist.

This Estonian standard EVS-EN 60300-3-15:2010 consists of the English text of the European standard EN 60300-3-15:2009.

This standard is ratified with the order of Estonian Centre for Standardisation dated 28.02.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

Date of Availability of the European standard text 04.12.2009.

The standard is available from Estonian standardisation organisation.

ICS 03.120.01

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

Right to reproduce and distribute Estonian Standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:
Aru str 10 Tallinn 10317 Estonia; www.evs.ee; Phone: +372 605 5050; E-mail: info@evs.ee

**Dependability management -
Part 3-15: Application guide -
Engineering of system dependability
(IEC 60300-3-15:2009)**

Gestion de la sûreté de fonctionnement -
Partie 3-15: Guide d'application -
Ingénierie de la sûreté de fonctionnement
des systèmes
(CEI 60300-3-15:2009)

Zuverlässigkeitsmanagement -
Teil 3-15: Anwendungsleitfaden -
Technische Realisierung der
Systemzuverlässigkeit
(IEC 60300-3-15:2009)

This European Standard was approved by CENELEC on 2009-10-01. 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: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 56/1315/FDIS, future edition 1 of IEC 60300-3-15, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 60300-3-15 on 2009-10-01

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) 2010-07-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2012-10-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 60300-3-15:2009 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:

[1] IEC 61069-1	NOTE Harmonized as EN 61069-1:1993 (not modified).
[2] IEC 62347	NOTE Harmonized as EN 62347:2007 (not modified).
[7] IEC 60300-3-1	NOTE Harmonized as EN 60300-3-1:2004 (not modified).
[9] IEC 61508	NOTE Harmonized in EN 61508 series (not modified).
[10] IEC 61508-1	NOTE Harmonized as EN 61508-1:2001 (not modified).
[12] IEC 61014	NOTE Harmonized as EN 61014:2003 (not modified).
[13] IEC 61164	NOTE Harmonized as EN 61164:2004 (not modified).
[14] ISO 10007	NOTE Harmonized as EN ISO 10007:1996 (not modified).
[16] IEC 60300-3-11	NOTE Harmonized as EN 60300-3-11:2009 (not modified).
[17] IEC 60300-3-12	NOTE Harmonized as EN 60300-3-12:2004 (not modified).
[22] IEC 60721	NOTE Harmonized in EN 60721 series (not modified).
IEC 60300-3-4	NOTE Harmonized as EN 60300-3-4:2008 (not modified).
IEC 60812	NOTE Harmonized as EN 60812:2006 (not modified).
IEC 61025	NOTE Harmonized as EN 61025:2007 (not modified).
IEC 61078	NOTE Harmonized as EN 61078:2006 (not modified).
IEC 61508-7	NOTE Harmonized as EN 61508-7:2001 (not modified).
IEC 61709	NOTE Harmonized as EN 61709:1998 (not modified).
IEC 62308	NOTE Harmonized as EN 62308:2006 (not modified).
ISO 13407	NOTE Harmonized as EN ISO 13407:1999 (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 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⁾

¹⁾ Undated reference.

²⁾ Valid edition at date of issue.

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	7
4 System dependability engineering and applications	8
4.1 Overview of system dependability engineering	8
4.2 System dependability attributes and performance characteristics	9
5 Managing system dependability	10
5.1 Dependability management	10
5.2 System dependability projects	10
5.3 Tailoring to meet project needs	11
5.4 Dependability assurance	11
6 Realization of system dependability.....	11
6.1 Process for engineering dependability into systems.....	11
6.1.1 Purpose of dependability process	11
6.1.2 System life cycle and processes	11
6.1.3 Process applications through the system life cycle	12
6.2 Achievement of system dependability	14
6.2.1 Purpose of system dependability achievements	14
6.2.2 Criteria for system dependability achievements	14
6.2.3 Methodology for system dependability achievements.....	15
6.2.4 Realization of system functions	16
6.2.5 Approaches to determine achievement of system dependability.....	17
6.2.6 Objective evidence of achievements	18
6.3 Assessment of system dependability	18
6.3.1 Purpose of system dependability assessments	18
6.3.2 Types of assessments	18
6.3.3 Methodology for system dependability assessments.....	20
6.3.4 Assessment value and implications	21
6.4 Measurement of system dependability	21
6.4.1 Purpose of system dependability measurements	21
6.4.2 Classification of system dependability measurements.....	22
6.4.3 Sources of measurements	23
6.4.4 Enabling systems for dependability measurements.....	23
6.4.5 Interpretation of dependability measurements.....	24
Annex A (informative) System life cycle processes and applications	25
Annex B (informative) Methods and tools for system dependability development and assurance.....	35
Annex C (informative) Guidance on system application environment.....	42
Annex D (informative) Checklists for System Dependability Engineering.....	47
Bibliography.....	54
Figure 1 – An overview of a system life cycle.....	12
Figure 2 – An example of a process model	13

Figure A.1 – An overview of system life cycle processes.....	25
Figure C.1 – Environmental requirements definition process	43
Figure C.2 – Mapping system application environments to exposures	44

This document is a preview generated by EVS

INTRODUCTION

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

- process,
- achievement,
- assessment, and
- measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

2 Normative references

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.

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

system

set of interrelated items considered as a whole for a defined purpose, separated from other items

NOTE 1 A system is generally defined with the view of performing a definite function.

NOTE 2 The system is considered to be bound by an imaginary surface that intersects the links between the system and the environment and the other external systems.

NOTE 3 External resources (i.e. outside the system boundary) may be required for the system to operate.

NOTE 4 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

3.2

subsystem

system that is part of a more complex system

3.3

operating profile

complete set of tasks to achieve a specific system objective