IEC/ISO 31010

Edition 1.0 2009-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Risk management – Risk assessment techniques

Gestion des risques – Techniques d'évaluation des risques

IEC/ISO 31010:2009

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/ISO 31010

Edition 1.0 2009-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Risk management – Risk assessment techniques

Gestion des risques – Techniques d'évaluation des risques

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 03.100.01

ISBN 2-8318-1068-2

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International standard IEC/ISO 31010 has been prepared by IEC technical committee 56: Dependability together with the ISO TMB "Risk management" working group.

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

FDIS	Rapport de vote
56/1329/FDIS	56/1346/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. In ISO, the standard has been approved by 17 member bodies out of 18 having cast a vote.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Organizations of all types and sizes face a range of risks that may affect the achievement of their objectives.

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that should be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management includes the application of logical and systematic methods for

- communicating and consulting throughout this process;
- establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- what can happen and why (by risk identification)?
- what are the consequences?
- what is the probability of their future occurrence?
- are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This standard is intended to reflect current good practices in selection and utilization of risk assessment 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 system. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these standards are in harmony with this standard, the specific standards will generally be sufficient.

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

1 Scope

This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

This standard is not intended for certification, regulatory or contractual use.

This standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

NOTE This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions of ISO/IEC Guide 73 apply.

4 Risk assessment concepts

4.1 Purpose and benefits

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

- understanding the risk and its potential impact upon objectives;

- providing information for decision makers;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identifying the important contributors to risks and weak links in systems and organizations;
- comparing of risks in alternative systems, technologies or approaches;
- communicating risks and uncertainties;
- assisting with establishing priorities;
- contributing towards incident prevention based upon post-incident investigation;
- selecting different forms of risk treatment;
- meeting regulatory requirements;
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- assessing risks for end-of-life disposal.

4.2 Risk assessment and the risk management framework

This standard assumes that the risk assessment is performed within the framework and process of risk management described in ISO 31000.

A risk management framework provides the policies, procedures and organizational arrangements that will embed risk management throughout the organization at all levels.

As part of this framework, the organization should have a policy or strategy for deciding when and how risks should be assessed.

In particular, those carrying out risk assessments should be clear about

- the context and objectives of the organization,
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- how risk assessment integrates into organizational processes,
- methods and techniques to be used for risk assessment, and their contribution to the risk management process,
- accountability, responsibility and authority for performing risk assessment,
- resources available to carry out risk assessment,
- how the risk assessment will be reported and reviewed.

4.3 Risk assessment and the risk management process

4.3.1 General

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- communication and consultation;
- establishing the context;
- risk assessment (comprising risk identification, risk analysis and risk evaluation);
- risk treatment;
- monitoring and review.

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

4.3.2 Communication and consultation

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in

- developing a communication plan,
- defining the context appropriately,
- ensuring that the interests of stakeholders are understood and considered,
- bringing together different areas of expertise for identifying and analysing risk,
- ensuring that different views are appropriately considered in evaluating risks,
- ensuring that risks are adequately identified,
- securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

4.3.3 Establishing the context

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment programme are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

a) Establishing the external context involves familiarization with the environment in which the organization and the system operates including :
   - cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local;
   - key drivers and trends having impact on the objectives of the organization; and
   - perceptions and values of external stakeholders.

b) Establishing the internal context involves understanding
   - capabilities of the organization in terms of resources and knowledge,
   - information flows and decision-making processes,
   - internal stakeholders,
   - objectives and the strategies that are in place to achieve them,
   - perceptions, values and culture,
   - policies and processes,
   - standards and reference models adopted by the organization, and
   - structures (e.g. governance, roles and accountabilities).

c) Establishing the context of the risk management process includes
   - defining accountabilities and responsibilities,
   - defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions,

- defining the extent of the project, process, function or activity in terms of time and location,
- defining the relationships between a particular project or activity and other projects or activities of the organization,
- defining the risk assessment methodologies,
- defining the risk criteria,
- defining how risk management performance is evaluated,
- identifying and specifying the decisions and actions that have to be made, and
- identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies.

d) Defining risk criteria involves deciding

- the nature and types of consequences to be included and how they will be measured,
- the way in which probabilities are to be expressed,
- how a level of risk will be determined,
- the criteria by which it will be decided when a risk needs treatment,
- the criteria for deciding when a risk is acceptable and/or tolerable,
- whether and how combinations of risks will be taken into account.

Criteria can be based on sources such as

- agreed process objectives,
- criteria identified in specifications,
- general data sources,
- generally accepted industry criteria such as safety integrity levels,
- organizational risk appetite,
- legal and other requirements for specific equipment or applications.

4.3.4 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can be assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- whether an activity should be undertaken;
- how to maximize opportunities;
- whether risks need to be treated;
- choosing between options with different risks;
- prioritizing risk treatment options;
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

4.3.5 Risk treatment

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

4.3.6 Monitoring and review

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- assumptions about risks remain valid;
- assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- expected results are being achieved;
- results of risk assessment are in line with actual experience;
- risk assessment techniques are being properly applied;
- risk treatments are effective.

Accountability for monitoring and performing reviews should be established.

5 Risk assessment process

5.1 Overview

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (see Figure 1). The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

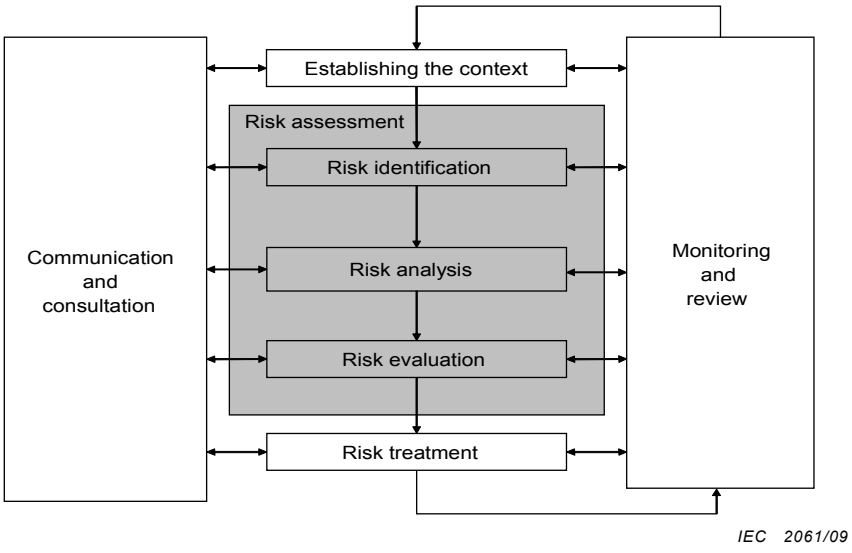

Figure 1 – Contribution of risk assessment to the risk management process

Risk assessment may require a multidisciplinary approach since risks may cover a wide range of causes and consequences.

5.2 Risk identification

Risk identification is the process of finding, recognizing and recording risks.

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact

Risk identification methods can include:

- evidence based methods, examples of which are check-lists and reviews of historical data;
- systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
- inductive reasoning techniques such as HAZOP.

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

5.3 Risk analysis

5.3.1 General

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. Various methods for these analyses are described in Annex B. More than one technique may be required for complex applications.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made

In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. 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 methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

5.3.2 Controls assessment

The level of risk will depend on the adequacy and effectiveness of existing controls. Questions to be addressed include:

- what are the existing controls for a particular risk?
- are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- in practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.

5.3.3 Consequence analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. The types of consequence to be analysed and the stakeholders affected will have been decided when the context was established.

Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.

Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyse both high and low consequence risks separately. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyse them separately.

Consequence analysis can involve:

- taking into consideration existing controls to treat the consequences, together with all relevant contributory factors that have an effect on the consequences;
- relating the consequences of the risk to the original objectives;
- considering both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the assessment;
- considering secondary consequences, such as those impacting upon associated systems, activities, equipment or organizations.

5.3.4 Likelihood analysis and probability estimation

Three general approaches are commonly employed to estimate probability; they may be used individually or jointly:

a) The use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future. The data used should be relevant to the type of system, facility, organization or activity being considered and also to the operational standards of the organization involved. If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain. This applies especially for zero occurrences, when one cannot assume the event, situation or circumstance will not occur in the future.

b) Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis (see Annex B). When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, humans, organizations and systems from operational experience, or published data sources are then combined to produce an estimate of the probability of the top event. 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 arising from the same cause. Simulation techniques may be required to generate probability of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.

c) Expert opinion can be used in a systematic and structured process to estimate probability. Expert judgements should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc. There are a number of formal methods for eliciting expert judgement which provide an aid to the formulation of appropriate questions. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

5.3.5 Preliminary analysis

Risks may be screened in order to identify the most significant risks, or to exclude less significant or minor risks from further analysis. The purpose is to ensure that resources will be focussed on the most important risks. Care should be taken not to screen out low risks which occur frequently and have a significant cumulative effect

Screening should be based on criteria defined in the context. The preliminary analysis determines one or more of the following courses of action:

- decide to treat risks without further assessment;
- set aside insignificant risks which would not justify treatment;
- proceed with more detailed risk assessment.

