NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
300-3-9

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

Partie 3:
Guide d'application –
Section 9: Analyse du risque des systèmes technologiques

Dependability management –

Part 3:
Application guide –
Section 9: Risk analysis of technological systems

Numéro de référence
Reference number
CEI/IEC 300-3-9: 1995

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
300-3-9

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

Partie 3:
Guide d'application –
Section 9: Analyse du risque des systèmes technologiques

Dependability management –

Part 3:
Application guide –
Section 9: Risk analysis of technological systems

© CEI 1995 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 procédé, 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 Varembé Genève, Suisse

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE V

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

SOMMAIRE

Pages

AVANT-PROPOS 4

INTRODUCTION 4

Articles

1 Domaine d'application 8

2 Références normatives 8

3 Définitions 10

4 Notions d'analyse du risque 12

5 Processus d'analyse du risque 18

6 Audits 28

7 Méthodes d'analyse du risque 28

Annexe A – Méthodes utilisées pour analyse 48

CONTENTS

Page

FOREWORD 5

INTRODUCTION 5

Clause

1 Scope 9

2 Normative references 9

3 Definitions 11

4 Risk analysis concepts 13

5 Risk analysis process 19

6 Audits 29

7 Risk analysis methods 29

Annex A – Methods for analysis 49

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques

AVANT-PROPOS

1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant des questions techniques, représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales; ils sont publiés comme normes, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 300-3-9 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

DIS	Rapport de vote
56/447/FDIS	56/489/RVD

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 9: Risk analysis of technological systems

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 cooperation 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 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. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 300-3-9 has been prepared by IEC technical committee 56: Dependability.

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

DIS	Report on voting
56/447/FDIS	56/489/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.

Annexe A is for information only.

INTRODUCTION

Le processus de gestion des risques comporte de nombreux éléments différents, depuis l'identification initiale et l'analyse du risque, jusqu'à l'évaluation de son caractère tolérable et l'identification des options de réduction de risques potentiels, en passant par le choix, la mise en oeuvre et la surveillance de mesures appropriées de maîtrise et de réduction. Cela est illustré à la figure 1.

L'analyse du risque, qui fait l'objet de la présente section de la CEI 300-3, est un processus structuré qui identifie à la fois la probabilité et l'étendue des conséquences néfastes résultant d'une activité, d'une installation ou d'un système donné. Dans le cadre de la présente norme, les conséquences néfastes envisagées sont des préjudices physiques aux personnes, aux biens ou à l'environnement.

L'analyse du risque s'efforce de répondre à trois questions fondamentales:

Quel élément risque d'être affecté (par identification des dangers)?

Quelle est la probabilité d'occurrence de l'événement (par analyse des fréquences)?

Quelles sont les conséquences (par analyse des conséquences)?

La présente norme est destinée à refléter les bons usages actuels en matière de choix et d'utilisation des techniques d'analyse du risque et ne fait pas référence à des notions nouvelles ou en cours de développement qui n'ont pas atteint un niveau satisfaisant de consensus professionnel.

La présente norme est par nature générale de sorte qu'elle puisse servir de guide dans de nombreuses industries et pour différents types de systèmes. Il se peut que dans ces industries, il existe des normes plus spécifiques établissant les méthodologies et niveaux d'analyse recommandés pour des applications particulières. Si ces normes ont été élaborées en harmonie avec la présente norme, les normes spécifiques seront généralement suffisantes.

La présente norme couvre seulement la partie «analyse du risque» des activités plus larges d'évaluation et de gestion des risques qui peuvent faire l'objet de normes futures. Dans la mesure du possible, la présente norme se fonde sur les notions et la terminologie données dans les documents énumérés dans l'article 2 et dans d'autres normes. Dans de nombreux cas, ces documents ne sont pas totalement cohérents avec la présente norme ou s'appliquent principalement à une industrie particulière. Dans de tels cas, la présente norme peut utiliser l'une des approches/définitions disponibles ou en présenter une d'usage plus général.

