SLOVENSKI STANDARD
SIST EN 60300-3-1:2007

01-januar-2007

Upravljanje zagotovljivosti - 3-1. del: Vodilo za uporabo - Tehnike analiziranja zagotovljivosti - Vodilo za metodologijo (IEC 60300-3-1:2003)

Dependability management -- Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology

Zuverlässigkeitsmanagement -- Teil 3-1: Anwendungsleitfaden - Verfahren zur Analyse der Zuverlässigkeit - Leitfaden zur Methodik

Gestion de la sûreté de fonctionnement -- Partie 3-1: Guide d'application - Techniques d'analyse de la sûreté de fonctionnement - Guide méthodologique

Ta slovenski standard je istoveten z: EN 60300-3-1:2004

ICS:

03.120.01	Kakovost na splošno	Quality in general
21.020	Značilnosti in načrtovanje strojev, aparatov, opreme	Characteristics and design of machines, apparatus, equipment

SIST EN 60300-3-1:2007 en

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60300-3-1

September 2004

ICS 03.120.30;21.020

English version

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

(IEC 60300-3-1:2003)

Gestion de la sûreté de fonctionnement
Partie 3-1: Guide d'application -
Techniques d'analyse de la sûreté
de fonctionnement –
Guide méthodologique
(CEI 60300-3-1:2003)

Zuverlässigkeitsmanagement
Teil 3-1: Anwendungsleitfaden –
Verfahren zur Analyse der Zuverlässigkeit -
Leitfaden zur Methodik
(IEC 60300-3-1:2003)

This European Standard was approved by CENELEC on 2004-09-01. 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, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and 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

Foreword

The text of the International Standard IEC 60300-3-1:2003, prepared by IEC TC 56, Dependability, was submitted to the formal vote and was approved by CENELEC as EN 60300-3-1 on 2004-09-01.

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)	2005-09-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2007-09-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 60300-3-1:2003 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 60300-2 NOTE Harmonized as EN 60300-2:1996 (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 Where 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	1990	International Electrotechnical Vocabulary (IEV) Chapter 191: Dependability and quality of service	-	-
IEC 60300-3-2	1993	Dependability management Part 3: Application guide – Section 2: Collection of dependability data from the field	-	-
IEC 60300-3-4	1996	Part 3: Application guide – Section 4: Guide to the specification of dependability requirements	-	-
IEC 60300-3-5	2001	Part 3-5: Application guide - Reliability test conditions and statistical test principles	-	-
IEC 60300-3-10	2001	Part 3-10: Application guide - Maintainability	-	-
IEC 60706-1	1982	Guide on maintainability of equipment Part 1 - Sections 1, 2 and 3: Introduction, requirements and maintainability programme	-	-
IEC 60706-2	1990	Part 2 - Section 5: Maintainability studies during the design phase	-	-
IEC 60812	1985	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)	HD 485 S1	1987
IEC 61078	1991	Analysis techniques for dependability - Reliability block diagram method	EN 61078	1993
IEC 61165	1995	Application of Markov techniques	-	-
IEC 61709	1996	Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion	EN 61709	1998

Publication	Year	Title	EN/HD	Year
IEC 61882	2001	Hazard and operability studies (HAZOP studies) - Application guide	-	-
ISO 9000	2000	Quality management systems - Fundamentals and vocabulary	EN ISO 9000	2000

INTERNATIONAL STANDARD

IEC 60300-3-1

Second edition
2003-01

Dependability management –

Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

Gestion de la sûreté de fonctionnement –

Partie 3-1:
Guide d'application –
Techniques d'analyse de la sûreté de fonctionnement –
Guide méthodologique

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XA

For price, see current catalogue

CONTENTS

FOREWORD 3
INTRODUCTION 4
1 Scope 5
2 Normative references 5
3 Definitions 6
4 Basic dependability analysis procedure 7
4.1 General procedure 7
4.2 Dependability analysis methods 8
4.3 Dependability allocations 10
4.4 Dependability analysis 11
4.5 Maintenance and repair analysis and considerations 13
5 Selecting the appropriate analysis method 13
Annex A (informative) Brief description of analysis techniques 16
Bibliography 58

