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

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

IEC
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

CONTENTS

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:** Evénement 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 décisionnaire 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 décisionnaire, quelques-un 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).

1) formulating the objectives of the risk analysis based on the main concerns identified;

2) defining the criteria for success/failure of the system. The main concern may be some undesirable outcome (e.g. system failure, release of poisonous material) or it may be a condition which is potentially harmful.

b) define the system being analysed. The definition should include:

1) a general description of the system;

2) a definition of boundaries and interfaces with related systems both physical and functional;

3) a definition of the environment;

4) a definition of energy, materials and information flowing across boundaries;

5) a definition of the operating conditions covered by the risk analysis and any relevant limitations.

c) identify sources giving details of all the technical, environmental, legal, organizational, and human circumstances that are relevant to the activity and the problem being analysed. In particular any circumstances related to safety should also be described;

d) state the assumptions and constraints governing the analysis;

e) identify the decisions that have to be made, the required output from the study and the decision-makers.

The task of defining the scope of the analysis should also include a thorough familiarization with the analysed system as a planned activity. One of the objectives of familiarization is a determination of where and how specialised knowledge can be accessed and integrated into the analysis.

5.3 *Hazard identification and initial consequence evaluation*

The hazards which generate risk in the system should be identified together with the ways in which the hazards could be realized. Known hazards (perhaps having been realized in previous accidents) should be clearly stated. To identify hazards not previously recognized, formal methods covering the specific situation should be used (see 7.3.1).

An initial evaluation of the significance of the identified hazards should be carried out based on a consequence analysis, together with an examination of root causes. This should determine one of the following courses of action:

a) take corrective actions at this point to eliminate or reduce the hazards;

b) end the analysis here because the hazards or their consequences are insignificant;

c) proceed with risk estimation.

The initial assumptions and results should be documented (see 5.6).

5.4 *Estimation des risques*

Il est recommandé que l'estimation des risques examine les événements ou les circonstances initiales, la séquence d'événements concernée, d'éventuelles circonstances atténuantes ainsi que la nature et la fréquence des conséquences délétères possibles des dangers identifiés pour obtenir une mesure du niveau des risques à analyser. Les mesures prises pourraient concerner les risques encourus par les personnes, les biens ou l'environnement et comprendre une indication de l'incertitude associée aux estimations. Le processus est décrit ci-après dans les paragraphes 5.4.1, 5.4.2 et 5.4.3. Les méthodes d'analyse du risque sont décrites dans le tableau 1.

Les méthodes utilisées pour l'estimation des risques sont souvent quantitatives même si le degré de détails requis pour la préparation des estimations dépendra de l'application particulière (voir 7.2). Cependant, il est admis qu'une analyse quantitative complète n'est pas toujours possible du fait du manque d'informations sur le système ou l'activité analysé, le manque de données sur les défaillances, l'influence des facteurs humains, etc. Dans ces circonstances, une classification comparative, quantitative ou qualitative des risques par des spécialistes compétents dans leur domaine respectif peut encore être efficace. Lorsque la classification est qualitative, il convient d'expliquer clairement tous les termes utilisés et d'enregistrer la base de toutes classifications de fréquences et de conséquences. Lorsqu'une quantification complète a été réalisée, il est nécessaire d'admettre que les valeurs de risque calculées sont des estimatifs et il convient de s'assurer qu'il ne leur est pas attribué un niveau d'exactitude et de précision non cohérent par rapport à la précision des données et des méthodes analytiques utilisées.

Les éléments du processus d'estimation du risque sont communs pour tous les dangers. En premier lieu, les causes éventuelles du danger sont analysées pour déterminer sa fréquence d'occurrence, sa durée ainsi que sa nature (quantité, composition, caractéristiques d'émission/utilisation, etc.). S'il s'agit d'analyser une installation industrielle, l'analyse de la fréquence peut être une activité majeure. S'il s'agit d'analyser la réaction chimique d'une chaîne alimentaire, par exemple, l'analyse nécessaire est bien moindre. En second lieu, les conséquences de la réalisation du danger sont analysées. L'analyse des conséquences implique une estimation de la sévérité, de la ou des conséquences associées au danger. L'analyse peut également nécessiter une estimation de la probabilité du danger ayant engendré la ou les conséquences et, par conséquent, impliquer une analyse de la séquence d'événements par laquelle le danger peut avoir une ou des conséquences.

5.4.1 *Analyse de fréquence*

L'analyse de fréquence est utilisée pour estimer la probabilité de tout événement indésirable identifié lors de l'étape d'identification du danger. Trois approches sont communément utilisées pour estimer les fréquences d'événements (voir 7.3.2.1). Celles-ci sont:

a) l'utilisation de données historiques pertinentes;

b) la déduction des fréquences d'événements au moyen de techniques analytiques ou de simulations;

c) l'utilisation d'avis d'experts.

Toutes ces techniques peuvent être utilisées séparément ou ensemble. Les deux premières approches sont complémentaires; chacune d'entre elles présente des avantages là où l'autre a des faiblesses. Il convient, dans la mesure du possible, d'utiliser les deux techniques. De cette manière, elles peuvent être employées comme éléments indépendants qui se vérifient l'un l'autre et servir à améliorer la fiabilité des résultats. Lorsque ces techniques ne peuvent pas être utilisées ou ne sont pas suffisantes, il peut être nécessaire de compter sur un certain degré d'avis expert.

5.4 *Risk estimation*

Risk estimation should examine the initiating events or circumstances, the sequence of events that are of concern, any mitigating features and the nature and frequency of the possible deleterious consequences of the identified hazards to produce a measure of the level of the risks being analysed. The measures could address human, property or environmental risks and should include an indication of the uncertainty associated with the estimates. The process is outlined below in 5.4.1, 5.4.2 and 5.4.3. Risk analysis methods are described in table 1.

Methods used in estimating risks are often quantitative though the degree of detail required in preparing the estimates will depend upon the particular application (see 7.2). However, full quantitative analysis may not always be possible due to insufficient information about the system or activity being analysed, lack of failure data, influence of human factors, etc. In such circumstances a comparative quantitative or qualitative ranking of risks by specialists knowledgeable in their respective field may still be effective. In cases where the ranking is qualitative, there should be clear explanation of all the terms employed and the basis for all frequency and consequence classifications should be recorded. Where full quantification has been carried out it needs to be recognized that the risk values calculated are estimates and care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and analytical methods employed.

The elements of the risk estimation process are common for all hazards. Firstly, the possible causes of the hazard are analysed to determine its frequency of occurrence, its duration and also its nature (quantity, composition, release/use characteristics, etc.). If analysing an industrial facility, this frequency analysis may be a major activity. If analysing a food chain chemical, for example, much less analysis may be necessary. Secondly, the consequences of the hazard's realisation are analysed. This consequence analysis involves estimating the severity of the consequence(s) associated with the hazard. The analysis may also require estimation of the probability of the hazard causing the consequence(s) and may therefore involve analysis of the sequence of events by which the hazard can result in the consequence(s).

5.4.1 *Frequency analysis*

Frequency analysis is used to estimate the likelihood of each undesired event identified at the hazard identification stage. Three approaches are commonly employed to estimate event frequencies (see 7.3.2.1). They are:

a) to use relevant historical data;

b) to derive event frequencies using analytical or simulation techniques;

c) to use expert judgement.

All of these techniques may be used individually or jointly. The first two approaches are complementary; each has strengths where the other has weaknesses. Wherever possible, both should be used. In this way, they can be used as independent checks on each other, and this may serve to increase confidence in the results. When these cannot be used or are not sufficient, it may be necessary to rely on some degree of expert judgement.

5.4.2 *Analyse des conséquences*

L'analyse des conséquences est utilisée pour estimer l'impact probable en cas d'occurrence de l'événement indésirable.

Il convient que l'analyse des conséquences:

a) soit fondée sur les événements indésirables choisis;

b) décrive toutes les conséquences des événements indésirables;

c) prenne en compte des mesures permettant de remédier à ces conséquences ainsi que de toutes les conditions applicables ayant un effet sur les conséquences;

d) donne les critères utilisés pour réaliser l'identification des conséquences;

e) tienne compte à la fois des effets immédiats et de ceux qui peuvent apparaître après un certain temps, si cela est conforme au domaine d'application de l'étude;

f) tienne compte des conséquences secondaires, telles que celles en rapport avec des équipements et systèmes adjacents.

5.4.3 *Calculs du risque*

Il convient d'exprimer les risques selon les termes les plus appropriés. Certaines des données communément utilisées en sortie sont les suivantes:

a) fréquence prévue de mortalité ou de morbidité pour un individu donné (risque individuel);

b) tracés de courbes de fréquence par rapport aux conséquences (désignés par le terme courbes F-N où F est la fréquence et N le nombre cumulé de personnes subissant un niveau spécifié de préjudice ou les coûts cumulés de dommage) pour les risques sociaux;

c) taux de perte prévu statistiquement en termes d'accidents, de coûts économiques ou de dommages à l'environnement;

d) répartition du risque d'un niveau de dommage spécifique, présentée comme une courbe de niveau affichant les niveaux d'iso-dommage.

Il convient d'indiquer si l'estimation du risque reflète le niveau de risque total ou si elle ne comprend qu'une partie du risque total.

Lors du calcul des niveaux de risque, il est nécessaire de tenir compte à la fois de la durée de l'événement indésirable et de la probabilité d'exposition de personnes à ce risque.

Il est recommandé que les données utilisées pour calculer les niveaux de risques conviennent à l'application particulière. Dans la mesure du possible, il est bon que ces données soient fondées sur les circonstances spécifiques analysées. Lorsque ces circonstances ne sont pas disponibles, il convient d'utiliser des données génériques représentatives de la situation ou de rechercher un avis expert.

Il convient que les données soient rassemblées et organisées de façon à faciliter une récupération convenable des informations afin de les utiliser comme données d'entrée pour l'analyse du risque et la traçabilité. Il convient d'identifier et d'exclure de l'analyse les données qui ne sont plus applicables à la situation courante.

5.4.2 *Consequence analysis*

Consequence analysis is used to estimate the likely impact should the undesired event occur.