INTRODUCTION

The process of risk management incorporates many different elements from the initial identification and analysis of risk, to the evaluation of its tolerability and identification of potential risk reduction options, through to the selection, implementation and monitoring of appropriate control and reduction measures. This is illustrated in figure 1.

Risk analysis, which is the subject of this section of IEC 300-3, is a structured process that identifies both the likelihood and extent of adverse consequences arising from a given activity, facility or system. Within the context of this standard, the adverse consequences of concern are physical harm to people, property or the environment.

Risk analysis attempts to answer three fundamental questions:

What can go wrong (by hazard identification)?

How likely is this to happen (by frequency analysis)?

What are the consequences (by consequence analysis)?

This standard is intended to reflect current good practices in selection and utilisation of the risk analysis techniques and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of systems. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of analysis for particular applications. If these standards are in harmony with this publication, the specific standards will generally be sufficient.

This standard only covers the risk analysis portion of the broader risk assessment and risk management activities. The latter may become the subject of future standards. To the extent possible, this standard has built on the concepts and terminology given in the documents listed in clause 2 and other standards. There are numerous instances where these documents are not entirely consistent or where they principally apply to one industry alone. In these cases, this standard may use one of the approaches/definitions available or may present a more general one.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques

1 Domaine d'application

La présente section de la CEI 300-3 fournit des lignes directrices permettant de choisir et de mettre en oeuvre des techniques d'analyse du risque, principalement pour l'évaluation du risque de systèmes technologiques. L'objectif de la présente norme est d'assurer la qualité et la cohérence de planification et d'exécution d'analyse des risques, ainsi que de présenter les résultats et les conclusions correspondants.

La présente norme contient des lignes directrices d'analyse des risques, présentées comme suit: notions d'analyse du risque, processus d'analyse du risque et méthodes d'analyse du risque.

La présente section de la CEI 300-3 est applicable en tant que:

- ligne directrice pour la planification, l'exécution et la documentation des analyses du risque;
- base de spécification des prescriptions de qualité pour mener les analyses du risque (cet élément est d'autant plus important lorsqu'il s'agit de traiter avec des consultants externes);
- base d'évaluation des analyses du risque après achèvement.

L'analyse du risque effectuée conformément à la présente norme constitue une donnée d'entrée pour les activités de gestion du risque (voir figure 1).

NOTE – La présente norme ne fournit pas de critères spécifiques d'identification du besoin d'analyse du risque et ne spécifie pas le type de méthode d'analyse du risque qui est requis pour une situation donnée. Elle ne donne pas non plus de principes directeurs détaillés pour des dangers spécifiques et ne comporte pas d'éléments relatifs aux assurances, à des aspects actuariels, légaux ou financiers.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente section de la CEI 300-3. 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 section de la CEI 300-3 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes 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 300-2, *Gestion de la sûreté de fonctionnement – Partie 2: Eléments et tâches du programme de sûreté de fonctionnement*

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

DEPENDABILITY MANAGEMENT –

Part 3: Application guide – Section 9: Risk analysis of technological systems

1 Scope

This section of IEC 300-3 provides guidelines for selecting and implementing risk analysis techniques, primarily for risk assessment of technological systems. The objective of this standard is to ensure quality and consistency in the planning and execution of risk analyses and the presentation of results and conclusions.

This standard contains guidelines for risk analysis, presented as follows: risk analysis concepts, risk analysis process, risk analysis methods.

This section of IEC 300-3 is applicable as:

- a guideline for planning, executing and documenting risk analyses;
- a basis for specifying quality requirements for risk analysis (this can be particularly important when dealing with external consultants);
- a basis for evaluating risk analyses after completion.

Risk analysis carried out to this standard provides an input to risk management activities (see figure 1).

NOTE – This standard does not provide specific criteria for identifying the need for risk analysis, or specify the type of risk analysis method that is required for a given situation. Nor does it offer detailed guidelines for specific hazards or include insurance, actuarial, legal, or financial interests.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 300-3. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this section of IEC 300-3 are encouraged to investigate the possibility of applying the most recent editions 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 (IEV) – Chapter 191: Dependability and quality of service*

IEC 300-2, *Dependability management – Part 2: Dependability programme elements and tasks*

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