The initial assumptions and results should be documented.

5.3.6 Uncertainties and sensitivities

There are often considerable uncertainties associated with the analysis of risk. An understanding of uncertainties is necessary to interpret and communicate risk analysis results effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyse risk plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the results, resulting from the collective variation in the parameters and assumptions used to define the results. An area closely related to uncertainty analysis is sensitivity analysis.

Sensitivity analysis involves the determination of the size and significance of the magnitude of risk to changes in individual input parameters. It is used to identify those data which need to be accurate, and those which are less sensitive and hence have less effect upon overall accuracy.

The completeness and accuracy of the risk analysis should be stated as fully as possible. Sources of uncertainty should be identified where possible and should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

5.4 Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk.

Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision.

Decisions may include:

- whether a risk needs treatment;
- priorities for treatment;
- whether an activity should be undertaken;
- which of a number of paths should be followed.

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but they need to be revisited in more detail at this stage now that more is known about the particular risks identified.

The simplest framework for defining risk criteria is a single level which divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect

the uncertainties involved both in estimating risks and in defining the boundary between those that need treatment and those that do not.

The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

A common approach is to divide risks into three bands:

a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;

b) a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;

c) a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

The 'as low as reasonably practicable' or ALARP criteria system used in safety applications follows this approach, where, in the middle band, there is a sliding scale for low risks where costs and benefits can be directly compared, whereas for high risks the potential for harm must be reduced, until the cost of further reduction is entirely disproportionate to the safety benefit gained.

5.5 Documentation

The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear.

The extent of the report will depend on the objectives and scope of the assessment. Except for very simple assessments, the documentation can include:

- objectives and scope;
- description of relevant parts of the system and their functions;
- a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed;
- risk criteria applied and their justification;
- limitations, assumptions and justification of hypotheses;
- assessment methodology;
- risk identification results;
- data, assumptions and their sources and validation;
- risk analysis results and their evaluation;
- sensitivity and uncertainty analysis;
- critical assumptions and other factors which need to be monitored;
- discussion of results;
- conclusions and recommendations;
- references.

If the risk assessment supports 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, organization, equipment or activity. The assessment should be updated as significant new information becomes available and the context changes, in accordance with the needs of the management process.

5.6 Monitoring and reviewing risk assessment

The risk assessment process will highlight context and other factors that might be expected to vary over time and which could change or invalidate the risk assessment. These factors should be specifically identified for on-going monitoring and review, so that the risk assessment can be updated when necessary.

Data to be monitored in order to refine the risk assessment should also be identified and collected.

The effectiveness of controls should also be monitored and documented in order to provide data for use in risk analysis. Accountabilities for creation and reviewing the evidence and documentation should be defined.

5.7 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycles phases have different requirements and need different techniques For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of positive and negative risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,
- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6 Selection of risk assessment techniques

6.1 General

This clause describes how techniques for risk assessment may be selected. The annexes list and further explain a range of tools and techniques that can be used to perform a risk assessment or to assist with the risk assessment process. It may sometimes be necessary to employ more than one method of assessment.

6.2 Selection of techniques

Risk assessment may be undertaken in varying degrees of depth and detail and using one or many methods ranging from simple to complex. The form of assessment and its output should be consistent with the risk criteria developed as part of establishing the context. Annex A illustrates the conceptual relationship between the broad categories of risk assessment techniques and the factors present in a given risk situation, and provides illustrative examples

of how organizations can select the appropriate risk assessment techniques for a particular situation.

In general terms, suitable techniques should exhibit the following characteristics:

- it should be justifiable and appropriate to the situation or organization under consideration;
- it should provide results in a form which enhances understanding of the nature of the risk and how it can be treated;
- it should be capable of use in a manner that is traceable, repeatable and verifiable.

The reasons for the choice of techniques should be given, with regard to relevance and suitability. When integrating the results from different studies, the techniques used and outputs should be comparable.

Once the decision has been made to perform a risk assessment and the objectives and scope have been defined, the techniques should be selected, based on applicable factors such as:

- the objectives of the study. The objectives of the risk assessment will have a direct bearing on the techniques used. For example, if a comparative study between different options is being undertaken, it may be acceptable to use less detailed consequence models for parts of the system not affected by the difference;
- the needs of decision-makers. In some cases a high level of detail is needed to make a good decision, in others a more general understanding is sufficient;
- the type and range of risks being analysed;
- the potential magnitude of the consequences. The decision on the depth to which risk assessment is carried out should reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);
- the degree of expertise, human and other resources needed. A simple method, well done, may provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the assessment. Ordinarily, the effort put into the assessment should be consistent with the potential level of risk being analysed;
- the availability of information and data. Some techniques require more information and data than others;
- the need for modification/updating of the risk assessment. The assessment may need to be modified/updated in future and some techniques are more amendable than others in this regard;
- any regulatory and contractual requirements.

Various factors influence the selection of an approach to risk assessment such as the availability of resources, the nature and degree of uncertainty in the data and information available, and the complexity of the application (see Table A.2).

6.3 Availability of resources

Resources and capabilities which may affect the choice of risk assessment techniques include:

- the skills experience capacity and capability of the risk assessment team;
- constraints on time and other resources within the organization;
- the budget available if external resources are required.

6.4 The nature and degree of uncertainty

The nature and degree of uncertainty requires an understanding of the quality, quantity and integrity of information available concerning the risk under consideration. This includes the extent to which sufficient information about the risk, its sources and causes, and its

consequences to the achievement of objectives is available. Uncertainty can stem from poor data quality or the lack of essential and reliable data. To illustrate, data collection methods may change, the way organizations use such methods may change or the organization may not have an effective collection method in place at all, for collecting data about the identified risk.

Uncertainty can also be inherent in the external and internal context of the organization. Available data do not always provide a reliable basis for the prediction of the future. For unique types of risks, historical data may not be available or there may be different interpretations of available data by different stakeholders. Those undertaking risk assessment need to understand the type and nature of the uncertainty and appreciate the implications for the reliability of the risk assessment results. These should always be communicated to decision-makers.

6.5 Complexity

Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions. In other cases, treating a single risk can have implications elsewhere and can impact on other activities. Consequential impacts and risk dependencies need to be understood to ensure that in managing one risk, an intolerable situation is not created elsewhere. Understanding the complexity of a single risk or of a portfolio of risks of an organization is crucial for the selection of the appropriate method or techniques for risk assessment.

6.6 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycle phases have different needs and require different techniques For example during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available, risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,
- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6.7 Types of risk assessment techniques

Risk assessment techniques can be classified in various ways to assist with understanding their relative strengths and weaknesses. The tables in Annex A correlate some potential techniques and their categories for illustrative purposes.

Each of the techniques is further elaborated upon in Annex B as to the nature of the assessment they provide and guidance to their applicability for certain situations.

Annex A
(informative)

Comparison of risk assessment techniques

A.1 Types of technique

The first classification shows how the techniques apply to each step of the risk assessment process as follows:

- risk identification;
- risk analysis – consequence analysis;
- risk analysis – qualitative, semi-quantitative or quantitative probability estimation;
- risk analysis – assessing the effectiveness of any existing controls;
- risk analysis – estimation the level of risk;
- risk evaluation.

For each step in the risk assessment process, the application of the method is described as being either strongly applicable, applicable or not applicable (see Table A.1).

A.2 Factors influencing selection of risk assessment techniques

Next the attributes of the methods are described in terms of

- complexity of the problem and the methods needed to analyse it,
- the nature and degree of uncertainty of the risk assessment based on the amount of information available and what is required to satisfy objectives,
- the extent of resources required in terms of time and level of expertise, data needs or cost,
- whether the method can provide a quantitative output.

Examples of types of risk assessment methods available are listed in Table A.2 where each method is rated as high medium or low in terms of these attributes.

Table A.1 – Applicability of tools used for risk assessment

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1)] Strongly applicable.

[2)] Not applicable.

[3)] Applicable.