Consequence analysis should:

a) be based on the undesirable events selected;

b) describe any consequences resulting from the undesirable events;

c) take into consideration existing measures to mitigate the consequences together with all relevant conditions that have an effect on the consequences;

d) give the criteria used for completing the identification of the consequences;

e) consider both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the study;

f) consider secondary consequences, such as those associated with adjacent equipment and systems.

5.4.3 *Risk calculations*

Risk should be expressed in the most suitable terms. Some of the commonly used outputs are:

a) predicted frequency of mortality or morbidity to an individual (individual risk);

b) frequency versus consequence plots (known as F-N curves where F stands for frequency and N the cumulative number of people suffering a specified level of harm or the cumulative cost of damage) for societal risk;

c) the statistically expected loss rate in terms of casualties, economic cost or environmental damage;

d) the distribution of the risk of a specific damage level, presented as a contour plot, displaying levels of equal damage.

It should be stated whether the risk estimate reflects the total risk level, or if only part of the total risk is included.

In calculating risk levels both the duration of the undesired event and the probability that people will be exposed to it need to be taken into account.

Data used to calculate risk levels should be appropriate for the particular application. Where possible, such data should be based on the specific circumstances under analysis. Where these are not available, data of a generic nature representative of the situation should be utilized, or expert judgement sought.

Data should be collected and organized in a form which facilitates convenient retrieval of information for input to risk analysis and traceability. Data that are no longer relevant to the current situation should be identified and excluded from use in the analysis.

5.4.4 *Incertitudes*

De nombreuses incertitudes sont associées à l'estimation du risque. Il est nécessaire de comprendre les incertitudes et leurs causes pour interpréter les valeurs de risque de manière efficace. L'analyse des incertitudes associées aux données, méthodes et modèles utilisés pour identifier et estimer les risques impliqués, joue un rôle important dans leur application. L'analyse des incertitudes implique la détermination de la variation ou de l'imprécision des résultats du modèle qui découle de la variation collective des paramètres et des hypothèses utilisés pour définir le modèle. L'analyse de sensibilité est un domaine en étroite relation avec l'analyse des incertitudes. L'analyse de sensibilité implique la détermination de la modification de réaction d'un modèle aux changements de paramètres individuels du modèle.

L'estimation de l'incertitude consiste à traduire l'incertitude sur les paramètres déterminants du modèle en incertitude des résultats du modèle de risque. Il convient de spécifier, dans la mesure du possible, l'exhaustivité et la précision de l'estimation du risque. Il est recommandé d'identifier, dans la mesure du possible, les sources d'incertitude. Il convient que cette identification concerne à la fois l'incertitude des données et du modèle. Il convient d'indiquer les paramètres auxquels l'analyse est sensible.

5.5 *Vérification de l'analyse*

Il convient d'utiliser un processus de revue formel conduit par du personnel non impliqué dans le travail afin de confirmer l'intégrité de l'analyse du risque. Ces revues peuvent être conduites à l'intérieur même de l'organisation qui effectue l'analyse du risque ou bien il peut être fait usage d'organisations extérieures.

Il convient que la vérification comprenne les étapes suivantes:

a) s'assurer que le domaine d'application convient aux objectifs déclarés;

b) réviser toutes les hypothèses critiques afin de s'assurer qu'elles sont crédibles, à la lumière des informations disponibles;

c) s'assurer que l'analyste a utilisé des méthodes, des modèles et des données appropriés;

d) vérifier que l'analyse est reproductible par du personnel autre que le ou les analystes initiaux;

e) vérifier que les résultats de l'analyse ne sont pas affectés par la manière dont les données ou les résultats sont formatés.

Lorsque des expériences pratiques adéquates sont disponibles, il est admis que la vérification soit effectuée en comparant les résultats de l'analyse à des observations directes.

5.6 *Documentation*

Le rapport d'analyse du risque documente le processus d'analyse du risque et il convient qu'il comprenne ou se réfère au plan d'analyse du risque ainsi que les résultats d'évaluation initiale des dangers. La présentation des informations techniques qu'il contient est une partie critique du processus d'analyse du risque. Il convient que les estimations du risque soient exprimées en termes compréhensibles et que les points forts ainsi que les limites des différentes mesures du risque soient expliqués et que les incertitudes qui entourent les estimations du risque soient définies en un langage compréhensible pour le lecteur auquel elles s'adressent.

5.4.4 *Uncertainties*

There are many uncertainties associated with the estimation of risk. An understanding of uncertainties and their causes is required to interpret risk values effectively. The analysis of uncertainties associated with data, methods and models used to identify and estimate the risks involved plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the model results, resulting from the collective variation in the parameters and assumptions used to define the model. An area closely related to uncertainty analysis is sensitivity analysis. Sensitivity analysis involves the determination of the change in response of a model to changes in individual model parameters.

Estimating uncertainty consists of translating uncertainty in the crucial model parameters into uncertainty in the outputs of the risk model. The completeness and accuracy of the risk estimation should be stated as fully as possible. Sources of uncertainty should be identified where possible. This should address both data and model uncertainties. Parameters to which the analysis is sensitive should be stated.

5.5 *Analysis verification*

A formal review process carried out by people not involved with the work should be used to confirm the integrity of the analysis. Reviews may be conducted internally or use made of organizations external to that which performed the analysis.

Verification should include the following steps:

a) check that the scope is appropriate for the stated objectives;

b) review all critical assumptions and ensure that they are credible in the light of available information;

c) ensure that the analyst used appropriate methods, models and data;

d) check that the analysis is repeatable by personnel other than the original analyst(s);

e) check that the results of the analysis are insensitive to the way data or results are formatted.

Where adequate field experience is available, verification may be accomplished by comparing the results of the analysis with direct observations.

5.6 *Documentation*

The risk analysis report documents the risk analysis process and should include or refer to the risk analysis plan and the initial hazard evaluation results. The presentation of technical information in it is a critical part of the risk analysis process. Risk estimates should be expressed in understandable terms, the strengths and limitations of different risk measures used should be explained, and the uncertainties surrounding estimates of risk should be set out in language appropriate to the intended reader.

La portée du rapport dépendra des objectifs et du domaine d'application de l'analyse. Sauf pour des analyses très simples, il convient normalement que la documentation comporte les sections suivantes:

a) le résumé;
b) les conclusions;
c) les objectifs et le domaine d'application;
d) les limites, hypothèses et la justification des hypothèses;
e) la description des parties pertinentes du système;
f) la méthodologie d'analyse;
g) les résultats d'identification de dangers;
h) les modèles utilisés, y compris les hypothèses et la validation;
i) les données et leurs sources;
j) les résultats d'estimation du risque;
k) l'analyse de sensibilité et d'incertitude;
m) la discussion des résultats (y compris une discussion des difficultés analytiques);
n) les références.

5.7 *Mise à jour de l'analyse*

Si l'analyse du risque est prescrite pour appuyer un processus continu de gestion des risques, il convient qu'elle soit réalisée et documentée de façon qu'elle puisse être maintenue pendant tout le cycle de vie du système, de l'installation ou de l'activité. Il convient que l'analyse soit remise à jour au fur et à mesure que de nouvelles informations importantes sont disponibles et conformément aux besoins du processus de gestion.

6 Audits

Si nécessaire, il convient qu'un audit du processus d'analyse du risque soit effectué par des personnes qui ne sont pas directement impliquées dans l'exécution de cette analyse du risque spécifique afin de s'assurer de son efficacité et de sa conformité à la présente norme. Il convient d'appliquer des processus et procédures d'assurance qualité pertinents.

7 Méthodes d'analyse du risque

7.1 *Généralités*

Le présent article décrit certaines méthodes d'analyse de systèmes technologiques couramment utilisées qui sont applicables à l'identification des dangers et à l'estimation des risques ainsi que les critères de sélection correspondants.

7.2 *Choix des méthodes*

De manière générale, il convient qu'une méthode appropriée ait les caractéristiques suivantes:

a) il est recommandé qu'elle soit scientifiquement défendable et applicable au système considéré;

The extent of the report will depend on the objectives and scope of the analysis. Except for very simple analyses, the documentation should normally address the following:

a) summary;
b) conclusions;
c) objectives and scope;
d) limitations, assumptions and justification of hypotheses;
e) description of relevant parts of the system;
f) analysis methodology;
g) hazard identification results;
h) models used, including assumptions and validation;
i) data and their sources;
j) risk estimation results;
k) sensitivity and uncertainty analysis;
m) discussion of results (including a discussion of analytical difficulties);
n) references.

5.7 *Analysis update*

If the risk analysis is required to support a continuing risk management process it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, facility or activity. The analysis should be updated as significant new information becomes available and in accordance with the needs of the management process.

6 Audits

When required, an audit of the risk analysis process should be carried out to assure its effectiveness and adherence to this standard by persons who are not directly involved in performing the specific risk analysis. Relevant quality assurance processes and procedures should apply.

7 Risk analysis methods

7.1 *General*

This clause describes some common types of methods for analysis of technological systems that are applicable to hazard identification and risk estimation, along with criteria for their selection.

7.2 *Selection of methods*

In general terms, a suitable method should exhibit the following characteristics:

a) it should be scientifically defensible and appropriate to the system under consideration;

b) il est recommandé que les résultats obtenus se présentent sous une forme permettant une meilleure compréhension de la nature des risques et de la manière dont ils peuvent être contrôlés;

c) il est recommandé qu'elle puisse être utilisée par divers opérateurs de telle sorte qu'elle soit traçable, reproductible et vérifiable.

Il convient de justifier le choix des méthodes en tenant compte de leur pertinence et de leur convenance. En cas de doute quant à leurs pertinence et convenance, il est recommandé d'utiliser d'autres méthodes et de comparer les résultats obtenus. Lorsqu'il s'agit d'intégrer les résultats de diverses études, il convient que les méthodologies et les données obtenues en sortie soient compatibles.

