

**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

AVA Documents
Document Sharing Hub

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)*

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

CEI 1078: 1991, *Techniques d'analyse de la sûreté de fonctionnement – Méthode du diagramme de fiabilité*

3 Définitions

Pour les besoins de la présente section de la CEI 300-3, les termes et définitions de la CEI 50(191) sont applicables. En outre, les termes et définitions suivants s'appliquent.

3.1 préjudice*: Dommages physiques nuisibles à la santé, aux biens ou à l'environnement.

3.2 danger*: Source de préjudice potentiel ou situation comportant un préjudice potentiel.

3.3 événement dangereux: Événement qui peut être à l'origine d'un préjudice.

3.4 identification du danger: Processus de reconnaissance de l'existence d'un danger et de définition de ses caractéristiques.

3.5 risque*: Combinaison de la fréquence, ou de la probabilité, et des conséquences d'un événement dangereux spécifié.

NOTE – La notion de risque comporte toujours deux éléments: la probabilité (c'est-à-dire la fréquence) d'occurrence d'un événement dangereux et les conséquences de l'événement dangereux.

3.6 analyse du risque: Utilisation systématique des informations disponibles pour identifier des dangers et pour estimer le risque encouru par des individus ou des populations, des biens ou l'environnement. (Voir figure 1.)

NOTE – L'analyse du risque est quelquefois appelée analyse probabiliste de sécurité, analyse probabiliste de risque, analyse quantitative de sécurité et analyse quantitative du risque.

3.7 appréciation du risque: Processus global d'analyse du risque et d'évaluation du risque. (Voir figure 1.)

3.8 maîtrise du risque: Processus décisionnaire de gestion et/ou de réduction du risque, sa mise en oeuvre, son application et sa réévaluation éventuelle, en utilisant les résultats d'appréciation du risque comme donnée d'entrée.

3.9 estimation du risque: Processus utilisé pour obtenir une mesure du niveau des risques analysés. L'estimation du risque comprend les étapes suivantes: analyse de la fréquence, analyse des conséquences et leur intégration.

* Ces définitions diffèrent de celles données dans ISO/IEC Guide 51: 1990. Ce dernier est actuellement en phase de révision.

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

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

3 Definitions

For the purposes of this section of IEC 300-3, the terms and definitions of IEC 50(191) apply. In addition, the following terms and definitions apply:

3.1 harm*: Physical injury or damage to health, property or the environment.

3.2 hazard*: Source of potential harm or a situation with a potential for harm.

3.3 hazardous event: Event which can cause harm.

3.4 hazard identification: Process of recognizing that a hazard exists and defining its characteristics.

3.5 risk*: Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.

NOTE – The concept of risk always has two elements: the frequency or probability with which a hazardous event occurs and the consequences of the hazardous event.

3.6 risk analysis: Systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment. (See figure 1.)

NOTE – Risk analysis is also sometimes referred to as probabilistic safety analysis, probabilistic risk analysis, quantitative safety analysis and quantitative risk analysis.

3.7 risk assessment: Overall process of risk analysis and risk evaluation. (See figure 1.)

3.8 risk control: Process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using the results of risk assessment as one input.

3.9 risk estimation: Process used to produce a measure of the level of risks being analysed. Risk estimation consists of the following steps: frequency analysis, consequence analysis and their integration.

* These definitions deviate from those given in ISO/IEC Guide 51: 1990, which is currently under revision.

3.10 évaluation du risque: Processus par lequel on juge le caractère tolérable du risque sur la base de l'analyse du risque et en tenant compte de facteurs tels que les aspects socio-économiques et environnementaux.

3.11 gestion du risque: Application systématique des politiques de gestion, des procédures et des usages aux tâches d'analyse, d'évaluation et de maîtrise du risque. (Voir figure 1.)

3.12 système: Entité composée, quel que soit son niveau de complexité, de personnel, de procédures, de matériaux, d'outils, d'équipements, d'installations et de logiciels. Les éléments de cette entité composée sont utilisés ensemble dans l'environnement opérationnel ou de soutien prévu pour exécuter une tâche donnée ou atteindre un objectif spécifique.

4 Notions d'analyse du risque

4.1 Objectif et notions fondamentales de l'analyse du risque

Le risque est présent dans toute activité humaine; il peut concerner la santé et la sécurité (lorsqu'il implique, par exemple, des effets sanitaires immédiats et à long terme d'exposition à des produits chimiques toxiques) ou l'économie (lorsqu'il entraîne, par exemple, la destruction des équipements et la perte de la production dues à des incendies, des explosions ou autres incidents) ou affecter l'environnement. L'objectif de la gestion des risques est de maîtriser, prévenir ou réduire les pertes de vie, les maladies, ou les blessures, les dommages aux biens et les pertes qui en résultent, ainsi que l'impact sur l'environnement.