Table A.2 – Attributes of a selection of risk assessment tools

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
LOOK-UP METHODS					
Check-lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards	Low	Low	Low	No
Preliminary hazard analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system	Low	High	Medium	No
SUPPORTING METHODS					
Structured Interview and brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many interview techniques	Low	Low	Low	No
Delphi technique	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts	Medium	Medium	Medium	No
SWIFT Structured "what-if")	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique	Medium	Medium	Any	No
Human reliability analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system	Medium	Medium	Medium	Yes
SCENARIO ANALYSIS					
Root cause analysis (single loss analysis)	A single loss that has occurred is analysed in order to understand contributory causes and how the system or process can be improved to avoid such future losses. The analysis shall consider what controls were in place at the time the loss occurred and how controls might be improved	Medium	Low	Medium	No

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
Scenario analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively	Medium	High	Medium	No
Toxicological risk assessment	Hazards are identified and analysed and possible pathways by which a specified target might be exposed to the hazard are identified. Information on the level of exposure and the nature of harm caused by a given level of exposure are combined to give a measure of the probability that the specified harm will occur	High	High	Medium	Yes
Business impact analysis	Provides an analysis of how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be required to manage it	Medium	Medium	Medium	No
Fault tree analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	High	High	Medium	Yes
Event tree analysis	Using inductive reasoning to translate probabilities of different initiating events into possible outcomes	Medium	Medium	Medium	Yes
Cause/ consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered	High	Medium	High	Yes
Cause-and-effect analysis	An effect can have a number of contributory factors which may be grouped into different categories. Contributory factors are identified often through brainstorming and displayed in a tree structure or fishbone diagram	Low	Low	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
FUNCTION ANALYSIS					
FMEA and FMECA	FMEA (Failure Mode and Effect Analysis) is a technique which identifies failure modes and mechanisms, and their effects. There are several types of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA. FMEA may be followed by a criticality analysis which defines the significance of each failure mode, qualitatively, semi-qualitatively, or quantitatively (FMECA). The criticality analysis may be based on the probability that the failure mode will result in system failure, or the level of risk associated with the failure mode, or a risk priority number	Medium	Medium	Medium	Yes
Reliability-centred maintenance	A method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment	Medium	Medium	Medium	Yes
Sneak analysis (Sneak circuit analysis)	A methodology for identifying design errors. A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel	Medium	Medium	Medium	No
HAZOP Hazard and operability studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed	Medium	High	High	No
HACCP Hazard analysis and critical control points	A systematic, proactive, and preventive system for assuring product quality, reliability and safety of processes by measuring and monitoring specific characteristics which are required to be within defined limits	Medium	Medium	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
CONTROLS ASSESSMENT					
LOPA (Layers of protection analysis	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated	Medium	Medium	Medium	Yes
Bow tie analysis	A simple diagrammatic way of describing and analysing the pathways of a risk from hazards to outcomes and reviewing controls. It can be considered to be a combination of the logic of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences	Medium	High	Medium	Yes
STATISTICAL METHODS					
Markov analysis	Markov analysis, sometimes called *State-space* analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including various degraded states	High	Low	High	Yes
Monte-Carlo analysis	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system, for a number of inputs, where each input has a defined distribution and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. The inputs can be based upon a variety of distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used	High	Low	High	Yes
Bayesian analysis	A statistical procedure which utilizes prior distribution data to assess the probability of the result. Bayesian analysis depends upon the accuracy of the prior distribution to deduce an accurate result. Bayesian belief networks model cause-and-effect in a variety of domains by capturing probabilistic relationships of variable inputs to derive a result	High	Low	High	Yes

Annex B
(informative)

Risk assessment techniques

B.1 Brainstorming

B.1.1 Overview

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify potential failure modes and associated hazards, risks, criteria for decisions and/or options for treatment. The term “brainstorming” is often used very loosely to mean any type of group discussion. However true brainstorming involves particular techniques to try to ensure that people's imagination is triggered by the thoughts and statements of others in the group.

Effective facilitation is very important in this technique and includes stimulation of the discussion at kick-off, periodic prompting of the group into other relevant areas and capture of the issues arising from the discussion (which is usually quite lively).

B.1.2 Use

Brainstorming can be used in conjunction with other risk assessment methods described below or may stand alone as a technique to encourage imaginative thinking at any stage of the risk management process and any stage of the life cycle of a system. It may be used for high-level discussions where issues are identified, for more detailed review or at a detailed level for particular problems.

Brainstorming places a heavy emphasis on imagination. It is therefore particularly useful when identifying risks of new technology, where there is no data or where novel solutions to problems are needed.

B.1.3 Inputs

A team of people with knowledge of the organization, system, process or application being assessed.

B.1.4 Process

Brainstorming may be formal or informal. Formal brainstorming is more structured with participants prepared in advance and the session has a defined purpose and outcome with a means of evaluating ideas put forward. Informal brainstorming is less structured and often more ad-hoc.

In a formal process:

- the facilitator prepares thinking prompts and triggers appropriate to the context prior to the session;
- objectives of the session are defined and rules explained;
- the facilitator starts off a train of thought and everyone explores ideas identifying as many issues as possible There is no discussion at this point about whether things should or should not be in a list or what is meant by particular statements because this tends to inhibit free-flowing thought. All input is accepted and none is criticized and the group moves on quickly to allow ideas to trigger lateral thinking;

- the facilitator may set people off on a new track when one direction of thought is exhausted or discussion deviates too far. The idea however, is to collect as many diverse ideas as possible for later analysis.

B.1.5 Outputs

Outputs depend on the stage of the risk management process at which it is applied, for example at the identification stage, outputs might be a list of risks and current controls.

B.1.6 Strengths and limitations

Strengths of brainstorming include:

- it encourages imagination which helps identify new risks and novel solutions;
- it involves key stakeholders and hence aids communication overall;
- it is relatively quick and easy to set up.

Limitations include:

- participants may lack the skill and knowledge to be effective contributors;
- since it is relatively unstructured, it is difficult to demonstrate that the process has been comprehensive, e.g. that all potential risks have been identified;
- there may be particular group dynamics where some people with valuable ideas stay quiet while others dominate the discussion. This can be overcome by computer brainstorming, using a chat forum or nominal group technique. Computer brainstorming can be set up to be anonymous, thus avoiding personal and political issues which may impede free flow of ideas. In nominal group technique ideas are submitted anonymously to a moderator and are then discussed by the group.

B.2 Structured or semi-structured interviews

B.2.1 Overview

In a structured interview, individual interviewees are asked a set of prepared questions from a prompting sheet which encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise.

B.2.2 Use

Structured and semi-structured interviews are useful where it is difficult to get people together for a brainstorming session or where free-flowing discussion in a group is not appropriate for the situation or people involved. They are most often used to identify risks or to assess effectiveness of existing controls as part of risk analysis. They may be applied at any stage of a project or process. They are a means of providing stakeholder input to risk assessment.

B.2.3 Inputs

Inputs include:

- a clear definition of the objectives of the interviews;
- a list of interviewees selected from relevant stakeholders;
- a prepared set of questions.

B.2.4 Process

A relevant question set, is created to guide the interviewer. Questions should be open-ended where possible, should be simple, in appropriate language for the interviewee and cover one issue only. Possible follow-up questions to seek clarification are also prepared.

Questions are then posed to the person being interviewed. When seeking elaboration, questions should be open-ended. Care should be taken not to “lead” the interviewee.

Responses should be considered with a degree of flexibility in order to provide the opportunity of exploring areas into which the interviewee may wish to go.

B.2.5 Outputs

The outputs are the stakeholder’s views on the issues which are the subject of the interviews.

B.2.6 Strengths and limitations

The strengths of structured interviews are as follows :

- structured interviews allow people time for considered thought about an issue;
- one-to-one communication may allow more in-depth consideration of issues;
- structured interviews enable involvement of a larger number of stakeholders than brainstorming which uses a relatively small group.

Limitations are as follows:

- it is time-consuming for the facilitator to obtain multiple opinions in this way;
- bias is tolerated and not removed through group discussion;
- the triggering of imagination which is a feature of brainstorming may not be achieved.

B.3 Delphi technique

B.3.1 Overview

The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts. Although the term is often now broadly used to mean any form of brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts expressed their opinions individually and anonymously while having access to the other expert’s views as the process progresses.

B.3.2 Use

The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

B.3.3 Inputs

A set of options for which consensus is needed.

B.3.4 Process

A group of experts are questioned using a semi-structured questionnaire. The experts do not meet so their opinions are independent.

The procedure is as follows:

- formation of a team to undertake and monitor the Delphi process;

- selection of a group of experts (may be one or more panels of experts);
- development of round 1 questionnaire;
- testing the questionnaire;
- sending the questionnaire to panellists individually;
- information from the first round of responses is analysed and combined and re-circulated to panellists;
- panellists respond and the process is repeated until consensus is reached.

B.3.5 Outputs

Convergence toward consensus on the matter in hand.

B.3.6 Strengths and limitations

Strengths include:

- as views are anonymous, unpopular opinions are more likely to be expressed;
- all views have equal weight, which avoids the problem of dominating personalities;
- achieves ownership of outcomes;
- people do not need to be brought together in one place at one time.

Limitations include:

- it is labour intensive and time consuming;
- participants need to be able to express themselves clearly in writing.