Une fois prise la décision d'effectuer une analyse du risque et une fois définis les objectifs et le domaine d'application, il est recommandé de choisir la ou les méthodes sur la base de facteurs applicables, illustrés à la figure 3, tels que:

a) la phase de développement du système. Il est admis d'utiliser des méthodes moins détaillées au début du développement du système, il est recommandé d'affiner ces méthodes au fur et à mesure de la disponibilité de nouvelles informations;

b) les objectifs de l'étude. Les objectifs de l'analyse auront un effet direct sur les méthodes utilisées. Par exemple, s'il est entrepris une étude comparative entre différentes options, il peut être acceptable d'utiliser des modèles d'analyse des conséquences assez grossiers pour les parties du système qui ne sont pas affectées par les différences d'options;

c) le type de système et de danger analysé;

d) le niveau de sévérité potentiel. La décision prise quant au niveau de profondeur de l'analyse doit refléter la perception initiale des conséquences (même s'il peut être nécessaire de la modifier après réalisation d'une évaluation préliminaire);

e) les besoins en ressources humaines et matérielles ainsi que le degré de compétence. Une méthode simple, correctement mise en oeuvre, fournira des résultats meilleurs qu'une procédure plus sophistiquée d'application médiocre, si elle satisfait aux objectifs et au domaine d'application de l'analyse. En général, il convient que l'effort d'analyse soit cohérent avec le niveau de risque potentiel analysé;

f) la disponibilité des informations et des données. Certaines méthodes nécessitent plus d'informations et de données que d'autres;

g) la modification/mise à jour nécessaire de l'analyse. Il est admis que l'analyse puisse nécessiter des modifications/mises à jour futures et qu'à cet égard, certaines méthodes soient, plus que d'autres, enclines à être modifiées;

h) toutes prescriptions réglementaires et contractuelles.

7.3 *Méthodes d'analyse*

Certaines des méthodes les plus fréquemment utilisées sont données dans le tableau 1 et également décrites ci-dessous. Cependant, la liste du tableau 1 n'est en aucune manière exhaustive. Une description brève de certaines des méthodes utilisées est donnée dans l'annexe A. Il est quelque fois nécessaire d'utiliser plusieurs méthodes d'analyse.

7.3.1 *Identification des dangers*

L'identification des dangers implique une revue systématique du système étudié afin d'identifier le type de dangers inhérents ainsi que la manière dont ils pourraient se concré-

b) it should provide results in a form which enhances understanding of the nature of the risk and how it can be controlled;

c) it should be capable of use by a variety of practitioners in a manner that is traceable, repeatable and verifiable.

The reasons for the choice of methods should be given, with regard to relevance and suitability. If there is any doubt as to their relevance and suitability, alternative methods should be used and the results compared. When integrating the results from different studies, the methodologies and outputs should be compatible.

Once the decision has been made to perform a risk analysis and the objectives and scope have been defined, the method or methods should be selected, based on applicable factors, shown in figure 3, such as:

a) the phase of the system's development. Early in system development less detailed methods may be used; they should be refined as more information becomes available;

b) the objectives of the study. The objectives of the analysis will have a direct bearing on the methods used. For example, if a comparative study between different options is being undertaken, it may be acceptable to use fairly coarse consequence models for parts of the system not affected by the difference;

c) the type of system and hazard being analysed;

d) the potential level of severity. The decision on the depth to which analysis is carried out shall reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);

e) the manpower, degree of expertise and resources requirement. A simple method, well done, will provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the analysis. Ordinarily the effort put into the analysis should be consistent with the potential level of risk being analysed;

f) the availability of information and data. Some methods require more information and data than others;

g) the need for modification/updating of the analysis. The analysis may need to be modified/updated in future and some methods are more amendable than others in this regard;

h) any regulatory and contractual requirements.

7.3 *Methods of analysis*

Some of the most frequently used methods are given in table 1 and also described below. The list in table 1 is however by no means exhaustive. Brief descriptions of certain methods used are also given in annex A. It may sometimes be necessary to employ more than one method of analysis.

7.3.1 *Hazard identification*

Hazard identification involves a systematic review of the system under study to identify the type of inherent hazards that are present together with the ways in which they could be

tiser. Des enregistrements historiques d'accidents ainsi que l'expérience acquise d'analyses de risque précédents peuvent fournir des données d'entrée utiles au processus d'identification des dangers. Il est nécessaire de reconnaître qu'il existe un élément de subjectivité dans le jugement des dangers et il est admis que les dangers identifiés peuvent ne pas être les seuls dangers qui pourraient menacer le système. Il est important que les dangers identifiés soient revus à la lumière de toute nouvelle donnée pertinente. Dans leurs grandes lignes, les méthodes d'identification des dangers s'inscrivent dans trois catégories:

a) les méthodes comparatives dont des exemples sont les listes de contrôle, les indices de danger et les revues de données historiques;

b) les méthodes fondamentales, qui sont structurées afin de stimuler un groupe d'individus afin qu'ils associent à leur connaissance une certaine optique perspectiviste pour l'identification des dangers, en posant une série de questions du type «que se passerait-il si ?». Des exemples de ce type de méthodologie sont les études de danger et de faisabilité (HAZOP) ainsi que les analyses des modes de défaillance et de leurs effets (AMDE);

c) les techniques qui utilisent un raisonnement inductif telles que les schémas logiques d'arbres d'événements.

Il est admis d'utiliser d'autres techniques pour des problèmes spécifiques, afin d'améliorer l'identification du danger (et les capacités d'estimation du risque). Quelques-unes de ces techniques sont, par exemple: l'analyse transitoire, la méthodologie de Delphi et l'analyse de fiabilité humaine.

Quelles que soient les techniques réellement utilisées, il est important d'admettre, dans le processus global d'identification des dangers, que les erreurs humaines et organisationnelles sont des facteurs importants dans nombre d'accidents. Par conséquent, il convient que les scénarios d'accidents impliquant une erreur humaine ou organisationnelle soient également inclus dans le processus d'identification des dangers pour lequel il est recommandé de ne pas s'orienter exclusivement vers les aspects «matériels».

7.3.2 *Estimation du risque*

Dans la pratique, l'identification du danger d'un système, d'une installation ou d'une activité particulière peut donner lieu à un très grand nombre de scénarios d'accidents potentiels et on peut considérer que la soumission de chacun de ces scénarios à une analyse quantitative détaillée des fréquences et des conséquences n'est pas faisable. Dans de telles situations, il peut être acceptable de classer qualitativement les scénarios d'accidents et de les insérer dans une matrice de risque exprimant les différents niveaux de risques. La quantification se concentre ensuite sur les scénarios considérés comme donnant lieu à des niveaux de risques plus élevés. La figure 4 donne un exemple d'un type de matrice de risque possible. L'application de la matrice de risque pourrait générer des scénarios considérés comme donnant lieu à des niveaux de risques faibles, voire insignifiants, dont on ne tiendrait plus compte dans la mesure où ils ne pourraient pas constituer collectivement des niveaux de risques significatifs. Il existe de nombreuses matrices du risque; celle qui convient le mieux pour une analyse donnée dépend de l'application particulière. Il est essentiel que la forme de toute matrice utilisée soit enregistrée avec les positions estimées de tous les scénarios d'accidents pris en compte, qu'ils soient ou non soumis ultérieurement à une analyse quantitative détaillée.

realized. Historical accident records and experience from previous risk analyses can provide a useful input to the hazard identification process. It needs to be recognized that there is an element of subjectivity in judgements about hazards, and that the hazards identified may not always be the only ones which could pose a threat to the system. It is important that the identified hazards are reviewed in the light of any relevant new data. Hazard identification methods fall broadly into three categories:

a) comparative methods, examples of which are checklists, hazard indices and reviews of historical data;

b) fundamental methods, that are structured to stimulate a group of people to apply foresight in conjunction with their knowledge to the task of identifying hazards by raising a series of "what if?" questions. Examples of this type of methodology are Hazard and Operability (HAZOP) studies, and Fault Modes and Effects Analysis (FMEA);

c) inductive reasoning techniques such as event tree logic diagrams.

Other techniques may be used for specific problems to improve hazard identification (and risk estimation capabilities). Some examples include: sneak analysis, Delphi methodology and human reliability analysis.

Irrespective of the actual techniques employed, it is important that in the overall hazard identification process due recognition is given to the fact that human and organizational errors are important factors in many accidents. Hence accident scenarios involving human and organizational error should also be included in the hazard identification process which should not be exclusively directed on "hardware" aspects.

7.3.2 *Risk estimation*

In practice, hazard identification of a particular system, facility or activity may yield a very large number of potential accident scenarios and it may not always be considered feasible to subject each one to detailed quantitative frequency and consequence analysis. In such situations it may be reasonable to rank the accident scenarios qualitatively and position them within a risk matrix denoting different levels of risk. Quantification is then concentrated on the scenarios assessed as giving rise to higher levels of risk. Figure 4 gives an example of one possible type of risk matrix. Application of the risk matrix could result in scenarios considered to give rise to low or trivial risks being dropped from further consideration so long as collectively they could not give rise to significant risk levels. There are many risk matrices in existence; the most appropriate one for a given analysis depends on the particular application. It is essential that the form of any matrix used should be recorded together with the estimated positions of all the accident scenarios considered, irrespective of whether they are subsequently subject to detailed quantitative analysis.

Une analyse du risque quantitative nécessite normalement des estimations de la fréquence (ou de la probabilité) de l'événement indésirable et des conséquences (ou sévérité) associées afin de fournir une mesure du risque. Cependant, dans certains cas, par exemple lorsque les calculs indiquent que les conséquences sont insignifiantes ou que la fréquence est extrêmement faible, l'estimation d'un seul paramètre peut être suffisante.

