

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
300-3-1**

Première édition
First edition
1991-11

Gestion de la sûreté de fonctionnement

Partie 3: Guide d'application

Section 1 : Techniques d'analyse de la sûreté
de fonctionnement: Guide méthodologique

Dependability management

Part 3: Application guide

Section 1: Analysis techniques for dependability:
Guide on methodology



Numéro de référence
Reference number
CEI/IEC 300-3-1: 1991

AVA Documents
Document Sharing Hub

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles auprès du Bureau Central de la CEI.

Les renseignements relatifs à ces révisions, à l'établissement des éditions révisées et aux amendements peuvent être obtenus auprès des Comités nationaux de la CEI et dans les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
Publié annuellement
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 50: *Vocabulaire Electrotechnique International* (VEI), qui se présente sous forme de chapitres séparés traitant chacun d'un sujet défini. Des détails complets sur le VEI peuvent être obtenus sur demande. Voir également le dictionnaire multilingue de la CEI.

Les termes et définitions figurant dans la présente publication ont été soit tirés du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera:

- la CEI 27: *Symboles littéraux à utiliser en électro-technique;*
- la CEI 417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles;*
- la CEI 617: *Symboles graphiques pour schémas;*

et pour les appareils électromédicaux,

- la CEI 878: *Symboles graphiques pour équipements électriques en pratique médicale.*

Les symboles et signes contenus dans la présente publication ont été soit tirés de la CEI 27, de la CEI 417, de la CEI 617 et/ou de la CEI 878, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même comité d'études

L'attention du lecteur est attirée sur les listes figurant à la fin de cette publication, qui énumèrent les publications de la CEI préparées par le comité d'études qui a établi la présente publication.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available from the IEC Central Office.

Information on the revision work, the issue of revised editions and amendments may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
Published yearly
- **Catalogue of IEC publications**
Published yearly with regular updates

Terminology

For general terminology, readers are referred to IEC 50: *International Electrotechnical Vocabulary* (IEV), which is issued in the form of separate chapters each dealing with a specific field. Full details of the IEV will be supplied on request. See also the IEC Multilingual Dictionary.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications:

- IEC 27: *Letter symbols to be used in electrical technology;*
- IEC 417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets;*
- IEC 617: *Graphical symbols for diagrams;*

and for medical electrical equipment,

- IEC 878: *Graphical symbols for electromedical equipment in medical practice.*

The symbols and signs contained in the present publication have either been taken from IEC 27, IEC 417, IEC 617 and/or IEC 878, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same technical committee

The attention of readers is drawn to the end pages of this publication which list the IEC publications issued by the technical committee which has prepared the present publication.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
300-3-1**

Première édition
First edition
1991– 11

Gestion de la sûreté de fonctionnement

Partie 3: Guide d'application

Section 1: Techniques d'analyse de la sûreté
de fonctionnement: Guide méthodologique

Dependability management

Part 3: Application guide

Section 1: Analysis techniques for dependability:
Guide on methodology

© CEI 1991 Droits de reproduction réservés — Copyright — all rights reserved

Aucune partie de cette publication ne peut être reproduite ni
utilisée sous quelque forme que ce soit et par aucun pro-
cédé, électronique ou mécanique, y compris la photocopie et
les microfilms, sans l'accord écrit de l'éditeur.

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 the publisher.

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembe Genève, Suisse



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

R

Pour prix, voir catalogue en vigueur
For price, see current catalogue



Documents

Document Sharing Hub

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	6
 Articles	
1 Domaine d'application	8
2 Références normatives	8
3 Définitions	8
4 Généralités	10
5 Analyse de la sûreté de fonctionnement des systèmes: démarche de base	10
5.1 Procédure générale	10
5.2 Analyse de la structure fonctionnelle	16
5.3 Analyse déductive	16
5.4 Analyse inductive	16
5.5 Analyse et examen de la maintenance et des réparations	18
6 Caractéristiques de diverses méthodes d'analyse de la sûreté de fonctionnement	18
6.1 Choix de la méthode appropriée d'analyse	18
6.2 Description résumée des méthodes d'analyse	18
6.3 Explications pour le tableau 2	22
6.4 Avantages et inconvénients des méthodes	30
 Annexe	
A - Autre référence	38

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	7
Clause	
1 Scope	9
2 Normative references	9
3 Definitions	9
4 General	11
5 Basic approach to system dependability analysis	11
5.1 General procedure	11
5.2 Analysis of functional structure	17
5.3 Deductive analysis	17
5.4 Inductive analysis	17
5.5 Maintenance and repair analysis and considerations	19
6 Characteristics of various dependability analysis methods	19
6.1 Selecting the appropriate analysis method	19
6.2 Short descriptions of analysis methods	19
6.3 Explanations to table 2	23
6.4 Advantages and disadvantages of methods	31
Annex	
A - Other reference	39

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT

Partie 3: Guide d'application

Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

AVANT-PROPOS

- 1) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.
- 2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.
- 3) Dans le but d'encourager l'unification internationale, la CEI exprime le vœu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

La présente Norme internationale a été établie par le Comité d'Etudes n° 56 de la CEI: Sûreté de fonctionnement

Le texte de cette norme est issu des documents suivants:

Règle des Six Mois	Rapport de vote
56(BC)138	56(BC)146

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT

Part 3: Application guide

Section 1: Analysis techniques for dependability: Guide on methodology

FOREWORD

- 1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.
- 2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.
- 3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

This International Standard has been prepared by IEC Technical Committee No. 56: Dependability.

