

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

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

CONTENTS

FOREWORD.....	4
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

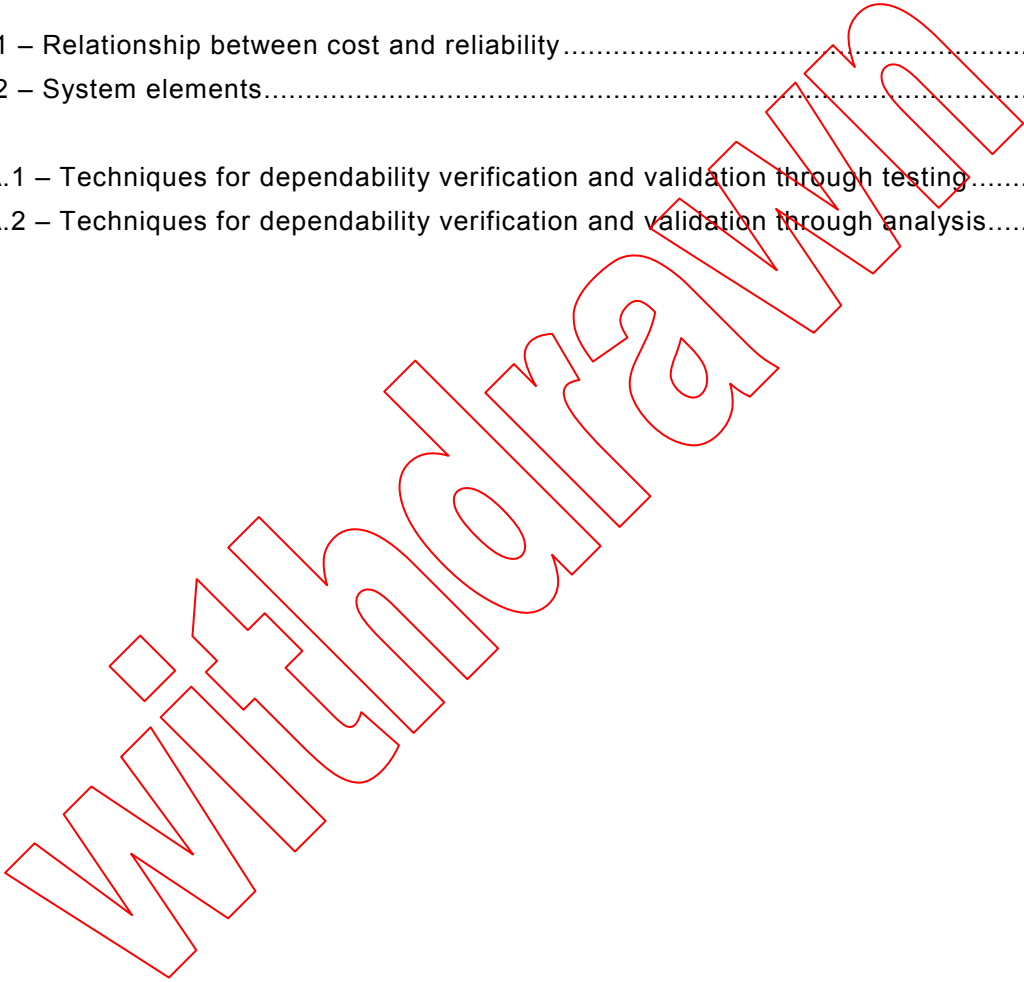
- 9.2.1 Quantitative requirements..... 27
- 9.2.2 Qualitative requirements..... 28
- 9.3 Maintenance support verification and validation 28

- 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



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.

Withdrawn

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.