B.4 Check-lists

B.4.1 Overview

Check-lists are lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.

B.4.2 Use

A check-list can be used to identify hazards and risks or to assess the effectiveness of controls. They can be used at any stage of the life cycle of a product, process or system. They may be used as part of other risk assessment techniques but are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems has been applied.

B.4.3 Inputs

Prior information and expertise on the issue, such that a relevant and preferably validated check-list can be selected or developed.

B.4.4 Process

The procedure is as follows:

- the scope of the activity is defined;
- a check-list is selected which adequately covers the scope. Check-lists need to be carefully selected for the purpose. For example a check-list of standard controls cannot be used to identify new hazards or risks;

- the person or team using the check-list steps through each element of the process or system and reviews whether items on the check-list are present.

B.4.5 Outputs

Outputs depend on the stage of the risk management process at which they are applied. For example output may be a list of controls which are inadequate or a list of risks.

B.4.6 Strengths and limitations

Strengths of check-lists include:

- they may be used by non experts;
- when well designed, they combine wide ranging expertise into an easy to use system;
- they can help ensure common problems are not forgotten.

Limitations include:

- they tend to inhibit imagination in the identification of risks;
- they address the ‘known known’s’, not the ‘known unknown’s or the ‘unknown unknowns’.
- they encourage ‘tick the box’ type behaviour;
- they tend to be observation based, so miss problems that are not readily seen.

B.5 Preliminary hazard analysis (PHA)

B.5.1 Overview

PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system.

B.5.2 Use

It is most commonly carried out early in the development of a project when there is little information on design details or operating procedures and can often be a precursor to further studies or to provide information for specification of the design of a system. It can also be useful when analysing existing systems for prioritizing hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

B.5.3 Inputs

Inputs include:

- information on the system to be assessed;
- such details of the design of the system as are available and relevant.

B.5.4 Process

A list of hazards and generic hazardous situations and risks is formulated by considering characteristics such as:

- materials used or produced and their reactivity;
- equipment employed;
- operating environment;
- layout;
- interfaces among system components, etc.

Qualitative analysis of consequences of an unwanted event and their probabilities may be carried out to identify risks for further assessment.

PHA should be updated during the phases of design, construction and testing in order to detect any new hazards and make corrections, if necessary. The results obtained may be presented in different ways such as tables and trees.

B.5.5 Outputs

Outputs include:

- a list of hazards and risks;
- recommendations in the form of acceptance, recommended controls, design specification or requests for more detailed assessment.

B.5.6 Strengths and limitations

Strengths include:

- that it is able to be used when there is limited information;
- it allows risks to be considered very early in the system lifecycle.

Limitations include:

- a PHA provides only preliminary information; it is not comprehensive, neither does it provide detailed information on risks and how they can best be prevented.

B.6 HAZOP

B.6.1 Overview

HAZOP is the acronym for **HA**Zard and **OP**erability study and, is a structured and systematic examination of a planned or existing product, process, procedure or system. It is a technique to identify risks to people, equipment, environment and/or organizational objectives. The study team is also expected, where possible, to provide a solution for treating the risk.

The HAZOP process is a qualitative technique based on use of guide words which question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure or system. It is generally carried out by a multi-disciplinary team during a set of meetings.

HAZOP is similar to FMEA in that it identifies failure modes of a process, system or procedure their causes and consequences. It differs in that the team considers unwanted outcomes and deviations from intended outcomes and conditions and works back to possible causes and failure modes, whereas FMEA starts by identifying failure modes.

B.6.2 Use

The HAZOP technique was initially developed to analyse chemical process systems, but has been extended to other types of systems and complex operations. These include mechanical and electronic systems, procedures, and software systems, and even to organizational changes and to legal contract design and review.

The HAZOP process can deal with all forms of deviation from design intent due to deficiencies in the design, component(s), planned procedures and human actions.

It is widely used for software design review. When applied to safety critical instrument control and computer systems it may be known as CHAZOP (**C**ontrol **HA**zards and **OP**erability Analysis or computer hazard and operability analysis).

A HAZOP study is usually undertaken at the detail design stage, when a full diagram of the intended process is available, but while design changes are still practicable. It may however, be carried out in a phased approach with different guidewords for each stage as a design develops in detail. A HAZOP study may also be carried out during operation but required changes can be costly at that stage.

B.6.3 Inputs

Essential inputs to a HAZOP study include current information about the system, the process or procedure to be reviewed and the intention and performance specifications of the design. The inputs may include: drawings, specification sheets, flow sheets, process control and logic diagrams, layout drawings, operating and maintenance procedures, and emergency response procedures. For non-hardware related HAZOP the inputs can be any document that describes functions and elements of the system or procedure under study. For example, inputs can be organizational diagrams and role descriptions, a draft contract or even a draft procedure.

B.6.4 Process

HAZOP takes the “design” and specification of the process, procedure or system being studied and reviews each part of it to discover what deviations from the intended performance can occur, what are the potential causes and what are the likely consequences of a deviation. This is achieved by systematically examining how each part of the system, process or procedure will respond to changes in key parameters by using suitable guidewords. Guidewords can be customized to a particular system, process or procedure or generic words can be used that encompass all types of deviation. Table B.1 provides examples of commonly used guidewords for technical systems. Similar guidewords such as ‘too early’, ‘too late’, ‘too much’, ‘too little’, ‘too long’, ‘too short’, ‘wrong direction’, on ‘wrong object’, ‘wrong action’ can be used to identify human error modes.

The normal steps in a HAZOP study include:

- nomination of a person with the necessary responsibility and authority to conduct the HAZOP study and to ensure that any actions arising from the study are completed;
- definition of the objectives and scope of the study;
- establishing a set of key or guidewords for the study;
- defining a HAZOP study team; this team is usually multidisciplinary and should include design and operations personnel with appropriate technical expertise to evaluate the effects of deviations from intended or current design. It is recommended that the team include persons not directly involved in the design or the system, process or procedure under review;
- collection of the required documentation.

Within a facilitated workshop with the study team:

- splitting the system, process or procedure into smaller elements or sub-systems or sub-processes or sub-elements to make the review tangible;
- agreeing the design intent for each subsystem, sub-process or sub-element and then for each item in that subsystem or element applying the guidewords one after the other to postulate possible deviations which will have undesirable outcomes;
- where an undesirable outcome is identified, agreeing the cause and consequences in each case and suggesting how they might be treated to prevent them occurring or mitigate the consequences if they do;
- documenting the discussion and agreeing specific actions to treat the risks identified.

Table B.1 – Example of possible HAZOP guidewords

Terms	Definitions
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase in output or in the operating condition
Less (lower)	Quantitative decrease
As well as	Quantitative increase (e.g. additional material)
Part of	Quantitative decrease (e.g. only one or two components in a mixture)
Reverse /opposite	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow or wrong material)
Compatibility	Material; environment
Guide words are applied to parameters such as	
	Physical properties of a material or process
	Physical conditions such as temperature, speed
	A specified intention of a component of a system or design (e.g. information transfer)
	Operational aspects

B.6.5 Outputs

Minutes of the HAZOP meeting(s) with items for each review point recorded. This should include: the guide word used, the deviation(s), possible causes, actions to address the identified problems and person responsible for the action.

For any deviation that cannot be corrected, then the risk for the deviation should be assessed.

B.6.6 Strengths and limitations

A HAZOP analysis offers the following advantages:

- it provides the means to systematically and thoroughly examine a system, process or procedure;
- it involves a multidisciplinary team including those with real-life operational experience and those who may have to carry out treatment actions;
- it generates solutions and risk treatment actions;
- it is applicable to a wide range of systems, processes and procedures;
- it allows explicit consideration of the causes and consequences of human error;
- it creates a written record of the process which can be used to demonstrate due diligence.

The limitations include:

- a detailed analysis can be very time-consuming and therefore expensive;
- a detailed analysis requires a high level of documentation or system/process and procedure specification;
- it can focus on finding detailed solutions rather than on challenging fundamental assumptions (however, this can be mitigated by a phased approach);
- the discussion can be focused on detail issues of design, and not on wider or external issues;

- it is constrained by the (draft) design and design intent, and the scope and objectives given to the team;
- the process relies heavily on the expertise of the designers who may find it difficult to be sufficiently objective to seek problems in their designs.

B.6.7 Reference document

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

B.7 Hazard analysis and critical control points (HACCP)

B.7.1 Overview

Hazard analysis and critical control point (HACCP) provides a structure for identifying hazards and putting controls in place at all relevant parts of a process to protect against the hazards and to maintain the quality reliability and safety of a product. HACCP aims to ensure that risks are minimized by controls throughout the process rather than through inspection of the end product.