Les risques doivent être analysés afin de pouvoir les gérer de manière efficace. L'analyse du risque est un outil utile pour:

- a) identifier les risques et les solutions envisageables;
- b) fournir des informations objectives pour la prise de décisions;
- c) satisfaire à des exigences réglementaires.

Les résultats d'une analyse du risque peuvent être utilisés par un décideur pour lui permettre de juger du caractère tolérable du risque et l'aider à choisir entre des mesures de réduction du risque potentiel ou de prévention du risque. Du point de vue du décideur, quelques-uns des principaux avantages de l'analyse du risque sont:

- a) l'identification systématique des dangers potentiels;
- b) l'identification systématique des modes de défaillance potentiels;
- c) les relevés quantitatifs ou la classification du risque;
- d) l'évaluation des éventuelles modifications permettant de réduire le risque ou d'obtenir de meilleurs niveaux de sûreté de fonctionnement;
- e) l'identification des principaux facteurs contribuant au risque ainsi que des maillons faibles d'un système;
- f) la meilleure compréhension du système et de son installation;
- g) la comparaison des risques avec ceux d'autres systèmes ou technologies;
- h) l'identification et la communication des risques et incertitudes;

3.10 risk evaluation: Process in which judgements are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects.

3.11 risk management: Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. (See figure 1.)

3.12 system: Composite entity, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific objective.

4 Risk analysis concepts

4.1 *Objective and basic concepts of risk analysis*

Risk is present in all human activity; it can be health and safety related (involving, for example, both immediate and long-term health effects of exposure to toxic chemicals), economic (resulting in, for example, destruction of equipment and lost production due to fires, explosions or other accidents) or affect the environment. The objective of risk management is to control, prevent or reduce loss of life, illness, or injury, damage to property and consequential loss, and environmental impact.

Before risk can be effectively managed, it should be analysed. The analysis of risk is a useful tool for:

- a) identifying risks and approaches to their solution;
- b) providing objective information for decision making;
- c) meeting regulatory requirements.

The results of a risk analysis can be used by a decision-maker to help judge the tolerability of risk and aid in choosing between potential risk-reduction or risk avoidance measures. From the decision-maker's perspective some of the principal benefits of risk analysis include:

- a) systematic identification of potential hazards;
- b) systematic identification of potential failure modes;
- c) quantitative risk statements or ranking;
- d) evaluation of possible modifications to reduce risk or achieve better dependability levels;
- e) identification of the important contributors to risk and weak links in a system;
- f) better understanding of the system and its installation;
- g) comparison of risks to those of alternative systems or technologies;
- h) identification and communication of risks and uncertainties;

- i) l'aide à l'établissement des priorités pour améliorer la santé et la sécurité;
- j) la base de rationalisation de la maintenance préventive et de contrôle;
- k) l'enquête post-accident et la prévention;
- l) le choix entre différentes solutions telles que des mesures et des technologies différentes de réduction du risque.

Tous ces éléments jouent un rôle important dans une gestion efficace du risque, qu'il s'agisse d'améliorer les conditions de santé et de sécurité, de prévenir les pertes économiques, ou de se conformer à des réglementations gouvernementales.

L'analyse du risque nécessite souvent une approche multidisciplinaire, étant donné qu'elle peut couvrir plusieurs domaines spécialisés tels que:

- a) l'analyse des systèmes;
- b) la probabilité et les statistiques;
- c) le génie chimique, mécanique, électrique, structurel ou nucléaire;
- d) les sciences physiques, chimiques ou biologiques;
- e) les sciences médicales, y compris la toxicologie et l'épidémiologie;
- f) les sciences sociales, y compris l'économie, la psychologie et la sociologie;
- g) les facteurs humains, l'ergonomie et la gestion.

4.2 *Gestion et classification du risque*

L'analyse du risque fait partie du processus d'appréciation et de gestion du risque tel qu'illustré à la figure 1, et comprend la définition du domaine d'application, l'identification du danger et l'estimation du risque.

Il est admis de grouper les dangers en quatre catégories générales, notamment:

- a) les dangers naturels (inondations, tremblements de terre, tornades, foudre, etc.);
- b) les dangers technologiques (installations industrielles, structures, systèmes de transport, produits de consommation, pesticides, herbicides, produits pharmaceutiques, etc.);
- c) les dangers sociaux (attaque, guerre, sabotage, maladie contagieuse, etc.);
- d) les dangers liés au style de vie (abus de drogue, d'alcool, de tabac, etc.).