Figure 1 – General dependability analysis procedure 7
Figure A.1 – Temperature dependence of the failure rate 19
Figure A.2 – Fault tree for an audio amplifier 21
Figure A.3 – Sub-tree from FTA in Figure A.2 22
Figure A.4 – Event tree 24
Figure A.5 – Elementary models 26
Figure A.6 – Example of unit 28
Figure A.7 – State-transition diagram 29
Figure A.8 – Block diagram of a multiprocessor system 32
Figure A.9 – Petri net of a multiprocessor system 33
Figure A.10 – The HAZOP study procedure 37
Figure A.11 – Human errors shown as an event tree 41
Figure A.12 – Example – Application of stress–strength criteria 43
Figure A.13 – Truth table for simple systems 44
Figure A.14 – Example 44
Figure A.15 – Cause and effect diagram 56

Table 1 – Use of methods for general dependability analysis tasks 9
Table 2 – Characteristics of selected dependability analysis methods 15
Table A.1 – Symbols used in the representation of the fault treee 22
Table A.2 – States of the unit 28
Table A.3 – Effects of failures in functional and diagnostic parts 29
Table A.4 – Transition rates 30
Table A.5 – Example of FMEA 35
Table A.6 – Basic guide words and their generic meanings 36
Table A.7 – Additional guide words relating to clock time and order or sequence 36
Table A.8 – Credible human errors 40
Table A.9 – Truth table example 45

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

DEPENDABILITY MANAGEMENT –

Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.

3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-1 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 1991, and constitutes a full technical revision. In particular, the guidance on the selection of analysis techniques and the number of analysis techniques covered has been extended.

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

FDIS	Report on voting
56/825/FDIS	56/840/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.

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

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

INTRODUCTION

The analysis techniques described in this part of IEC 60300 are used for the prediction, review and improvement of reliability, availability and maintainability of an item.

These analyses are conducted during the concept and definition phase, the design and development phase and the operation and maintenance phase, at various system levels and degrees of detail, in order to evaluate, determine and improve the dependability measures of an item. They can also be used to compare the results of the analysis with specified requirements.

In addition, they are used in logistics and maintenance planning to estimate frequency of maintenance and part replacement. These estimates often determine major life cycle cost elements and should be carefully applied in life cycle cost and comparative studies.

In order to deliver meaningful results, the analysis should consider all possible contributions to the dependability of a system: hardware, software, as well as human factors and organizational aspects.

DEPENDABILITY MANAGEMENT –

Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

1 Scope

This part of IEC 60300 gives a general overview of commonly used dependability analysis techniques. It describes the usual methodologies, their advantages and disadvantages, data input and other conditions for using various techniques.

This standard is an introduction to selected methodologies and is intended to provide the necessary information for choosing the most appropriate analysis methods.

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 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-3-2:1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*

IEC 60300-3-4:1996, *Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements*

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10:2001, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60706-1:1982, *Guide on maintainability of equipment – Part 1: Sections One, Two and Three – Introduction, requirements and maintainability programme*

IEC 60706-2:1990, *Guide on maintainability of equipment – Part 2: Section Five – Maintainability studies during the design phase*

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61078:1991, *Analysis techniques for dependability – Reliability block diagram method*

IEC 61165:1995, *Application of Markov techniques*

IEC 61709:1996, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61882:2001, *Hazard and operability studies (HAZOP studies) – Application guide*

ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*

3 Definitions

For the purposes of this part of IEC 60300, the definitions given in IEC 60050(191), some of which are reproduced below, together with the following definitions, apply.

3.1
item, entity
any part, component, device, sub-system, functional unit, equipment or system that can be individually considered

NOTE An item may consist of hardware, software or both, and may also in particular cases, include people.

[IEV 191-01-01]

3.2
system
set of interrelated or interacting elements

[ISO 9000, 2000]

NOTE 1 In the context of dependability, a system will have

a) a defined purpose expressed in terms of required functions, and

b) stated conditions of operation/use.

NOTE 2 The concept of a system is hierarchical.

3.3
component
item on the lowest level considered in the analysis

3.4
allocation
procedure applied during the design of an item intended to apportion the requirements for performance measures for an item to its sub-items according to given criteria

3.5
failure
termination of the ability of an item to perform a required function

NOTE 1 After failure the item has a fault.

NOTE 2 ‘Failure’ is an event, as distinguished from ‘fault’, which is a state.