B.7.2 Use

HACCP was developed to ensure food quality for the NASA space program. It is now used by organizations operating anywhere within the food chain to control risks from physical, chemical or biological contaminants of food. It has also been extended for use in manufacture of pharmaceuticals and to medical devices. The principle of identifying things which can influence product quality, and defining points in a process where critical parameters can be monitored and hazards controlled, can be generalized to other technical systems.

B.7.3 Inputs

HACCP starts from a basic flow diagram or process diagram and information on hazards which might affect the quality, safety or reliability of the product or process output. Information on the hazards and their risks and ways in which they can be controlled is an input to HACCP.

B.7.4 Process

HACCP consists of the following seven principles:

- identifies hazards and preventive measures related to such hazards;
- determines the points in the process where the hazards can be controlled or eliminated (the critical control points or CCPs);
- establishes critical limits needed to control the hazards, i.e. each CCP should operate within specific parameters to ensure the hazard is controlled;
- monitors the critical limits for each CCP at defined intervals;
- establishes corrective actions if the process falls outside established limits;
- establishes verification procedures;
- implements record keeping and documentation procedures for each step.

B.7.5 Outputs

Documented records including a hazard analysis worksheet and a HACCP **plan**.

The hazard analysis worksheet lists for each step of the process:

- hazards which could be introduced, controlled or exacerbated at this step;

- whether the hazards present a significant risk (based on consideration of consequence and probability from a combination of experience, data and technical literature);
- a justification for the significance;
- possible preventative measures for each hazard;
- whether monitoring or control measures can be applied at this step (i.e. is it a CCP?).

The HACCP plan delineates the procedures to be followed to assure the control of a specific design, product, process or procedure. The plan includes a list of all CCPs and for each CCP:

- the critical limits for preventative measures;
- monitoring and continuing control activities (including what, how, and when monitoring will be carried out and by whom);
- corrective actions required if deviations from critical limits are detected;
- verification and record-keeping activities.

B.7.6 Strengths and limitations

Strengths include:

- a structured process that provides documented evidence for quality control as well as identifying and reducing risks;
- a focus on the practicalities of how and where, in a process, hazards can be prevented and risks controlled;
- better risk control throughout the process rather than relying on final product inspection;
- an ability to identify hazards introduced through human actions and how these can be controlled at the point of introduction or subsequently.

Limitations include:

- HACCP requires that hazards are identified, the risks they represent defined, and their significance understood as inputs to the process. Appropriate controls also need to be defined. These are required in order to specify critical control points and control parameters during HACCP and may need to be combined with other tools to achieve this;
- taking action when control parameters exceed defined limits may miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.7.7 Reference document

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

B.8 Toxicity assessment

B.8.1 Overview

Environmental risk assessment is used here to cover the process followed in assessing risks to plants, animals and humans as a result of exposure to a range of environmental hazards. Risk management refers to decision-making steps including risk evaluation and risk treatment.

The method involves analysing the hazard or source of harm and how it affects the target population, and the pathways by which the hazard can reach a susceptible target population. This information is then combined to give an estimate of the likely extent and nature of harm.

B.8.2 Use

The process is used to assess risks to plants, animals and humans as a result of exposure to hazards such as chemicals, micro-organisms or other species.

Aspects of the methodology, such as pathway analysis which explore different routes by which a target might be exposed to a source of risk, can be adapted and used across a very wide range of different risk areas, outside human health and the environment, and is useful in identifying treatments to reduce risk.

B.8.3 Inputs

The method requires good data on the nature and properties of hazards, the susceptibilities of the target population (or populations) and the way in which the two interact. This data is normally based on research which may be laboratory based or epidemiological.

B.8.4 Process

The procedure is as follows:

a) Problem formulation – this includes setting the scope of the assessment by defining the range of target populations and hazard types of interest;

b) Hazard identification – this involves identifying all possible sources of harm to the target population from hazards within the scope of the study. Hazard identification normally relies on expert knowledge and a review of literature;

c) Hazard analysis – this involves understanding the nature of the hazard and how it interacts with the target. For example, in considering human exposure to chemical effects, the hazard might include acute and chronic toxicity, the potential to damage DNA, or the potential to cause cancer or birth defects. For each hazardous effect, the magnitude of the effect (the response) is compared to the amount of hazard to which the target is exposed (the dose) and, wherever possible, the mechanism by which the effect is produced is determined. The levels at which there is No Observable Effect (NOEL) and no Observable Adverse Effect (NOAEL) are noted. These are sometimes used as criteria for acceptability of the risk.

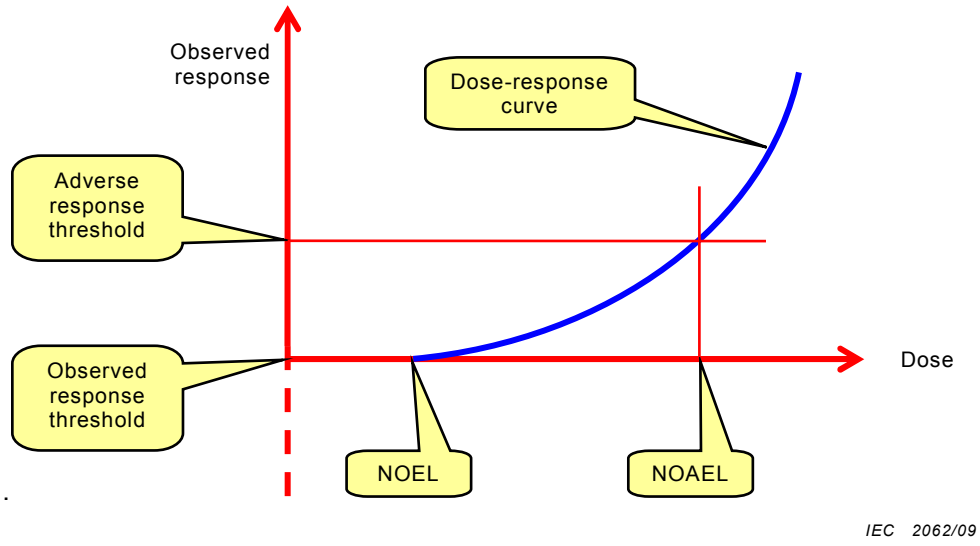

Figure B.1 – Dose-response curve

For chemical exposure, test results are used to derive dose-response curves such as that shown schematically in Figure B.1. These are usually derived from tests on animals or from experimental systems such as cultured tissues or cells.

Effects of other hazards such as micro-organisms or introduced species may be determined from field data and epidemiological studies. The nature of the interaction of diseases or pests with the target is determined and the probability that a particular level of harm from a particular exposure to the hazard is estimated.

d) Exposure analysis – this step examines how a hazardous substance or its residues might reach a susceptible target population and in what amount. It often involves a pathway analysis which considers the different routes the hazard might take, the barriers which might prevent it from reaching the target and the factors that might influence the level of exposure. For example, in considering the risk from chemical spraying the exposure analysis would consider how much chemical was sprayed, in what way and under what conditions, whether there was any direct exposure of humans or animals, how much might be left as residue on plant life, the environmental fate of pesticides reaching the ground, whether it can accumulate in animals or whether it enters groundwater. In bio security, the pathway analysis might consider how any pests entering the country might enter the environment, become established and spread.

e) Risk characterization – in this step, the information from the hazard analysis and the exposure analysis are brought together to estimate the probabilities of particular consequences when effects from all pathways are combined. Where there are large numbers of hazards or pathways, an initial screening may be carried out and the detailed hazard and exposure analysis and risk characterization carried out on the higher risk scenarios.

B.8.5 Outputs

The output is normally an indication of the level of risk from exposure of a particular target to a particular hazard in the context concerned. The risk may be expressed quantitatively semi-quantitatively or qualitatively. For example, the risk of cancer is often expressed quantitatively as the probability, that a person will develop cancer over a specified period given a specified exposure to a contaminant. Semi-quantitative analysis may be used to derive a risk index for a particular contaminant or pest and qualitative output may be a level of risk (e.g. high, medium, low) or a description with practical data of likely effects.

B.8.6 Strengths and limitations

The strength of this analysis is that it provides a very detailed understanding of the nature of the problem and the factors which increase risk.

Pathway analysis is a useful tool, generally, for all areas of risk and permits the identification of how and where it may be possible to improve controls or introduce new ones.

It does, however, need good data which is often not available or has a high level of uncertainty associated with it. For example, dose response curves derived from exposing animals to high levels of a hazard should be extrapolated to estimate the effects of very low levels of the contaminants to humans and there are multiple models by which this is achieved. Where the target is the environment rather than humans and the hazard is not chemical, data which is directly relevant to the particular conditions of the study may be limited.

B.9 Structured “What-if” Technique (SWIFT)

B.9.1 Overview

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team-based study, utilizing a set of ‘prompt’ words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard ‘what-if’ type phrases in combination with the prompts to investigate how a system, plant item,

organization or procedure will be affected by deviations from normal operations and behaviour. SWIFT is normally applied at more of a systems level with a lower level of detail than HAZOP.