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

Six Months' Rule	Report on Voting
56(CO)138	56(CO)146

Full information on the voting for the approval of this standard can be found in the Voting Report indicated in the above table.

Annex A is for information only.

INTRODUCTION

Les techniques d'analyse de la sûreté de fonctionnement servent à examiner et prévoir les caractéristiques de fiabilité, de disponibilité, de maintenabilité et de sécurité d'un système.

Les analyses de sûreté de fonctionnement sont surtout effectuées pendant les phases de concept et de définition, de conception et de développement, d'exploitation et de maintenance, à des niveaux différents et avec plus ou moins de détails afin d'évaluer et de déterminer les caractéristiques de sûreté de fonctionnement d'un système ou d'une installation. Elles permettent aussi de confronter les résultats de l'analyse aux exigences prescrites.

Withdrawn

INTRODUCTION

Dependability analysis techniques are used for the review and prediction of the reliability, availability, maintainability and safety measures of a system.

Dependability analyses are conducted mainly 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 and determine the dependability measures of a system or an installation. They are also used to compare the results of the analysis with specified requirements.

Withdrawn

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT

Partie 3: Guide d'application

Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

1 Domaine d'application

La présente Norme internationale présente une vue générale des procédures d'analyse de la sûreté de fonctionnement communément employées. Pour ces différentes techniques, elle décrit la méthodologie habituelle, les avantages et les inconvénients, les données d'entrées ainsi que d'autres spécifications.

Ce guide est une introduction à la méthodologie existante. Il est destiné à fournir à l'analyste les informations qui lui sont nécessaires pour choisir les méthodes d'analyse les plus appropriées au système. Des normes disponibles de la CEI donnant des détails sur des méthodes sont indiquées dans le tableau 2.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions variables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer l'édition la plus récente des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 50(191): 1990, *Vocabulaire Electrotechnique International (VEI), Chapitre 191: Sûreté de fonctionnement et qualité de service.*

CEI 812: 1985, *Techniques d'analyse de la fiabilité des systèmes – Procédures d'analyse des modes de défaillance et de leurs effets (AMDE).*

CEI 1025: 1990, *Analyse par arbre de panne (AAP).*

CEI 1078: 1991, *Technique d'analyse de la sûreté de fonctionnement - Méthode du diagramme de fiabilité.*

3 Définitions

Les termes et les définitions sont conformes au Chapitre 191 du Vocabulaire Electro-technique International (VEI).

En outre, les définitions suivantes sont applicables pour cette norme:

3.1 système: Entité du plus haut niveau considéré dans l'analyse.

3.2 composant: Entité du plus bas niveau considéré dans l'analyse.

3.3 allocation: Procédure mise en oeuvre pendant la conception d'une entité en vue de répartir les exigences imposées aux caractéristiques relatives à cette entité entre ses sous-entités, conformément à des critères donnés.

NOTE - «Système» peut être remplacé par «sous-système», etc., le cas échéant.

DEPENDABILITY MANAGEMENT

Part 3: Application guide

Section 1: Analysis techniques for dependability: Guide on methodology

1 Scope

This International Standard gives a general overview of commonly used dependability analysis procedures. It describes the usual methodologies, the advantages and disadvantages, data input and other requirements for the various techniques.

This guide is an introduction to the available methodology and is intended to provide the analyst with the necessary information in order to choose the analysis method most appropriate to the system. Available IEC standards, providing details, are indicated in table 2.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent edition of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191): 1990, *International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service*.

IEC 812: 1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*.

IEC 1025: 1990, *Fault tree analysis (FTA)*.

IEC 1078: 1991, *Analysis techniques for dependability - Reliability block diagram method*.

3 Definitions

Terms and definitions are in accordance with Chapter 191 of the International Electrotechnical Vocabulary.

In addition, the following definitions are applicable for this standard:

3.1 system: Item on the highest level considered in the analysis.

3.2 component: Item on the lowest level considered in the analysis.

3.3 allocation: A procedure applied during the design of an item intended to apportion the requirements for performance measures for an item to its subitems according to given criteria.

NOTE - "System" may be replaced by "sub-system", etc., as applicable.

4 Généralités

Les méthodes d'analyse permettent l'évaluation de caractéristiques qualitatives et l'estimation de caractéristiques quantitatives (par exemple, taux de défaillance, MTTF, MTBF, fiabilité, disponibilité en régime établi) qui décrivent le fonctionnement prévu à long terme d'un système. Afin de réaliser une analyse de système qui soit systématique et reproductible, il est important d'employer une procédure cohérente.