De toute évidence, ces groupes ne sont pas mutuellement exclusifs, et il est souvent nécessaire, lors de l'analyse des dangers technologiques, de tenir compte de l'influence des facteurs d'autres catégories (en particulier, les dangers naturels) et d'autres systèmes, comme faisant partie de l'analyse du risque.

Il est possible également de classer l'analyse du risque selon le type de conséquences étudié, comme par exemple:

- a) le risque individuel (impact sur les membres individuels du grand public);
- b) le risque professionnel (impact sur les travailleurs);
- c) les risques sociaux (impact global sur le grand public);
- d) le dommage aux biens et les pertes économiques (interruptions de l'activité, pénalités, etc.);
- e) les risques environnementaux (impact sur la terre, l'air, l'eau, la flore, la faune et l'héritage culturel).

- i) help in establishing priorities for improving health and safety;
- j) a basis for preventive maintenance and inspection to be rationalised;
- k) post-accident investigation and prevention;
- l) selection between alternatives such as different risk-reduction measures and technologies.

All these play an important role in effective risk management, whether the objective is improving conditions related to health and safety, prevention of economic loss, or compliance with government regulations.

Risk analysis often requires a multidisciplinary approach, since it may cover such areas of expertise as:

- a) systems analysis;
- b) probability and statistics;
- c) chemical, mechanical, electrical, structural or nuclear engineering;
- d) physical, chemical, or biological sciences;
- e) health sciences, including toxicology and epidemiology;
- f) social sciences, including economics, psychology, and sociology;
- g) human factors, ergonomics and management science.

4.2 Risk management and risk categorization

Risk analysis is a part of the risk assessment and management process as illustrated in figure 1 and consists of scope definition, hazard identification, and risk estimation.

Hazards may be grouped into four general categories, namely:

- a) natural hazards (floods, earthquakes, tornadoes, lightning, etc.);
- b) technological hazards (industrial facilities, structures, transportation systems, consumer products, pesticides, herbicides, pharmaceuticals, etc.);
- c) social hazards (assault, war, sabotage, communicable disease, etc.);
- d) lifestyle hazards (drug abuse, alcohol, smoking, etc.).

These groups are clearly not mutually exclusive, and in analysing technological hazards it is often necessary to consider the influence of factors from other categories (particularly natural hazards) and other systems, as part of the risk analysis.

Risk can also be categorized by the nature of the consequences that are being investigated, for example:

- a) individual (impact on individual members of the general public);
- b) occupational (impact on workers);
- c) societal (overall impact on the general public);
- d) property damage and economic losses (business interruptions, penalties, etc.);
- e) environmental (impact on land, air, water, flora, fauna and cultural heritage).

L'objectif global de l'analyse du risque est de fournir un fondement rationnel permettant de prendre des décisions relatives au risque. Ces décisions peuvent être prises dans le cadre d'un processus plus large de gestion du risque, en comparant les résultats d'analyse du risque aux critères de risque tolérable. Dans de nombreuses situations, il sera nécessaire d'apprécier les avantages au cas par cas, afin de prendre une décision pondérée. Le sujet d'ensemble des critères de risque tolérable est très complexe et implique des considérations sociales, économiques et politiques et, par conséquent, ne fait pas partie du domaine d'application de la présente norme.

4.3 *Application de l'analyse du risque au cours des phases du cycle de vie*

Certains objectifs spécifiques de l'analyse du risque, relatifs aux diverses phases du cycle de vie (voir la CEI 300-2) de systèmes, installations ou produits dangereux sont énumérés ci-dessous.

- a) Phases de concept et définition/de conception et développement:
 - 1) identifier les principaux éléments qui contribuent au risque ainsi que les facteurs significatifs impliqués;
 - 2) fournir une donnée d'entrée au processus de conception et estimer l'adéquation de la conception globale;
 - 3) identifier et évaluer les mesures de sécurité possibles au niveau de la conception;
 - 4) fournir des données d'entrée pour l'estimation du caractère acceptable des installations, activités ou systèmes potentiellement dangereux proposés;
 - 5) fournir des informations permettant d'aider au développement de procédures pour les conditions normales et d'urgence;
 - 6) évaluer le risque en termes de prescriptions réglementaires et autres;
 - 7) évaluer d'autres alternatives de conception.
- b) Phases de fabrication, d'installation, d'exploitation et de maintenance:
 - 1) surveiller et évaluer l'expérience acquise afin de comparer le niveau de performance réel aux prescriptions pertinentes;
 - 2) fournir une donnée d'entrée pour optimiser les procédures de fonctionnement normal, de maintenance/contrôle et d'urgence;
 - 3) mettre à jour les informations relatives aux principaux éléments qui contribuent au risque ainsi que les facteurs d'influence;
 - 4) fournir des informations sur l'importance du risque pour une prise de décision opérationnelle;
 - 5) évaluer les effets des modifications de structure, organisationnelles, d'usage et de procédures opérationnelles et de composants du système;
 - 6) cibler les efforts de formation.
- c) Phase de mise au rebut; mise hors service:
 - 1) évaluer le risque relatif aux activités de mise au rebut du système et s'assurer que les exigences correspondantes peuvent être remplies;
 - 2) fournir des données d'entrée aux procédures de mise au rebut.