B.9.2 Use

While SWIFT was originally designed for chemical and petrochemical plant hazard study, the technique is now widely applied to systems, plant items, procedures, organizations generally. In particular it is used to examine the consequences of changes and the risks thereby altered or created.

B.9.3 Inputs

The system, procedure, plant item and/or change has to be carefully defined before the study can commence. Both the external and internal contexts are established through interviews and through the study of documents, plans and drawings by the facilitator. Normally, the item, situation or system for study is split into nodes or key elements to facilitate the analysis process but this rarely occurs at the level of definition required for HAZOP.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience of similar items, systems, changes or situations.

B.9.4 Process

The general process is as follows:

a) Before the study commences, the facilitator prepares a suitable prompt list of words or phrases that may be based on a standard set or be created to enable a comprehensive review of hazards or risks.

b) At the workshop the external and internal context of the item, system, change or situation and the scope of the study are discussed and agreed.

c) The facilitator asks the participants to raise and discuss:
   - known risks and hazards;
   - previous experience and incidents;
   - known and existing controls and safeguards;
   - regulatory requirements and constraints.

d) Discussion is facilitated by creating a question using a ‘what-if’ phrase and a prompt word or subject. The ‘what-if’ phrases to be used are “what if…”, “what would happen if…”, “could someone or something…”, “has anyone or anything ever….” The intent is to stimulate the study team into exploring potential scenarios, their causes and consequences and impacts.

e) Risks are summarized and the team considers controls in place.

f) The description of the risk, its causes, consequences and expected controls are confirmed with the team and recorded.

g) The team considers whether the controls are adequate and effective and agree a statement of risk control effectiveness. If this is less than satisfactory, the team further considers risk treatment tasks and potential controls are defined.

h) During this discussion further ‘what-if’ questions are posed to identify further risks.

i) The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss.

j) It is normal to use a qualitative or semi-quantitative risk assessment method to rank the actions created in terms of priority. This risk assessment is normally conducted by taking into account the existing controls and their effectiveness.

B.9.5 Outputs

Outputs include a risk register with risk-ranked actions or tasks. These tasks can then become the basis for a treatment plan.

B.9.6 Strengths and limitations

Strengths of SWIFT:

- it is widely applicable to all forms of physical plant or system, situation or circumstance, organization or activity;
- it needs minimal preparation by the team;
- it is relatively rapid and the major hazards and risks quickly become apparent within the workshop session;
- the study is 'systems orientated' and allows participants to look at the system response to deviations rather than just examining the consequences of component failure;
- it can be used to identify opportunities for improvement of processes and systems and generally can be used to identify actions that lead to and enhance their probabilities of success;
- involvement in the workshop by those who are accountable for existing controls and for further risk treatment actions, reinforces their responsibility;
- it creates a risk register and risk treatment plan with little more effort;
- while often a qualitative or semi-quantitative form of risk rating is used for risk assessment and to prioritize attention on the resulting actions, SWIFT can be used to identify risks and hazards that can be taken forward into a quantitative study.

Limitations of SWIFT:

- it needs an experienced and capable facilitator to be efficient;
- careful preparation is needed so that the workshop team's time is not wasted;
- if the workshop team does not have a wide enough experience base or if the prompt system is not comprehensive, some risks or hazards may not be identified;
- the high-level application of the technique may not reveal complex, detailed or correlated causes.

B.10 Scenario analysis

B.10.1 Overview

Scenario analysis is a name given to the development of descriptive models of how the future might turn out. It can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting (for example) 'best case', 'worst case' and 'expected case' may be used to analyse potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risk.

The power of scenario analysis is illustrated by considering major shifts over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable changes.

B.10.2 Use

Scenario analysis can be used to assist in making policy decisions and planning future strategies as well as to consider existing activities. It can play a part in all three components of risk assessment. For identification and analysis, sets of scenarios reflecting (for example) best case, worst case and 'expected' case may be used to identify what might happen under

particular circumstances and analyse potential consequences and their probabilities for each scenario.

Scenario analysis may be used to anticipate how both threats and opportunities might develop and may be used for all types of risk with both short and long term time frames. With short time frames and good data, likely scenarios may be extrapolated from the present. For longer time frames or with weak data, scenario analysis becomes more imaginative and may be referred to as futures analysis.

Scenario analysis may be useful where there are strong distributional differences between positive outcomes and negative outcomes in space, time and groups in the community or an organization.

B.10.3 Inputs

The prerequisite for a scenario analysis is a team of people who between them have an understanding of the nature of relevant changes (for example possible advances in technology) and imagination to think into the future without necessarily extrapolating from the past. Access to literature and data about changes already occurring is also useful.

B.10.4 Process

The structure for scenario analysis may be informal or formal.

Having established a team and relevant communication channels, and defined the context of the problem and issues to be considered, the next step is to identify the nature of changes that might occur. This will need research into the major trends and the probable timing of changes in trends as well as imaginative thinking about the future.

Changes to be considered may include:

- external changes (such as technological changes);
- decisions that need to be made in the near future but which may have a variety of outcomes;
- stakeholder needs and how they might change;
- changes in the macro environment (regulatory, demographics, etc). Some will be inevitable and some will be uncertain.

Sometimes, a change may be due to the consequences of another risk. For example, the risk of climate change is resulting in changes in consumer demand related to food miles. This will influence which foods can be profitably exported as well as which foods can be grown locally.

The local and macro factors or trends can now be listed and ranked for (1) importance (2) uncertainty. Special attention is paid to the factors that are most important and most uncertain. Key factors or trends are mapped against each other to show areas where scenarios can be developed.

A series of scenarios is proposed with each one focussing on a plausible change in parameters.

A “story” is then written for each scenario that tells how you might move from here towards the subject scenario. The stories may include plausible details that add value to the scenarios.

The scenarios can then be used to test or evaluate the original question. The test takes into account any significant but predictable factors (e.g. use patterns), and then explores how ‘successful’ the policy (activity) would be in this new scenario, and ‘pre-tests’ outcomes by using ‘what if’ questions based on model assumptions.

When the question or proposal has been evaluated with respect to each scenario, it may be obvious that it needs to be modified to make it more robust or less risky. It should also be possible to identify some leading indicators that show when change is occurring. Monitoring and responding to leading indicators can provide opportunity for change in planned strategies.

Since scenarios are only defined 'slices' of possible futures, it is important to make sure that account is taken of the probability of a particular outcome (scenario) occurring, i.e. to adopt a risk framework. For example, where best case, worst case and expected case scenarios are used, some attempt should be made to qualify, or express the probability of each scenario occurring.

B.10.5 Outputs

There may be no best-fit scenario but one should end with a clearer perception of the range of options and how to modify the chosen course of action as indicators move.

B.10.6 Strengths and limitations

Scenario analysis takes account of a range of possible futures which may be preferable to the traditional approach of relying on high-medium-low forecasts that assume, through the use of historical data, that future events will probably continue to follow past trends. This is important for situations where there is little current knowledge on which to base predictions or where risks are being considered in the longer term future.

This strength however has an associated weakness which is that where there is high uncertainty some of the scenarios may be unrealistic.

The main difficulties in using scenario analysis are associated with the availability of data, and the ability of the analysts and decision makers to be able to develop realistic scenarios that are amenable to probing of possible outcomes.

The dangers of using scenario analysis as a decision-making tool are that the scenarios used may not have an adequate foundation; that data may be speculative; and that unrealistic results may not be recognized as such.

B.11 Business impact analysis (BIA)

B.11.1 Overview

Business impact analysis, also known as business impact assessment, analyses how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

- the identification and criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization;
- how disruptive events will affect the capacity and capability of achieving critical business objectives;
- the capacity and capability needed to manage the impact of a disruption and recover the organization to agreed levels of operation.

B.11.2 Use

BIA is used to determine the criticality and recovery timeframes of processes and associated resources (people, equipment, information technology) to ensure the continued achievement of objectives. Additionally, the BIA assists in determining interdependencies and interrelationships between processes, internal and external parties and any supply chain linkages.

B.11.3 Inputs

Inputs include:

- a team to undertake the analysis and develop a plan;
- information concerning the objectives, environment, operations and interdependencies of the organization;
- details on the activities and operations of the organization, including processes, supporting resources, relationships with other organizations, outsourced arrangements, stakeholders;
- financial and operational consequences of loss of critical processes;
- prepared questionnaire;
- list of interviewees from relevant areas of the organization and/or stakeholders that will be contacted.

B.11.4 Process

A BIA can be undertaken using questionnaires, interviews, structured workshops or combinations of all three, to obtain an understanding of the critical processes, the effects of the loss of those processes and the required recovery timeframes and supporting resources.