[IEV 191-04-01]

3.6
fault
state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEV 191-05-01]

4 Basic dependability analysis procedure

4.1 General procedure

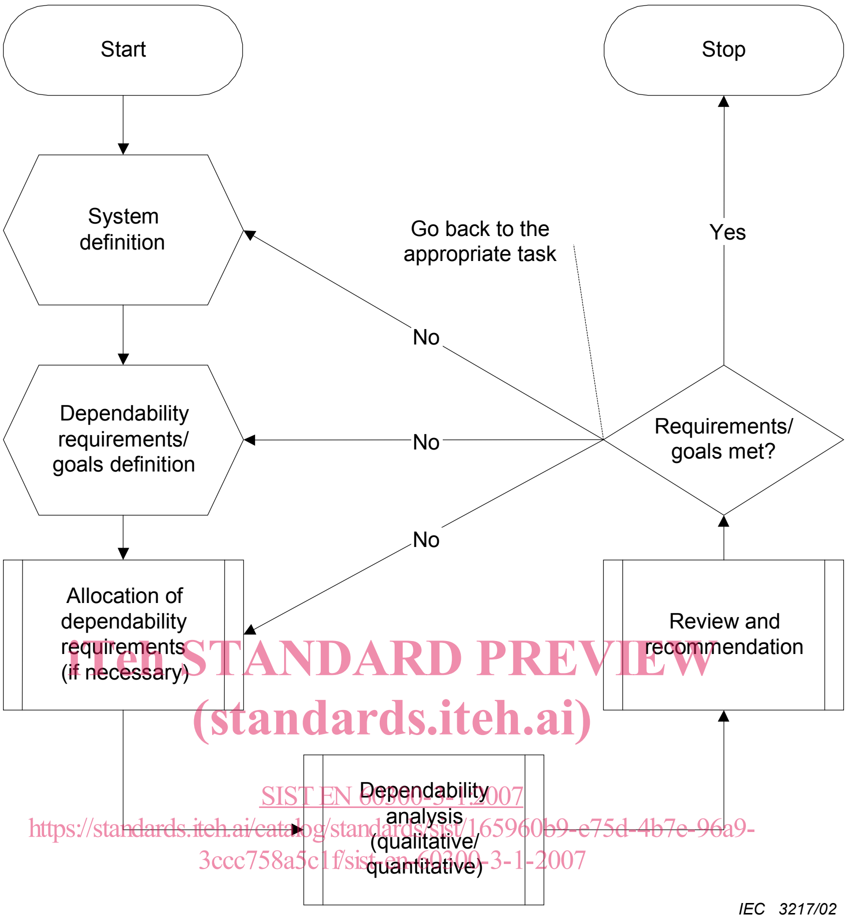
Start
Stop
System definition
Go back to the appropriate task
Yes
No
Dependability requirements/ goals definition
No
Requirements/ goals met?
No
Allocation of dependability requirements (if necessary)
Review and recommendation
Dependability analysis (qualitative/ quantitative)
IEC 3217/02

Figure 1 – General dependability analysis procedure

A general dependability analysis procedure consists of the following tasks (as applicable):

a) System definition

Define the system to be analysed, its modes of operation, the functional relationships to its environment including interfaces or processes. Generally the system definition is an input from the system engineering process.

b) Dependability requirements/goals definition

List all system reliability and availability requirements or goals, characteristics and features, together with environmental and operating conditions, as well as maintenance requirements. Define system failure, failure criteria and conditions based on system functional specification, expected duration of operation and operating environment (mission profile and mission time). IEC 60300-3-4 should be used as guidance.

c) Allocation of dependability requirements

Allocate system dependability requirements or goals to the various sub-systems in the early design phase when necessary.

d) Dependability analysis

Analyse the system usually on the basis of the dependability techniques and relevant performance data.