The overall objective of risk analysis is to provide a rational foundation for decisions concerning risk. Such decisions can be made as part of the larger risk management process, through the comparison of results of risk analysis with tolerable risk criteria. In many situations there will be a need to assess benefits on a case-by-case basis, in order to make a balanced decision. The overall subject of tolerable risk criteria is very complex, involving social, economic and political considerations and as such is outside the scope of this standard.

4.3 *Application of risk analysis during life cycle phases*

Some specific objectives of risk analysis pertinent to various life cycle phases (see IEC 300-2) of hazardous systems, facilities, or products are listed below.

- a) Concept and definition/design and development phases:
 - 1) to identify major contributors to risk and significant factors involved;
 - 2) to provide input to the design process and to assess the adequacy of the overall design;
 - 3) to identify and evaluate possible safety measures in design;
 - 4) to provide input to the assessment of the acceptability of proposed potentially hazardous facilities, activities or systems;
 - 5) to provide information to assist in developing procedures for normal and emergency conditions;
 - 6) to evaluate risk with respect to regulatory and other requirements;
 - 7) to evaluate alternative design concepts.
- b) Manufacturing, installation, operation and maintenance phases:
 - 1) to monitor and evaluate experience for the purpose of comparing actual performance with relevant requirements;
 - 2) to provide input into the optimization of normal operating, maintenance/inspection and emergency procedures;
 - 3) to update information on major contributors to risk and influencing factors;
 - 4) to provide information on the significance of the risk for operational decision-making;
 - 5) to evaluate the effects of changes in organizational structure, operational practices and procedures, and system components;
 - 6) to focus training efforts.
- c) Disposal phase; decommissioning:
 - 1) to evaluate the risk related to system disposal activities and to ensure that relevant requirements can be met;
 - 2) to provide input into disposal procedures.

5 Processus d'analyse du risque

5.1 Aperçu

Pour améliorer l'efficacité et l'objectivité d'une analyse du risque ainsi que pour faciliter la comparaison avec d'autres analyses du risque, il convient de suivre un certain nombre de règles générales. Il convient d'effectuer le processus d'analyse du risque conformément à une séquence d'étapes définie:

- a) définition du domaine d'application;
- b) identification du danger et évaluation initiale des conséquences;
- c) estimation du risque;
- d) vérification;
- e) documentation;
- f) mise à jour de l'analyse.

Ce processus est illustré à la figure 2. L'estimation du risque comprend l'analyse de la fréquence et des conséquences. Bien que la documentation soit présentée comme un élément séparé, elle est développée à chaque étape du processus. Selon le domaine d'application, il est admis qu'il ne soit nécessaire de tenir compte que de certains éléments du processus illustré. Par exemple, dans certains cas, il peut ne pas être nécessaire d'aller au-delà d'une analyse initiale du danger et de ses conséquences.

Il est nécessaire de connaître parfaitement le système et les méthodes d'analyse utilisées. Si une analyse du risque est disponible pour un système similaire, elle peut être utilisée comme référence. Cependant, il convient de démontrer que les processus sont similaires ou que les modifications qui ont été effectuées n'introduiront pas de différences significatives des résultats. Il est bon de se fonder sur une évaluation systématique des modifications et de la manière dont elles peuvent influencer les divers dangers présents.

5.1.1 Personnel chargé de l'analyse du risque

Il est recommandé que les analystes du risque disposent de la compétence nécessaire pour entreprendre la tâche qui leur est confiée. De nombreux systèmes sont trop complexes pour être pleinement compris par une seule personne et un groupe d'analystes sera nécessaire pour effectuer le travail. Il convient que l'individu ou le groupe de travail soit familiarisé avec les méthodes utilisées pour l'analyse du risque et dispose de connaissances approfondies du sujet considéré. Le cas échéant, il est recommandé de prévoir et d'intégrer à l'analyse d'autres connaissances spécialisées et essentielles. Il est recommandé de spécifier et d'enregistrer le niveau de compétence du groupe de travail.