The key steps include:

- based on the risk and vulnerability assessment, confirmation of the key processes and outputs of the organization to determine the criticality of the processes;
- determination of the consequences of a disruption on the identified critical processes in financial and/or operational terms, over defined periods;
- identification of the interdependencies with key internal and external stakeholders. This could include mapping the nature of the interdependencies through the supply chain;
- determination of the current available resources and the essential level of resources needed to continue to operate at a minimum acceptable level following a disruption;
- identification of alternate workarounds and processes currently in use or planned to be developed. Alternate workarounds and processes may need to be developed where resources or capability are inaccessible or insufficient during the disruption;
- determination of the maximum acceptable outage time (MAO) for each process based on the identified consequences and the critical success factors for the function. The MAO represents the maximum period of time the organization can tolerate the loss of capability;
- determination of the recovery time objective(s) (RTO) for any specialized equipment or information technology. The RTO represents the time within which the organization aims to recover the specialized equipment or information technology capability;
- confirmation of the current level of preparedness of the critical processes to manage a disruption. This may include evaluating the level of redundancy within the process (e.g. spare equipment) or the existence of alternate suppliers.

B.11.5 Outputs

The outputs are as follows:

- a priority list of critical processes and associated interdependencies;
- documented financial and operational impacts from a loss of the critical processes;
- supporting resources needed for the identified critical processes;
- outage time frames for the critical process and the associated information technology recovery time frames.

B.11.6 Strengths and limitations

Strengths of the BIA include:

- an understanding of the critical processes that provide the organization with the ability to continue to achieve their stated objectives;
- an understanding of the required resources;
- an opportunity to redefine the operational process of an organization to assist in the resilience of the organization.

Limitations include:

- lack of knowledge by the participants involved in completing questionnaires, undertaking interviews or workshops;
- group dynamics may affect the complete analysis of a critical process;
- simplistic or over-optimistic expectations of recovery requirements;
- difficulty in obtaining an adequate level of understanding of the organization's operations and activities.

B.12 Root cause analysis (RCA)

B.12.1 Overview

The analysis of a major loss to prevent its reoccurrence is commonly referred to as Root Cause Analysis (RCA), Root Cause Failure Analysis (RCFA) or loss analysis. RCA is focused on asset losses due to various types of failures while loss analysis is mainly concerned with financial or economic losses due to external factors or catastrophes. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyse losses on a more global basis to determine where improvements can be made.

B.12.2 Use

RCA is applied in various contexts with the following broad areas of usage:

- safety-based RCA is used for accident investigations and occupational health and safety;
- failure analysis is used in technological systems related to reliability and maintenance;
- production-based RCA is applied in the field of quality control for industrial manufacturing;
- process-based RCA is focused on business processes;
- system-based RCA has developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

B.12.3 Inputs

The basic input to an RCA is all of the evidence gathered from the failure or loss. Data from other similar failures may also be considered in the analysis. Other inputs may be results that are carried out to test specific hypotheses.

B.12.4 Process

When the need for an RCA is identified, a group of experts is appointed to carry out the analysis and make recommendations. The type of expert will mostly be dependent on the specific expertise needed to analyse the failure.

Even though different methods can be used to perform the analysis, the basic steps in executing an RCA are similar and include:

- forming the team;
- establishing the scope and objectives of the RCA;
- gathering data and evidence from the failure or loss;
- performing a structured analysis to determine the root cause;
- developing solutions and make recommendations;
- implementing the recommendations;
- verifying the success of the implemented recommendations.

Structured analysis techniques may consist of one of the following:

- "5 whys" technique, i.e. repeatedly asking 'why?' to peel away layers of cause and sub cause);
- failure mode and effects analysis;
- fault tree analysis;
- Fishbone or Ishikawa diagrams;
- Pareto analysis;
- root cause mapping.

The evaluation of causes often progresses from initially evident physical causes to human-related causes and finally to underlying management or fundamental causes. Causal factors have to be able to be controlled or eliminated by involved parties in order for corrective action to be effective and worthwhile.

B.12.5 Outputs

The outputs from an RCA include:

- documentation of data and evidence gathered;
- hypotheses considered;
- conclusion about the most likely root causes for the failure or loss;
- recommendations for corrective action.

B.12.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- documentation of results;
- need to produce final recommendations.

Limitations of an RCA:

- required experts may not be available;
- critical evidence may be destroyed in the failure or removed during clean-up;
- the team may not be allowed enough time or resources to fully evaluate the situation;
- it may not be possible to adequately implement recommendations.

B.13 Failure modes and effects analysis (FMEA) and failure modes and effects and criticality analysis (FMECA)

B.13.1 Overview

Failure modes and effects analysis (FMEA) is a technique used to identify the ways in which components, systems or processes can fail to fulfil their design intent.

FMEA identifies:

- all potential failure modes of the various parts of a system (a failure mode is what is observed to fail or to perform incorrectly);
- the effects these failures may have on the system;
- the mechanisms of failure;
- how to avoid the failures, and/or mitigate the effects of the failures on the system.

FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality

This criticality analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

B.13.2 Use

There are several applications of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA.

FMEA/FMECA may be applied during the design, manufacture or operation of a physical system.

To improve dependability, however, changes are usually more easily implemented at the design stage. FMEA AND FMECA may also be applied to processes and procedures. For example, it is used to identify potential for medical error in healthcare systems and failures in maintenance procedures.

FMEA/FMECA can be used to

- assist in selecting design alternatives with high dependability,
- ensure that all failure modes of systems and processes, and their effects on operational success have been considered,
- identify human error modes and effects,
- provide a basis for planning testing and maintenance of physical systems,
- improve the design of procedures and processes,
- provide qualitative or quantitative information for analysis techniques such as fault tree analysis.

FMEA and FMECA can provide input to other analyses techniques such as fault tree analysis at either a qualitative or quantitative level.

B.13.3 Inputs

FMEA and FMECA need information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail. For a detailed Design FMEA the element may be at the detailed individual component level, while for higher level Systems FMEA, elements may be defined at a higher level.

Information may include:

- drawings or a flow chart of the system being analysed and its components, or the steps of a process;
- an understanding of the function of each step of a process or component of a system;
- details of environmental and other parameters, which may affect operation;
- an understanding of the results of particular failures;
- historical information on failures including failure rate data where available.

B.13.4 Process

The FMEA process is as follows:

a) define the scope and objectives of the study;
b) assemble the team;
c) understand the system/process to be subjected to the FMECA;
d) breakdown of the system into its components or steps;
e) define the function of each step or component;
f) for every component or step listed identify:
   - how can each part conceivably fail?
   - what mechanisms might produce these modes of failure?
   - what could the effects be if the failures did occur?
   - is the failure harmless or damaging?
   - how is the failure detected?
g) identify inherent provisions in the design to compensate for the failure.

For FMECA, the study team goes on to classify each of the identified failure modes according to its criticality

There are several ways this may be done. Common methods include

- the mode criticality index,
- the level of risk,
- the risk priority number.

The model criticality is a measure of the probability that the mode being considered will result in failure of the system as a whole; it is defined as:

Failure effect probability * Mode failure rate * Operating time of the system

It is most often applied to equipment failures where each of these terms can be defined quantitatively and failure modes all have the same consequence.

The risk level is obtained by combining the consequences of a failure mode occurring with the probability of failure. It is used when consequences of different failure modes differ and can be applied to equipment systems or processes. Risk level can be expressed qualitatively, semi-quantitatively or quantitatively.

The risk priority number (RPN) is a semi-quantitative measure of criticality obtained by multiplying numbers from rating scales (usually between 1 and 10) for consequence of failure, likelihood of failure and ability to detect the problem. (A failure is given a higher priority if it is difficult to detect.) This method is used most often in quality assurance applications

Once failure modes and mechanisms are identified, corrective actions can be defined and implemented for the more significant failure modes.

FMEA is documented in a report that contains:

- details of the system that was analysed;
- the way the exercise was carried out;
- assumptions made in the analysis;
- sources of data;
- the results, including the completed worksheets;
- the criticality (if completed) and the methodology used to define it;
- any recommendations for further analyses, design changes or features to be incorporated in test plans, etc.

The system may be reassessed by another cycle of FMEA after the actions have been completed.

B.13.5 Outputs

The primary output of FMEA is a list of failure modes, the failure mechanisms and effects for each component or step of a system or process (which may include information on the likelihood of failure). Information is also given on the causes of failure and the consequences to the system as a whole. The output from FMECA includes a rating of importance based on the likelihood that the system will fail, the level of risk resulting from the failure mode or a combination of the level of risk and the 'detectability' of the failure mode.

FMECA can give a quantitative output if suitable failure rate data and quantitative consequences are used.

B.13.6 Strengths and limitations

The strengths of FMEA/FMECA are as follows:

- widely applicable to human, equipment and system failure modes and to hardware, software and procedures;
- identify component failure modes, their causes and their effects on the system, and present them in an easily readable format;
- avoid the need for costly equipment modifications in service by identifying problems early in the design process;
- identify single point failure modes and requirements for redundancy or safety systems;
- provide input to the development monitoring programmes by highlighting key features to be monitored.