7.3.2.1 *Analyse de fréquence*

L'objet de l'analyse de fréquence est de déterminer la fréquence de chacun des événements indésirables ou scénarios d'accidents décelés lors de l'étape d'identification des dangers. En général, trois approches fondamentales sont utilisées:

a) l'utilisation de données historiques applicables afin de déterminer la fréquence d'apparition de ces événements dans le passé, et par conséquent de juger la fréquence d'apparition de ces événements à l'avenir. Il convient que les données utilisées s'appliquent au type de système, d'installation ou d'activité considérés ainsi qu'aux normes opérationnelles de l'organisation concernée;

b) la prédiction de fréquence d'événements au moyen de techniques telles que l'analyse par arbre de panne et l'analyse par arbre d'événement. Lorsque les données historiques ne sont pas disponibles, ou inadéquates, il est nécessaire de synthétiser les fréquences d'événements en analysant le système ainsi que ses modes de défaillance associés. Des données numériques relatives à l'ensemble des événements applicables, y compris la défaillance des équipements et les erreurs humaines, sur la base d'expériences opérationnelles ou de sources de données publiées, sont alors combinées afin de produire une estimation de la fréquence des événements indésirables. Lorsque des techniques de prédiction sont utilisées, il est important de s'assurer que, lors de l'analyse, il a été dûment tenu compte de l'éventualité de défaillance de mode commun qui implique la défaillance simultanée d'un certain nombre de pièces ou de composants différents du système. Des techniques de simulation peuvent être nécessaires pour estimer les fréquences de défaillance des équipements et de la structure du fait du vieillissement et d'autres processus de dégradation, en calculant les effets des incertitudes;

c) l'utilisation d'avis experts. Il existe un certain nombre de méthodes formelles permettant d'obtenir des avis experts; ces méthodes utilisent des opinions visibles et explicites et fournissent une aide à la formulation de questions appropriées. Il convient que ces avis experts se fondent sur toute information disponible applicable, y compris les données historiques, spécifiques au système, expérimentales, conceptuelles, etc. Les méthodes disponibles comprennent l'approche Delphi, les méthodes de comparaison par paires, de catégorisation, et de probabilité absolue.

L'analyse par arbre de panne et l'analyse par arbre d'événement sont décrites dans l'annexe A. La CEI 1025 traite de manière détaillée de l'analyse par arbre de panne.

7.3.2.2 *Analyse des conséquences*

L'analyse des conséquences implique une estimation de l'impact sur les personnes, les biens ou l'environnement en cas d'apparition de l'événement indésirable. Normalement, pour les calculs de risque relatif à la sécurité (du public ou des travailleurs), elle consiste à estimer le nombre de personnes placées dans différents environnements, à des distances différentes de la source de l'événement, qui peuvent être soit tuées, soit blessées ou gravement affectées si l'événement indésirable a lieu.

A quantitative risk analysis normally requires estimates of both the frequency (or probability) of the undesired event and the associated consequence (or severity), to provide a measure of risk. However in some instances, such as where calculations indicate the consequences to be insignificant or the frequency to be extremely low, a single parameter estimate may be sufficient.

7.3.2.1 *Frequency analysis*

The purpose of frequency analysis is to determine the frequency of each of the undesired events or accident scenarios identified at the hazard identification stage. Three basic approaches are commonly taken:

a) use relevant historical data to determine the frequency with which these events have occurred in the past and hence make judgements as to the frequency of their occurrence in the future. The data used should be relevant to the type of system, facility or activity being considered and also to the operational standards of the organization involved;

b) predict event frequencies using techniques such as fault tree analysis and event tree analysis. When historical data are unavailable or inadequate, it is necessary to derive event frequencies by analysis of the system and its associated fault modes. Numerical data on all relevant events, including equipment failure and human error from operational experience or published data sources, are then combined to produce an estimate of the frequency of the undesired events. When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the co-incidental failure of a number of different parts or components within the system. Simulation techniques may be required to generate frequencies of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties;

c) use expert judgement. There are a number of formal methods for eliciting expert judgement which make the use of judgements visible and explicit and provide an aid to the asking of appropriate questions. Expert judgements should draw upon all relevant available information including historical, system-specific, experimental, design, etc. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

Fault tree analysis and event tree analysis are outlined in annex A to this standard. IEC 1025 deals in detail with fault tree analysis.

7.3.2.2 *Consequence analysis*

Consequence analysis involves estimating the impact on people, property or environment, should the undesired event occur. Normally, for risk calculations related to safety (of the public or workers), it consists of estimating the number of people located in different environments, at different distances from the source of the event, that may be either killed, injured or seriously affected, given the undesired event has occurred.

Les événements indésirables comprennent en général des situations telles que l'émanation de matières toxiques, les incendies, les explosions, les éclats projetés du fait de la désintégration d'équipements, etc. Des modèles de conséquence sont nécessaires pour prédire l'étendue des pertes et autres effets. La connaissance du mécanisme de déclenchement et du sort de la matière (ou de l'énergie) libérée qui en résulte permet d'en prédire les effets à toute distance de la source et à tout moment.

Il existe plusieurs méthodes d'estimation de ces effets qui vont des approches analytiques simplifiées à des modèles informatiques très complexes. Il est recommandé de s'assurer que les méthodes conviennent au problème pris en compte.

Tableau 1 – Méthodes utilisées en analyse du risque

a) Méthodes les plus couramment utilisées

Méthode	Description et usage	Référence
Analyse par arbre d'événement	Technique d'identification et d'analyse de la fréquence des dangers qui utilise un raisonnement inductif pour convertir différents événements initiateurs en conséquences éventuelles	A.4
Analyse des modes de défaillance et de leurs effets; analyse des modes de défaillance, de leurs effets et de leur criticité	Technique fondamentale d'identification et d'analyse de la fréquence des dangers qui analyse tous les modes de défaillance d'un équipement donné et leurs effets tant sur les autres composants que sur le système	CEI 812 A.2
Analyse par arbre de panne	Technique d'identification et d'analyse de la fréquence des dangers qui débute en considérant l'événement indésirable et détermine toutes les manières par lesquelles il peut survenir. Ces différents chemins sont représentés graphiquement	CEI 1025 A.3
Etude de danger et d'aptitude à l'exploitation	Technique fondamentale d'identification du danger qui évalue systématiquement chaque partie du système pour voir comment des écarts par rapport à la conception peuvent survenir et si ses écarts peuvent créer des problèmes	A.1
Analyse de fiabilité humaine	Technique d'analyse de fréquence qui traite de l'impact des individus sur les caractéristiques du système et évalue l'influence des erreurs humaines sur la fiabilité	A.6
Analyse préliminaire du danger	Technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité	A.5
Diagramme de fiabilité	Technique d'analyse de fréquence qui développe un modèle du système et de ses redondances pour évaluer la fiabilité globale du système	CEI 1078

The undesired events usually comprise situations such as release of toxic materials, fires, explosions, projectiles from disintegrating equipment, etc. Consequence models are needed for predicting the extent of casualties and other effects. The knowledge of the release mechanism and the subsequent fate of the released material (or energy) enables prediction to be made of the effects of the release at any distance from the source at any time.

There are many methods for estimating such effects ranging from simplified analytical approaches to very complex computer models. Care should be taken to ensure that the methods are appropriate to the problem being considered.

Table 1 – Methods used in risk analysis

a) Most Common Methods

Method	Description and usage	Reference
Event Tree Analysis	A hazard identification and frquency analysis technique which employs inductive reasoning to translate different initiating events into possible outcomes	A.4
Fault Modes and Effects Analysis & Fault Modes, Effect and Criticality Analysis	A fundamental hazard identification and frequency analysis technique which analyses all the fault modes of a given equipment item for their effects both on other components and the system	IEC 812 A.2
Fault Tree Analysis	A hazard identification and frequency analysis technique which starts with the undesired event and determines all the ways in which it could occur. These are displayed graphically	IEC 1025 A.3
Hazard & Operability Study	A fundamental hazard identification technique which systematically evaluates each part of the system to see how deviations from the design intent can occur and whether they can cause problems	A.1
Human Reliability Analysis	A frequency analysis technique which deals with the impact of people on system performance and evaluates the influence of human errors on reliability	A.6
Preliminary Hazard Analysis	A hazard identification and frequency analysis technique that can be used early in the design stage to identify hazards and assess their criticality	A.5
Reliability Block Diagram	A frequency analysis technique that creates a model of the system and its redundancies to evaluate the overall system reliability	IEC 1078

b) Autres méthode

Méthode	Description et usage
Catégorisation	Moyen de classer les risques selon les catégories auxquelles ils appartiennent afin de créer des groupes de risques prioritaires
Listes de contrôle	Technique d'identification des dangers qui fournit une liste de substances typiquement dangereuses et/ou les origines d'accidents potentiels qui doivent être prises en compte. Cette méthode peut évaluer la conformité avec les règlements et les normes
Analyse des défaillances de mode commun	Méthode qui permet d'évaluer si la défaillance simultanée d'un certain nombre de parties différentes ou de composants d'un système est possible et son effet global probable
Modèles de conséquence	Estimation de l'impact d'un événement sur les personnes, les biens ou l'environnement. Des méthodes analytiques simplifiées, aussi bien que des modèles complexes informatisés sont disponibles
Technique de Delphi	Moyen de combiner des avis d'experts qui peut comprendre une analyse de fréquence, une modélisation des conséquences et/ou une estimation du risque
Indice de danger	Technique d'identification/évaluation du danger qui peut être utilisée pour classer différentes option d'un système et identifier les options les moins dangereuses
Simulation de Monte-Carlo et autres techniques de simulation	Technique d'analyse de fréquence qui utilise un modèle du système pour évaluer les variations des conditions initiales et des hypothèses
Comparaison par paires	Moyen d'estimer et de classifier un ensemble de risques en envisageant des paires de risques et en évaluant une seule paire à la fois
Revue de données historiques	Technique d'identification du danger qui peut être utilisée pour identifier les domaines de problèmes potentiels et aussi fournir à l'analyse de fréquence une entrée basée sur les accidents et les données de fiabilité
Analyse transitoire	Méthode d'identification de chemins latents qui pourraient être à l'origine de l'apparition d'événements imprévus

b) Additional methods

Method	Description and usage
Category Rating	A means of rating risks by the categories in which they fall in order to create prioritized groups of risks
Checklists	A hazard identification technique which provides a listing of typical hazardous substances and/or potential accident sources which need to be considered. Can evaluate conformance with codes and standards
Common Mode Failure Analysis	A method for assessing whether the coincidental failure of a number of different parts or components within a system is possible and its likely overall effect
Consequence Models	The estimation of the impact of an event on people, property or the environment. Both simplified analytical approaches and complex computer models are available
Delphi Technique	A means of combining expert opinions that may support frequency analysis, consequence modelling and/or risk estimation
Hazard Indices	A hazard identification/evaluation technique which can be used to rank different system options and identify the less hazardous options
Monte-Carlo Simulation and other simulation techniques	A frequency analysis technique which uses a model of the system to evaluate variations in input conditions and assumptions
Paired Comparisons	A means of estimation and ranking a set of risks by looking at pairs of risks and evaluating just one pair at a time
Review of Historical Data	A hazard identification technique that can be used to identify potential problem areas and also provide an input into frequency analysis based on accident and reliability data *et al*
Sneak Analysis	A method of identifying latent paths that could cause the occurrence of unforeseen events