Toutefois, il n'existe pas de méthode d'analyse de la sûreté de fonctionnement qui, seule, soit suffisamment exhaustive et souple pour couvrir toutes les complexités possibles du modèle, indispensables à l'évaluation des caractéristiques de systèmes réels (matériel et logiciel, structure fonctionnelle complexe, diverses technologies, structures réparables et pouvant être entretenues, etc.). Diverses méthodes d'analyse complémentaires devront peut-être être appliquées pour parvenir à une analyse correcte de systèmes complexes ou à fonctions multiples.

5 Analyse de la sûreté de fonctionnement des systèmes: démarche de base

Les procédures spécifiques d'analyse sont données dans les normes décrivant chaque méthode d'analyse. On trouvera dans ce qui suit une description des procédures, démarches et exigences générales.

5.1 Procédure générale

La procédure comprend, selon le cas, les étapes suivantes:

Etape 1

Enumérer tous les impératifs et toutes les caractéristiques et propriétés concernant la fiabilité et la disponibilité des systèmes, les conditions ambiantes, les conditions de fonctionnement ainsi que les exigences relatives à l'entretien et aux réparations. Définir le système à analyser et inclure une description de tous les modes de fonctionnement du système et de toutes les relations fonctionnelles jusqu'à des niveaux plus élevés et jusqu'aux processus et systèmes à interface.

Etape 2

Définir la panne du système, les critères et les conditions de panne d'après les impératifs de fonctionnement du système, le fonctionnement attendu et le milieu dans lequel le système fonctionne. Il convient également de tenir compte des performances du logiciel.

Etape 3

Lorsque des résultats numériques sont nécessaires, il est recommandé de procéder à une allocation de la fiabilité en fonction d'une conception préliminaire (attribution à chaque sous-système d'une partie du taux de défaillance ou de l'indisponibilité totale autorisée du système).

4 General

The analysis methods allow the evaluation of qualitative characteristics and estimation of measures (e.g. failure rate, MTTF, MTBF, reliability, steady state availability) which describe the predicted long-term operating behaviour of a system. In order to perform a systematic and reproducible system analysis, use of a consistent procedure is essential.

However, no single dependability analysis method is sufficiently comprehensive and flexible to deal with all the possible model complexities required to evaluate the features of practical systems (hardware and software, complex functional structures, various technologies, repairable and maintainable structures, etc.). It may be necessary to consider several additional analysis methods to ensure proper treatment of complex or multi-functional systems.

5 Basic approach to system dependability analysis

Specific procedures for analysis are contained in the standards describing each analysis method. General procedures, approaches and requirements are described hereinafter.

5.1 General procedure

The procedure consists of the following steps (as applicable):

Step 1

List all system reliability and availability requirements, characteristics and features, together with environmental and operating conditions, and maintenance requirements. Define the system to be analyzed, its modes of operation, the functional relationships to higher levels and to interfacing systems or processes.

Step 2

Define system fault, fault criteria and conditions based on system functional requirements, expected operation and operating environment. Software performance should also be considered.

Step 3

When numerical results are required, it is recommended to carry out an allocation based on a preliminary design (assignment of a portion of the total permitted system failure rate or unavailability to each sub-system).

Etape 4

Analyse du système de la manière suivante:

4.1) Analyse qualitative (méthode déductive/inductive):

Analyser la structure fonctionnelle du système, rechercher les modes de panne du système/composants, les mécanismes de défaillance, les effets et les conséquences des défaillances, considérer la maintenabilité des entités, établir un modèle de fiabilité et/ou de disponibilité, mettre au point des stratégies de maintenance et de réparation, etc.

4.2) Analyse quantitative (analytique/simulation d'événements):

Rassembler ou identifier les données de fiabilité des composants (par exemple, taux de défaillance), construire un modèle mathématique de fiabilité et/ou de disponibilité, réaliser une estimation numérique des modèles mathématiques, effectuer une analyse de la criticité des composants et des analyses de sensibilité, estimer l'amélioration des performances du système réalisable grâce à la mise en place de sous-structures redondantes et de stratégies de maintenance, etc.

Etape 5

Evaluation des résultats. Comparer ceux-ci aux exigences ou à ceux qui résultent d'autres conceptions. Parmi les autres actions, on peut citer:

5.1) Examiner la conception du système, identifier les faiblesses, les déséquilibres, les modes de défaillance et les composants critiques/à haut risque, étudier les problèmes d'interface du système, les dispositifs et les mécanismes à sûreté intégrée, etc.;

5.2) Trouver des solutions de rechange pour améliorer la sûreté de fonctionnement (par exemple, attribution de redondance, surveillance des performances, détection des pannes, procédure de reconfiguration du système, maintenabilité, possibilité de remplacement et de réparation des composants).

5.3) Réaliser des études de coût/bénéfice et évaluer les coûts de conceptions différentes.

La relation entre la procédure générale d'analyse et les méthodes et procédures spécifiques est donnée dans le tableau 1 qui, toutefois, ne se veut pas exhaustif. Les méthodes sont explicitées ci-après de 5.2 à 5.5.