5.2 Définition du domaine d'application

Il convient de définir et de formuler le domaine d'application de l'analyse du risque afin de produire un plan d'analyse du risque dès le début du projet (voir la CEI 300-2). Il convient d'inclure, dans la définition du domaine d'application d'une analyse du risque, les étapes suivantes:

- a) description des raisons et/ou problèmes qui ont donné lieu à l'analyse du risque. Cela comprend:

5 Risk analysis process

5.1 Overview

General rules should be followed in order to both enhance the effectiveness and objectivity of a risk analysis, and to facilitate comparison with other risk analyses. The risk analysis process should be performed according to a defined sequence of steps:

- a) scope definition;
- b) hazard identification and initial consequence evaluation;
- c) risk estimation;
- d) verification;
- e) documentation;
- f) analysis update.

This process is shown in figure 2. Risk estimation incorporates frequency and consequence analysis. While documentation is shown as a separate item it is developed at each stage of the process. Depending on the area of application, only certain elements of the process shown may need to be considered. For example, in some instances it may not be necessary to go beyond an initial hazard and consequence analysis.

A thorough knowledge of the system and of the analysis methods used is required. If a risk analysis is available for a similar system, it may be used as a reference. However, it should be demonstrated that the processes are similar or that the changes that have been made will not introduce significant differences in results. This should be based on a systematic evaluation of the changes and the ways they can influence the various hazards present.

5.1.1 Risk analysis personnel

Risk analysts should be competent to undertake the task. Many systems are too complex to be fully understood by one person and a group of analysts will be required to carry out the work. The individual or working group should be familiar with the methods used for risk analysis and have a thorough knowledge of the subject under consideration. Other necessary specialised knowledge should be provided and integrated into the analysis as required. The expertise of the working group should be specified and recorded.

5.2 Scope definition

The scope of the risk analysis should be defined and documented to create a risk analysis plan at the start of the project (see IEC 300-2). Defining the scope of a risk analysis should involve the following steps:

- a) describe the reasons for and/or the problems that originated the risk analysis. This will involve:

- 1) formulation des objectifs de l'analyse du risque, sur la base des principales préoccupations identifiées;
 - 2) définition des critères de succès/de défaillance du système. La principale préoccupation peut être un certain résultat indésirable (par exemple: défaillance du système, émanation toxique) ou un état potentiellement dangereux.
- b) définition du système à analyser. Il convient que la définition comprenne:
- 1) une description générale du système;
 - 2) une définition des frontières et interfaces à la fois physiques et fonctionnelles avec les systèmes apparentés;
 - 3) une définition de l'environnement;
 - 4) une définition des flux d'énergie, de matières et d'informations au travers des limites;
 - 5) une définition des conditions de fonctionnement couverte par l'analyse du risque ainsi que d'éventuelles limites applicables.
- c) identification des sources permettant d'obtenir des détails des aspects techniques, environnementaux, légaux, organisationnels et humains concernant l'activité et le problème à analyser. Il convient, en particulier, de décrire également tout aspect sécuritaire;
- d) détermination des hypothèses et contraintes régissant l'analyse;
- e) identification des décisions à prendre, du résultat requis de l'étude ainsi que des décisionnaires.

Il est également recommandé que la tâche qui consiste à définir le domaine d'application de l'analyse comprenne une familiarisation approfondie avec le système analysé, en tant qu'activité planifiée. L'un des objectifs de cette familiarisation est de déterminer le lieu et la manière dont on peut accéder et intégrer des connaissances spécialisées à l'analyse.

5.3 Identification des dangers et évaluation initiale des conséquences

Il convient d'identifier les dangers qui engendrent un risque dans le système ainsi que les formes qu'il pourrait prendre. Il convient d'énoncer clairement les dangers connus (peut-être ceux qui sont apparus lors d'accidents précédents); pour identifier des dangers non reconnus précédemment, il est recommandé d'utiliser des méthodes formelles applicables à la situation spécifique (voir 7.3.1).

Il est recommandé d'effectuer une évaluation initiale de l'importance des dangers identifiés sur la base d'une analyse des conséquences, ainsi que d'un examen des causes premières. Il convient que cette évaluation détermine l'une des actions suivantes:

- a) mesures correctives prises à ce point pour éliminer ou réduire les dangers;
- b) arrêt de l'analyse à ce niveau parce que les dangers et leurs conséquences sont négligeables;
- c) poursuite de l'estimation du risque.

Il convient de documenter les hypothèses et résultats de l'évaluation initiale (voir 5.6).