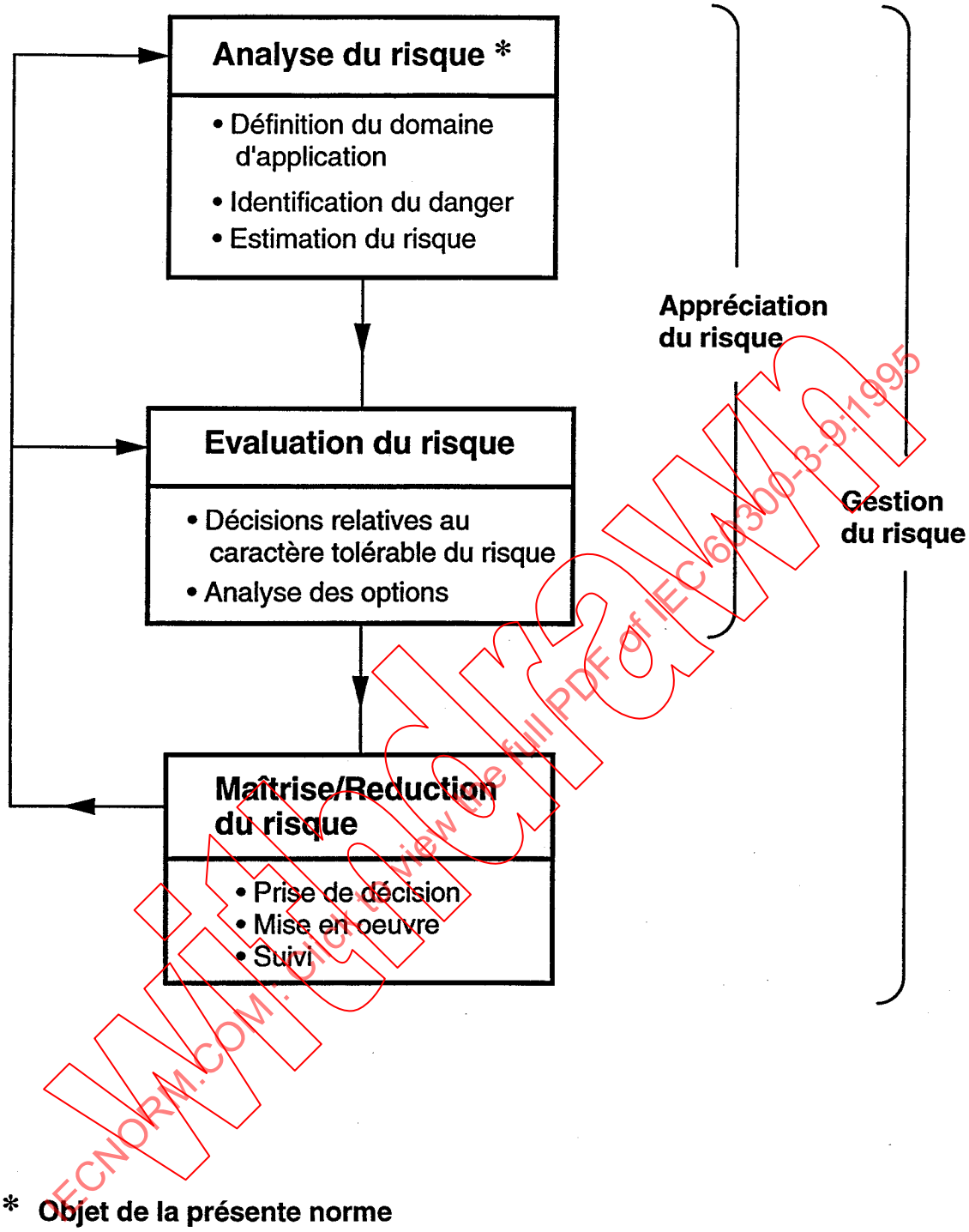

Figure 1 – Rapport simplifié entre analyse du risque et autres activités de gestion du risque

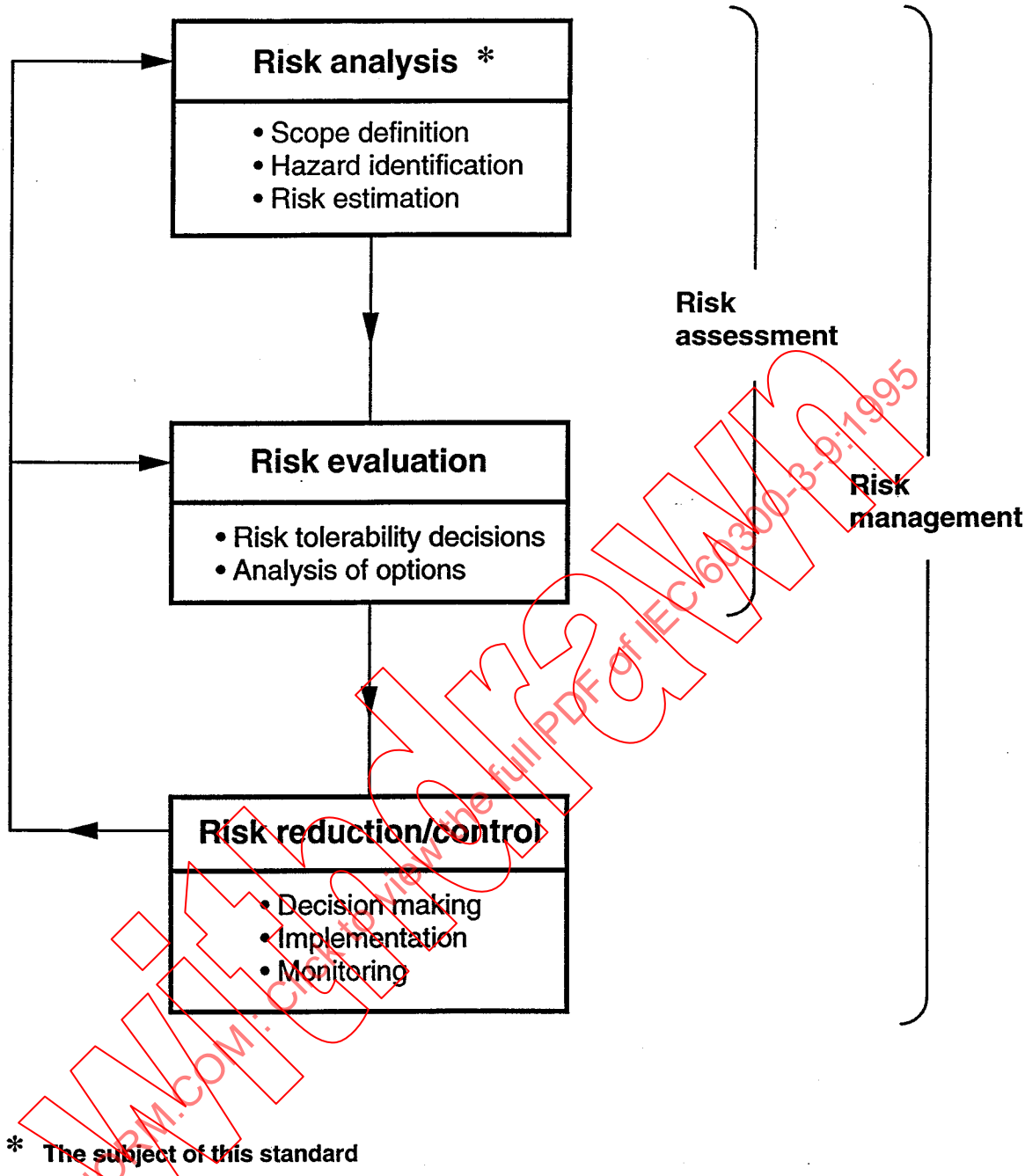

Figure 1 – A simplified relationship between risk analysis and other risk management activities