1) Qualitative analysis
   - Analyse the functional system structure.
   - Determine system and component fault modes, failure mechanisms, causes, effects and consequences of failures.
   - Determine degradation mechanism that may cause failures.
   - Analyse failure/fault paths.
   - Analyse maintainability with respect to time, problem isolation method, and repair method.
   - Determine the adequacy of the diagnostics provided to detect faults.
   - Analyse possibility for fault avoidance.
   - Determine possible maintenance and repair strategies, etc.
2) Quantitative analysis
   - Develop reliability and/or availability models.
   - Define numerical reference data to be used.
   - Perform numerical dependability evaluations.
   - Perform component criticality and sensitivity analyses as required.

e) Review and recommendations

Analyse whether the dependability requirements/goals are met and if alternative designs may cost effectively enhance dependability. Activities may include the following tasks (as appropriate):

- Evaluate improvement of system dependability as a result of design and manufacture improvement (e.g. redundancy, stress reduction, improvement of maintenance strategies, test systems, technological processes and quality control system).

NOTE 1 The inherent dependability performance measures can be improved only by design. When poor measured values are observed due to bad manufacturing processing, from the operating point of view, observed dependability performance measures can be enhanced by improving the manufacturing process.

- Review system design, determine weaknesses and critical fault modes and components.
- Consider system interface problems, fail-safe features and mechanisms, etc.
- Develop alternative ways for improving dependability, e.g. redundancy, performance monitoring, fault detection, system reconfiguration techniques, maintenance procedures, component replaceability, repair procedures.
- Perform trade-off studies evaluating the cost and complexity of alternative designs.
- Evaluate the effect of manufacturing process capability.
- Evaluate the results and compare with requirements.

NOTE 2 The general procedure summarizes, from an engineering point of view, the specific dependability programme elements from IEC 60300-2, which are applicable for dependability analysis: dependability specifications, analysis of use environment, reliability engineering, maintainability engineering, human factors, reliability modelling and simulation, design analysis and product evaluation, cause-effect impact and risk analysis, prediction and trade-off analysis.

4.2 Dependability analysis methods

The methods presented in this standard fall into two main categories:

- methods which are primarily used for dependability analysis;
- general engineering methods which support dependability analysis or add value to design for dependability.

The usability of the dependability analysis methods within the general dependability analysis tasks of the general analysis procedure is given in Table 1. Table 2 gives more detailed characteristics. The methods are explained briefly in Annex A.

Table 1 – Use of methods for general dependability analysis tasks

Analysis method	Allocation of dependability requirements/goals	Qualitative analysis	Quantitative analysis	Review and recommen-dations	Annex
Failure rate prediction	Applicable for serial systems without redundancy	Possible for maintenance strategy analysis	Calculation of failure rates and MTTF for electronic components and equipment	Supporting	A.1.1
Fault tree analysis	Applicable, if system behaviour is not heavily time- or sequence-dependent	Fault combinations	Calculation of system reliability, availability and relative contributions of subsystems to system unavailability	Applicable	A.1.2
Event tree analysis	Possible	Failure sequences	Calculation of system failure rates	Applicable	A.1.3
Reliability block diagram analysis	Applicable, for systems where independent blocks can be assumed	Success paths	Calculation of system reliability, availability	Applicable	A.1.4
Markov analysis	Applicable	Failure sequences	Calculation of system reliability, availability	Applicable	A.1.5
Petri net analysis	Applicable	Failure sequences	To provide the system description for Markov analysis	Applicable	A.1.6
Failure modes and effects (and criticality) analysis; FME(C)A	Applicable for systems where independent single failure is predominant	Effects of failures	Calculation of system failure rates (and criticality)	Applicable	A.1.7
HAZOP studies	Supporting	Causes and consequences of deviations	Not applicable	Supporting	A.1.8
Human reliability analysis	Supporting	Impact of human performance on system operation	Calculation of error probabilities for human tasks	Supporting	A.1.9
Stress-strength analysis	Not applicable	Usable as a means of fault avoidance	Calculation of reliability for (electro) mechanical components	Supporting	A.1.10
Truth table (structure function analysis)	Not applicable	Possible	Calculation of system reliability, availability	Supporting	A.1.11
Statistical reliability methods	Possible	Impact of faults	Quantitative estimation of reliability with uncertainties	Supporting	A.1.12

NOTE The particular wording in the table is used as follows:

'Applicable' means that the method is generally applicable and recommended for the task (possibly with the mentioned restrictions).

'Possible' means that the method may be used for this task but has certain drawbacks compared to other methods.

'Supporting' means that the method is generally applicable for a certain part of the task but not as a stand-alone method for the complete task.

'Not applicable' means that the method cannot be used for this task.