IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

IEC 60300-3-4:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

W

ICS 03.100.40; 03.120.01

ISBN 2-8318-9308-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Guide to the 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

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

This second edition cancels and replaces the first edition published in 1996 and constitutes a technical revision.

The main changes from the previous edition are as follows:

– the concept of systems has been included and the need to specify the dependability of the system and not just the physical equipment has been stressed;
– the need for verification and validation of the requirement has been included;
– differentiation has been made between requirements, that can be measured and verified and validated, and goals, which cannot;
– the content on availability, maintainability and maintenance support has been updated and expanded to similar level of detail to reliability.

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

FDIS	Report on voting
56/1212/FDIS	56/1233/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 2.

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

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

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