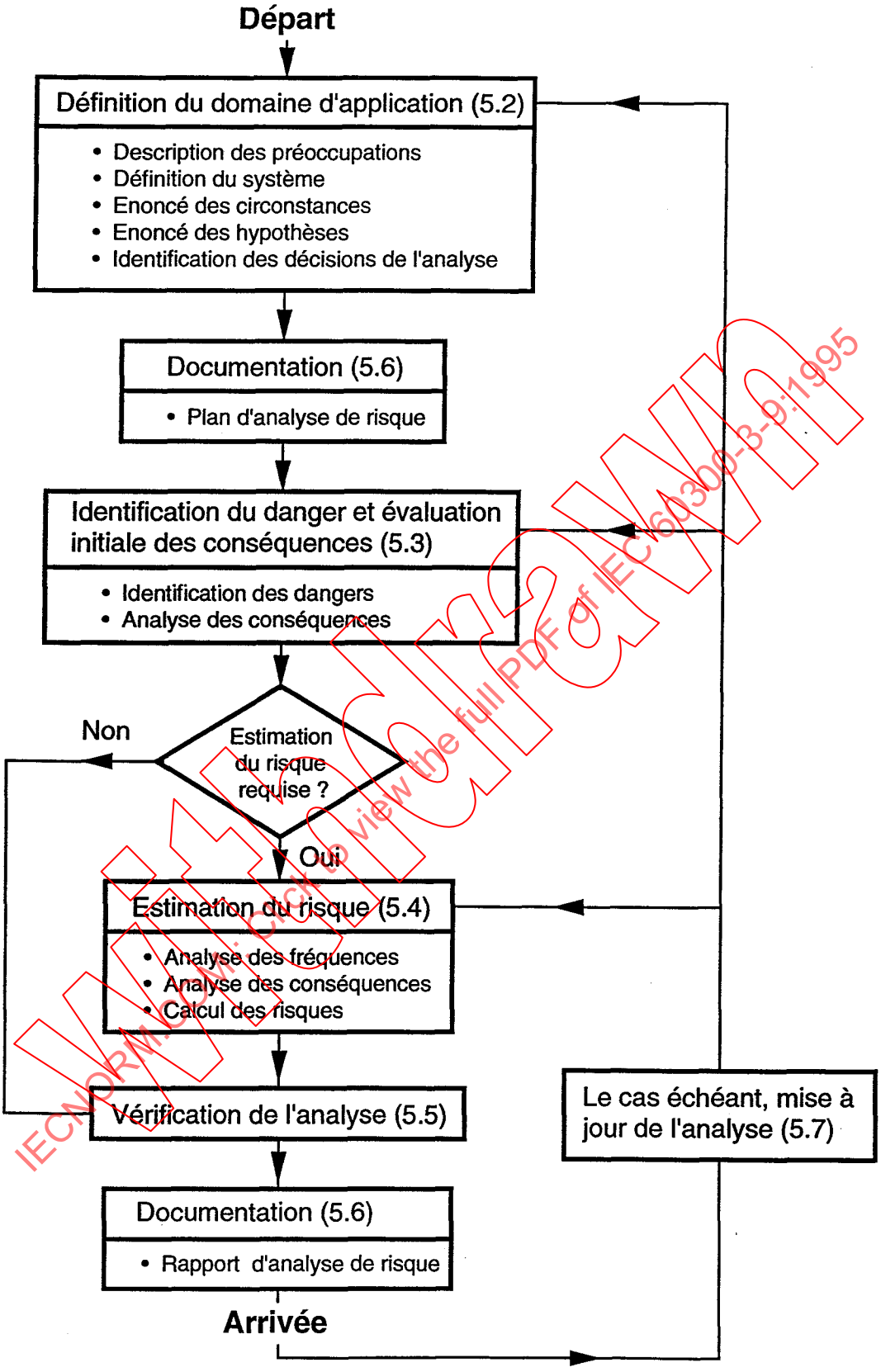

Figure 2 – Processus d'analyse du risque (article 5)

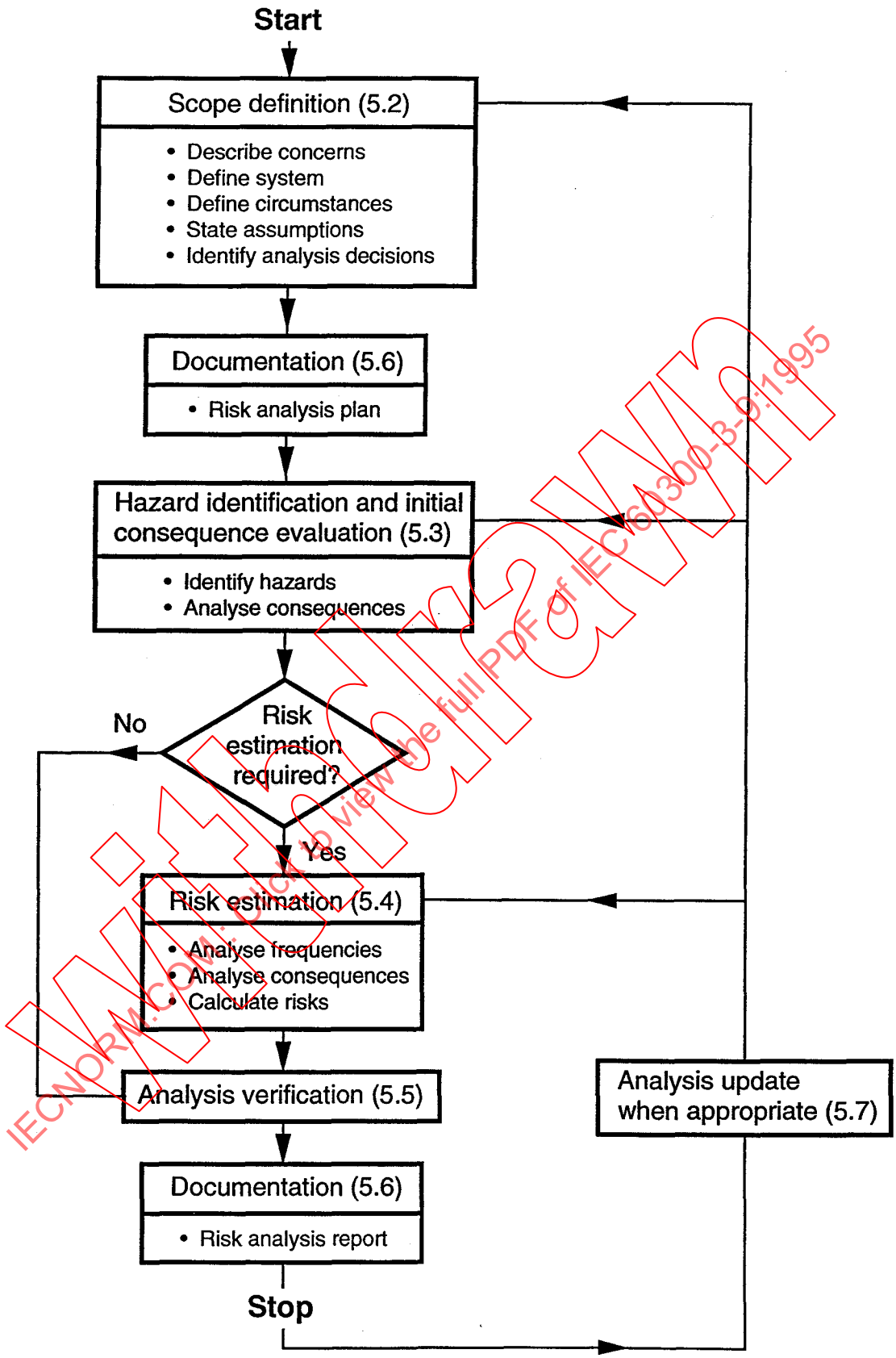

Figure 2 – The risk analysis process (clause 5)

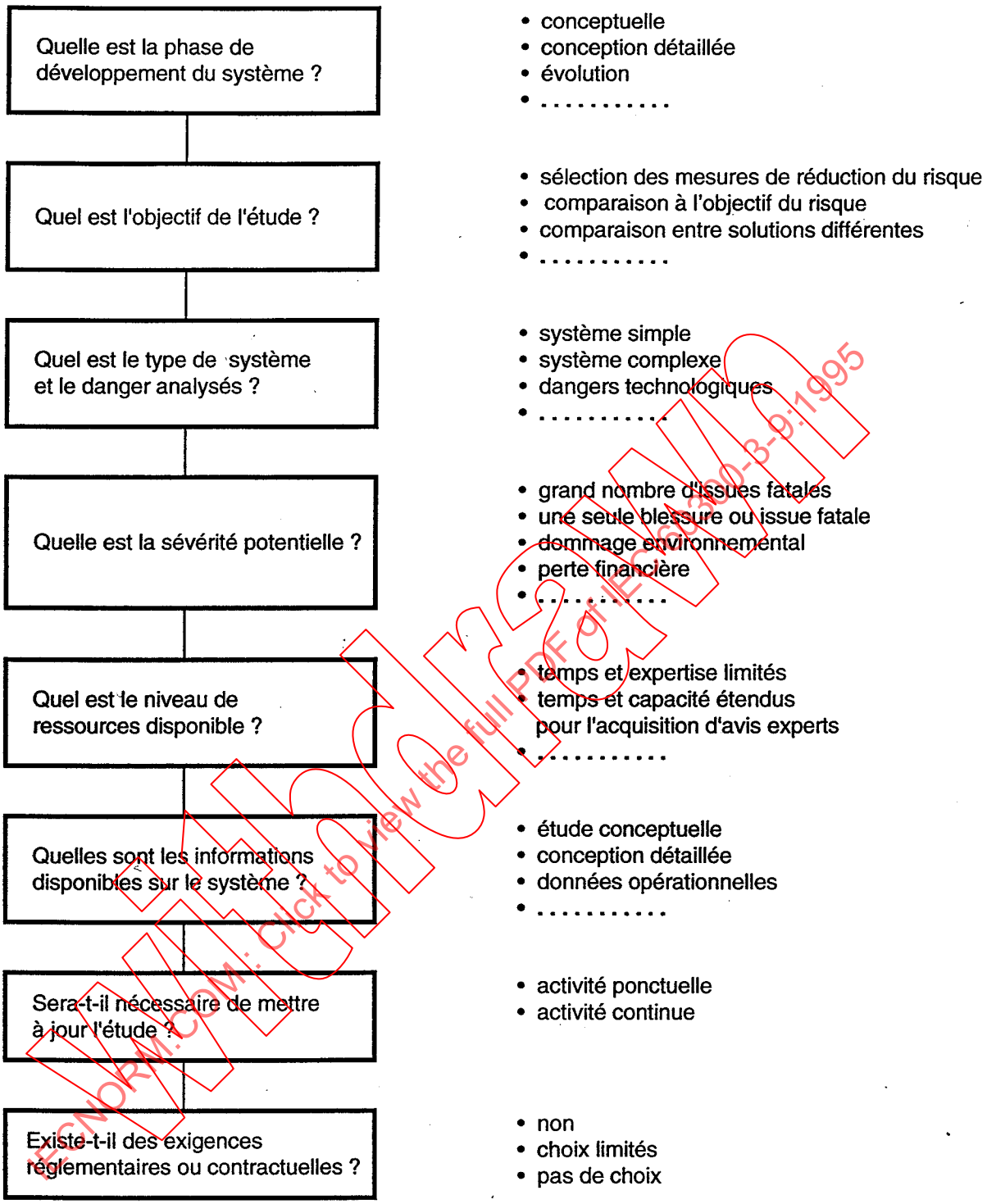

Figure 3 – Considérations types pour le choix du type d'analyse et de la profondeur de l'étude

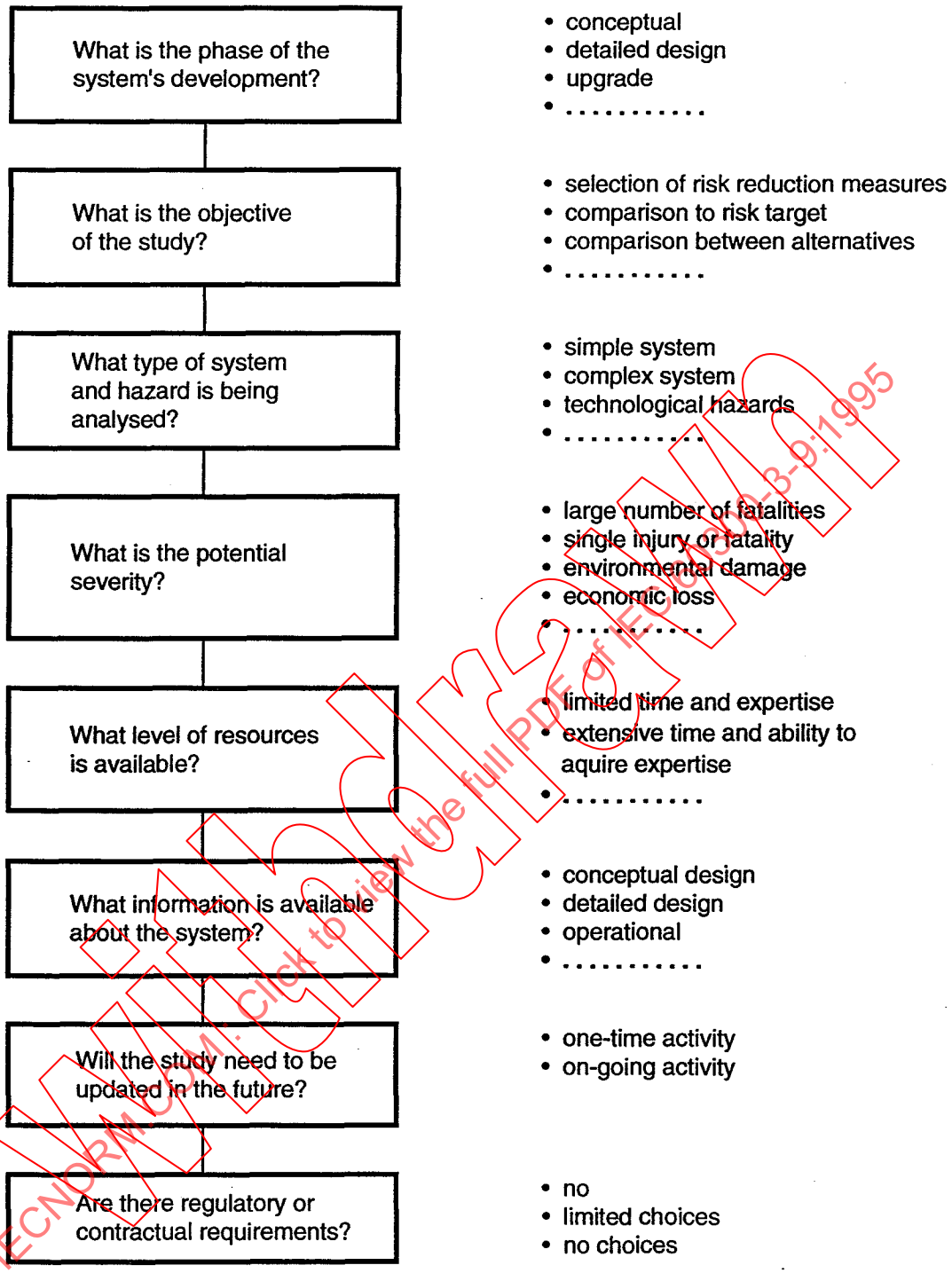

Figure 3 – Typical considerations in selecting type of analysis and depth of study

Fréquence d'événement	Fréquence Indicative (par année)	Sévérité des conséquences			
		Catastrophique	Majeure	Grave	Mineure
Fréquente	> 1	H	H	H	I
Probable	$1 - 10^{-1}$	H	H	I	L
Occasionelle	$10^{-1} - 10^{-2}$	H	H	L	L
Rare	$10^{-2} - 10^{-4}$	H	H	L	L
Improbable	$10^{-4} - 10^{-6}$	H	I	L	T
Invraisemblable	$< 10^{-6}$	I	I	T	T

NOTE - La définition des catégories et les valeurs utilisées dans la matrice sont uniquement fournies à titre d'exemple.

Où les classes de risque sont:

H = Haut risque
I = Risque intermédiaire
L = Faible risque
T = Risque insignifiant

Dans cet exemple, la sévérité des catégories de conséquence est définie comme:

Catastrophique — Perte pratiquement totale de l'installation ou du système. Nombreuses issues fatales

Majeure — Dommage important à l'installation ou au système. Peu d'issues fatales

Grave — Blessure grave, maladies professionnelles graves, dommage significatif à l'installation ou au système

Mineure — Blessure mineure, maladie professionnelles mineures ou dommage mineur au système

Figure 4 – Matrice de risque

Frequency of occurrence	Indicative frequency (per year)	Severity of consequence			
		Catastrophic	Major	Severe	Minor
Frequent	> 1	H	H	H	I
Probable	$1 - 10^{-1}$	H	H	I	L
Occasional	$10^{-1} - 10^{-2}$	H	H	L	L
Remote	$10^{-2} - 10^{-4}$	H	H	L	L
Improbable	$10^{-4} - 10^{-6}$	H	I	L	T
Incredible	$< 10^{-6}$	I	I	T	T

NOTE - The category definitions and values used within this matrix are illustrative only

Where the risk classes are:

H = High risk
I = Intermediate risk
L = Low risk
T = Trivial risk

For this example the severity of the consequence categories are defined as:

Catastrophic — Virtually complete loss of plant or system. Many fatalities

Major — Extensive damage to plant or system. Few fatalities

Severe — Severe injury, severe occupational illness, significant damage to the plant or system

Minor — Minor injury, minor occupational illness or minor system damage

Figure 4 – A risk matrix

Annexe A
(Informative)

Méthodes utilisées pour analyse

A.1 Etude de danger et de faisabilité (HAZOP)

Une étude HAZOP est une forme de l'analyse des modes de défaillance et de leurs effets (AMDE). A l'origine, les études HAZOP furent développées pour l'industrie chimique. Il s'agit d'une technique systématique d'identification des dangers et des problèmes de faisabilité pour l'ensemble d'une installation. Cette méthode est particulièrement utile pour identifier des dangers non prévus induits lors de la conception de l'installation et dus au manque d'information, ou introduits dans des installations existantes du fait des modifications des conditions de processus ou des procédures de fonctionnement. Les objectifs fondamentaux de cette technique sont:

a) fournir une description complète de l'installation ou du processus, y compris les conditions de conception prévues;

b) revoir systématiquement chaque partie de l'installation ou du processus afin de déceler la manière dont peuvent apparaître les écarts par rapport à la conception prévue; et

c) décider si ces écarts peuvent donner lieu à des dangers ou à des problèmes de faisabilité.

Les principes des études HAZOP peuvent être appliqués aux installations de processus en cours de fonctionnement ou à diverses étapes de conception. Une étude HAZOP effectuée pendant la phase initiale de conception peut fréquemment servir de guide pour donner lieu à une conception détaillée plus sûre.

La forme la plus fréquente d'étude HAZOP est réalisée lors de la phase de conception détaillée et est appelée étude HAZOP II.

Une étude HAZOP II comporte les étapes suivantes:

1) Définition des objectifs et du domaine d'application de l'étude, par exemple: les dangers ayant uniquement des impacts hors site ou uniquement des impacts sur site, les zones de l'installation à prendre en compte, etc.

2) La mise en place d'une équipe d'étude HAZOP. Il convient que cette équipe soit constituée de personnel de conception et de fonctionnement ayant la compétence technique nécessaire pour évaluer les effets des écarts par rapport au fonctionnement prévu.

3) La collecte de la documentation, plans et description de processus nécessaires. Ceci comprend des diagrammes de processus, des plans de la tuyauterie et de l'instrumentation, des spécifications des équipements, de la tuyauterie et de l'instrumentation, des logigrammes de contrôle de processus, des plans d'implantation, des procédures de fonctionnement et de maintenance, des procédures de réaction d'urgence, etc.

Annex A
(Informative)

Methods of analysis

A.1 Hazard and Operability (HAZOP) study

A HAZOP study is a form of fault modes and effects analysis (FMEA). HAZOP studies were originally developed for the chemical industry. It is a systematic technique for identifying hazards and operability problems throughout an entire facility. It is particularly useful in identifying unforeseen hazards designed into facilities due to lack of information, or introduced into existing facilities due to changes in process conditions or operating procedures. The basic objectives of the techniques are:

a) to produce a full description of the facility or process, including the intended design conditions;

b) to review systematically every part of the facility or process to discover how deviations from the intention of the design can occur; and

c) to decide whether these deviations can lead to hazards or operability problems.

The principles of HAZOP studies can be applied to process plants in operation or in various stages of design. A HAZOP study carried out during the initial phase of design can frequently provide a guide to safer detailed design.

The most common form of HAZOP study is carried out at the detailed design phase and is referred to as a HAZOP II study.

A HAZOP II study involves the following steps:

1) Definition of the objectives and scope of the study, for example hazards having only off-site impact or only on-site impact, areas of the plant to be considered, etc.

2) Assembly of a HAZOP study team. This team should consist of design and operation personnel with technical expertise to evaluate the effects of deviations from intended operation.

3) Collection of the required documentation, drawings and process description. This includes process flowsheets, piping and instrument drawings, equipment, piping and instrument specifications, process control logic diagrams, layout drawings, operating and maintenance procedures, emergency response procedures, etc.

4) L'analyse de chaque équipement important et de tous les équipements de soutien, tuyauterie et instrumentation, au moyen des documents rassemblés lors de l'étape 3. La conception du processus prévue est tout d'abord définie puis, pour chaque ligne et équipement, des mots guides (voir tableau A.1) sont appliqués aux variables du processus telles que la température, la pression, le débit, le niveau et la composition chimique. (Ces mots guides stimulent la réflexion individuelle et induisent des discussions en groupe.)

5) La documentation relative aux conséquences de tout écart par rapport à la normale et la mise en évidence des écarts qui sont considérés dangereux et vraisemblables. En outre, les moyens de détecter et/ou de prévenir l'écart sont identifiés. Cette documentation est en général réalisée sur la base de fiches de travail HAZOP. Un exemple de fiche de travail pour le mot guide «non, aucun» appliqué au «débit» est illustré dans le tableau A.2.

Il est admis qu'une étude HAZOP mette en lumière des écarts spécifiques pour lesquels il est nécessaire de développer des mesures correctives. Pour les cas où les mesures correctives ne sont pas évidentes ou sont potentiellement très coûteuses, les résultats de l'étude HAZOP identifient les événements initiateurs nécessaires à une analyse ultérieure du risque.

Tableau A.1 – Mots guides HAZOP II

Termes	Définitions
Aucun ou non	Aucune partie du résultat prévu n'est réalisée (par exemple: aucun débit)
Plus	Augmentation quantitative (par exemple: haute pression)
Moins	Diminution quantitative (par exemple: basse pression)
Autant que	Augmentation qualitative (par exemple: matériau supplémentaire)
En partie	Diminution qualitative (par exemple: un ou deux composants uniquement dans un mélange donné)
Inversion	Opposé (par exemple: refoulement)
Autre que	Aucune partie prévue n'est réalisée, l'événement qui a lieu est totalement différent (par exemple: écoulement du mauvais produit)

Tableau A.2 – Exemple de fiche de travail HAZOP II pour le mot guide «non, aucun»

Mot guide	Ecart	Causes possibles	Conséquences	Action nécessaire
Non, aucun	Aucun débit	1) Aucune alimentation en produit n'est disponible	Le polymère formé en sortie sera réduit	a) Assurer une bonne communication avec l'opérateur b) Prévoir une alarme de niveau bas sur le réservoir d'alimentation
		2) Défaillance de la pompe (pour diverses raisons)	Idem que 1)	Idem que b)
		3) Conduite bouchée ou fermeture erronée de la vanne ou défaillance à l'arrêt de la vanne pilote	Idem que A.1 Surchauffe de la pompe	Installer une conduite de retour sur chaque pompe

4) Analysis of each major item of equipment, and all supporting equipment, piping and instrumentation, using documents collected in step 3. The process design intent is first defined, then, for each line and item of equipment, guide words (see table A.1) are applied to process variables such as temperature, pressure, flow, level and chemical composition. (These guide words stimulate individual thought and induce group discussion.)

5) Documentation of the consequences of any deviation from normal and highlights of those deviations which are considered hazardous and credible. In addition, an identification is made of means to detect and/or prevent the deviation. This documentation is usually done on HAZOP worksheets. A sample of such a worksheet for the guide word "not, no" applied to "flow" is shown in table A.2.

A HAZOP study may highlight specific deviations for which mitigating measures need to be developed. For those cases where mitigating measures are not obvious or are potentially very costly, the results of the HAZOP study identify the initiating events necessary for further risk analysis.

Table A.1 – HAZOP II guide words

Terms	Definitions
No or not	No part of the intended result is achieved (e.g. no flow)
More	Quantitative increase (e.g. high pressure)
Less	Quantitative decrease (e.g. low pressure)
As well as	Qualitative increase (e.g. additional material)
Part of	Qualitative decrease (e.g. only one or two components in a mixture)
Reverse	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow of wrong material)

Table A.2 – Sample HAZOP II worksheet for guideword "not, no"

Guideword	Deviation	Possible causes	Consequences	Action required
Not, no	No flow	1) No feed material available	Reduced output polymer will be formed	a) Ensure good communication with operator b) Provided low level alarm on setting tank
		2) Pump fails (variety of reasons)	As for 1)	As for b)
		3) Line blockage or valve closed in error or control valve fails shut	As for A.1 Pump will overheat	Install recirculation line on each pump

A.2 Analyse des modes de défaillance et de leurs effets (AMDE)

La technique AMDE est principalement qualitative même si elle peut être quantifiée et permet d'identifier systématiquement les effets ou les conséquences de modes de panne de composant individuel. Il s'agit d'une technique inductive fondée sur la question «qu'arrive-t-il si... ?». La caractéristique essentielle de toute analyse AMDE est la prise en compte de chaque pièce/composant majeur du système, comment il tombe en panne (le mode de défaillance) et quels seraient les effets de la défaillance sur le système (effet des défaillances). En général, l'analyse est descriptive et organisée sous forme de tableau ou de fiche présentant les informations. En tant que telle, la procédure AMDE met clairement en rapport les modes de défaillance des composants, leurs causes et effets sur le système, et les présente sous une forme facilement lisible.

La procédure AMDE est une approche «du bas vers le haut» (inductive) et tient compte des modes de défaillance de chaque composant pris séparément. En tant que telle, la méthode permet une certaine forme de redondance avant que son exécution ne devienne encombrante. De même, les résultats peuvent être facilement vérifiés par une autre personne familiarisée avec le système.

Les principaux inconvénients de la technique sont la difficulté de traiter la redondance et l'intégration des actions de remise en état ainsi que l'accent mis sur des défaillances de composant unique.

Une procédure AMDE peut être étendue pour réaliser ce que l'on appelle une analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). Dans une procédure AMDEC, chaque mode de défaillance identifié est placé selon l'effet combiné de sa probabilité d'apparition et de la sévérité de ses conséquences.

La technique AMDE (et AMDEC) fournit des données d'entrée pour des analyses telles que analyse par arbre de panne. Comme pour les composants de système, il est admis qu'elle soit utilisée pour traiter les erreurs humaines. Ces techniques peuvent être utilisées à la fois pour l'identification des dangers et l'estimation de la probabilité (s'il n'existe dans le système qu'un niveau limité de redondance). D'autres détails relatifs aux techniques AMDE et AMDEC sont fournis dans la CEI 812.

A.3 Analyse par arbre de panne (AAP)

La technique AAP peut être qualitative ou quantitative et permet d'identifier de manière déductive les conditions et facteurs qui peuvent contribuer à un événement indésirable spécifié (appelé événement de tête); l'arbre des pannes est organisé de manière logique et graphique. Les pannes identifiées dans l'arbre peuvent être des événements associés à des défaillances matérielles de composants, à des erreurs humaines ou à tout autre événement pertinent donnant lieu à l'événement indésirable. En partant de l'événement de tête, les causes possibles ou les modes de défaillance du niveau fonctionnel immédiatement inférieur du système sont identifiés. En suivant progressivement l'identification du fonctionnement indésirable du système jusqu'au niveau système successivement inférieur, on obtient le niveau système requis qui est généralement le mode de panne du composant. La figure A.1 fournit un exemple d'arbre de panne d'un groupe électrogène de secours. La figure A.2 fournit un tableau des symboles d'arbres de panne les plus communément utilisés.

A.2 Fault Modes and Effects Analysis (FMEA)

FMEA is a technique, primarily qualitative although it can be quantified, by which the effect or consequences of individual component fault modes are systematically identified. It is an inductive technique which is based on the question "what happens if...?". The essential feature in any FMEA is the consideration of each major part/component of the system, how it becomes faulty (the fault mode), and what the effect of the fault mode on the system would be (the fault mode effect). Usually, the analysis is descriptive and is organized by creating a table or worksheet for the information. As such, FMEA clearly relates component fault modes, their causative factors and effects on the system, and presents them in an easily readable format.

FMEA is a "bottom-up" approach and considers consequences of component fault modes one at a time. As such, the method is tolerant of a slight amount of redundancy before becoming cumbersome to perform. Also, the results can be readily verified by another person familiar with the system.

The major disadvantages of the technique are the difficulty of dealing with redundancy and the incorporation of repair actions as well as the focus on single component failures.

An FMEA can be extended to perform what is called Fault Modes, Effects and Criticality Analysis (FMECA). In an FMECA each fault mode identified is ranked according to the combined influence of its probability of occurrence and the severity of its consequences.

FMEA and FMECA provide input to analyses such as fault tree analysis. As well as dealing with system components, they may be used to deal with human error. They can be used for both hazard identification and probability estimation (if only a limited level of redundancy is present in the system). Further details on both FMEA and FMECA are given in IEC 812.

A.3 Fault Tree Analysis (FTA)

FTA is a technique, which can be either qualitative or quantitative, by which conditions and factors that can contribute to a specified undesired event (called the top event) are deductively identified, organized in a logical manner and represented pictorially. The faults identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event. Starting with the top event, the possible causes or fault modes of the next lower functional system level are identified. Following stepwise identification of undesirable system operation to successively lower system levels will lead to the desired system level, which is usually the component fault mode. An example of a fault tree for an emergency generator is given in figure A.1. A table of the most common fault tree symbols is given in figure A.2.

La technique AAP constitue une approche disciplinée et hautement systématique, mais également suffisamment souple pour permettre d'analyser divers facteurs, y compris les interactions humaines et les phénomènes physiques. L'application de l'approche déductive («du haut vers le bas») fait partie intégrante de cette technique et met l'accent sur les effets de défaillance qui sont en rapport direct avec l'événement de tête. Il s'agit d'un avantage particulier même s'il risque également d'omettre des effets qui sont par ailleurs importants. La technique AAP est particulièrement utile à l'analyse de systèmes disposant de nombreux interfaces et interactions. La représentation graphique permet de comprendre plus facilement le comportement du système et de ses facteurs inhérents bien que la taille souvent importante des arbres puisse nécessiter un traitement informatique. De ce fait, la vérification de l'arbre de panne est également difficile.

La technique AAP peut être utilisée pour l'identification des dangers bien qu'elle soit principalement utilisée comme outil d'appréciation des risques permettant d'estimer les probabilités ou les fréquences de panne. D'autres détails sur la technique AAP sont fournis dans la CEI 1025.