Limitations include:

- they can only be used to identify single failure modes, not combinations of failure modes;
- unless adequately controlled and focussed, the studies can be time consuming and costly;
- they can be difficult and tedious for complex multi-layered systems.

B.13.7 Reference document

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Fault tree analysis (FTA)

B.14.1 Overview

FTA is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the “top event”). Causal factors are deductively identified, organized in a logical manner and represented pictorially in a tree diagram which depicts causal factors and their logical relationship to the top event.

The factors 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.

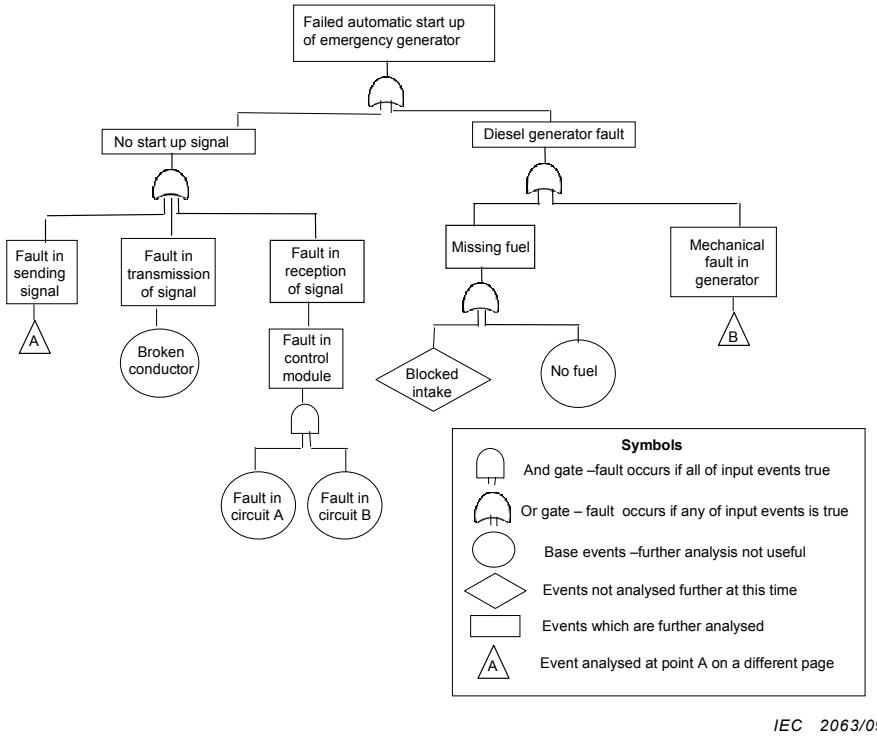

Figure B.2 – Example of an FTA from IEC 60300-3-9

B.14.2 Use

A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

It may be used at the design stage of a system to identify potential causes of failure and hence to select between different design options. It may be used at the operating phase to identify how major failures can occur and the relative importance of different pathways to the head event. A fault tree may also be used to analyse a failure which has occurred to display diagrammatically how different events came together to cause the failure.

B.14.3 Inputs

For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to aid the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state for all basic events in the fault tree are required.

B.14.4 Process

The steps for developing a fault tree are as follows:

- The top event to be analysed is defined. This may be a failure or maybe a broader outcome of that failure. Where the outcome is analysed, the tree may contain a section relating to mitigation of the actual failure.
- Starting with the top event, the possible immediate causes or failure modes leading to the top event are identified.
- Each of these causes/fault modes is analysed to identify how their failure could be caused.
- Stepwise identification of undesirable system operation is followed to successively lower system levels until further analysis becomes unproductive. In a hardware system this may be the component failure level. Events and causal factors at the lowest system level analysed are known as base events.
- Where probabilities can be assigned to base events the probability of the top event may be calculated. For quantification to be valid it must be able to be shown that, for each gate, all inputs are both necessary and sufficient to produce the output event. If this is not the case, the fault tree is not valid for probability analysis but may be a useful tool for displaying causal relationships.

As part of quantification the fault tree may need to be simplified using Boolean algebra to account for duplicate failure modes.

As well as providing an estimate of the probability of the head event, minimal cut sets, which form individual separate pathways to the head event, can be identified and their influence on the top event calculated.

Except for simple fault trees, a software package is needed to properly handle the calculations when repeated events are present at several places in the fault tree, and to calculate minimal cut sets. Software tools help ensure consistency, correctness and verifiability.

B.14.5 Outputs

The outputs from fault tree analysis are as follows:

- a pictorial representation of how the top event can occur which shows interacting pathways where two or more simultaneous events must occur;
- a list of minimal cut sets (individual pathways to failure) with (where data is available) the probability that each will occur;
- the probability of the top event.

B.14.6 Strengths and limitations

Strengths of FTA:

- It affords a disciplined approach which is highly systematic, but at the same time sufficiently flexible to allow analysis of a variety of factors, including human interactions and physical phenomena.
- The application of the "top-down" approach, implicit in the technique, focuses attention on those effects of failure which are directly related to the top event.
- FTA is especially useful for analysing systems with many interfaces and interactions.
- The pictorial representation leads to an easy understanding of the system behaviour and the factors included, but as the trees are often large, processing of fault trees may require computer systems. This feature enables more complex logical relationships to be included (e.g. NAND and NOR) but also makes the verification of the fault tree difficult.

- Logic analysis of the fault trees and the identification of cut sets is useful in identifying simple failure pathways in a very complex system where particular combinations of events which lead to the top event could be overlooked.

Limitations include:

- Uncertainties in the probabilities of base events are included in calculations of the probability of the top event. This can result in high levels of uncertainty where base event failure probabilities are not known accurately; however, a high degree of confidence is possible in a well understood system.
- In some situations, causal events are not bound together and it can be difficult to ascertain whether all important pathways to the top event are included. For example, including all ignition sources in an analysis of a fire as a top event. In this situation probability analysis is not possible.
- Fault tree is a static model; time interdependencies are not addressed.
- Fault trees can only deal with binary states (failed/not failed) only.
- While human error modes can be included in a qualitative fault tree, in general failures of degree or quality which often characterize human error cannot easily be included;
- A fault tree does not enable domino effects or conditional failures to be included easily.

B.14.7 Reference document

IEC 61025, *Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems*

B.15 Event tree analysis (ETA)

B.15.1 Overview

ETA is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences (see Figure B.3). It can be applied both qualitatively and quantitatively.

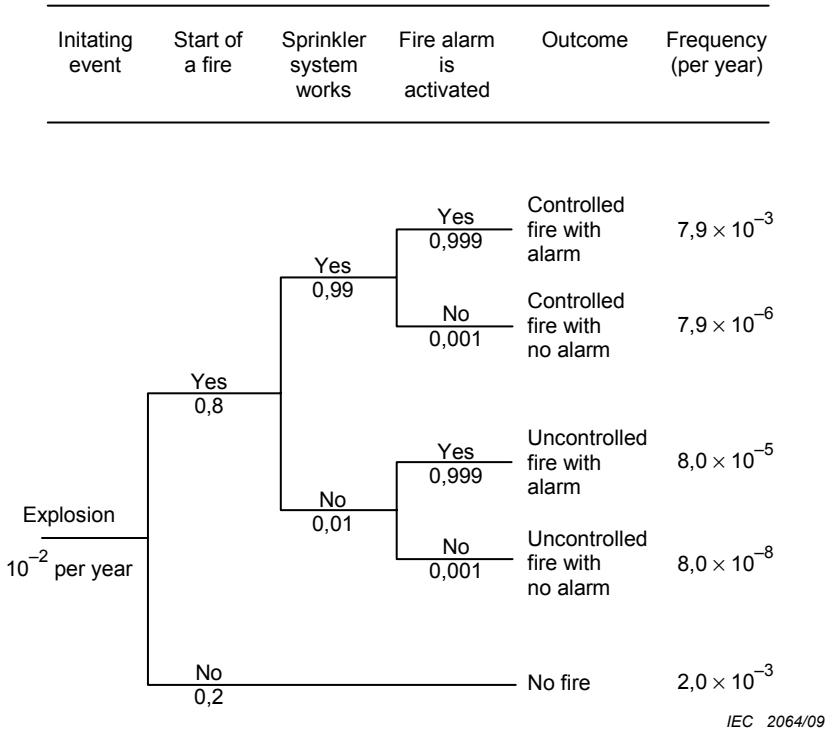

Figure B.3 – Example of an event tree

Figure B.3 shows simple calculations for a sample event tree, when branches are fully independent.

By fanning out like a tree, ETA is able to represent the aggravating or mitigating events in response to the initiating event, taking into account additional systems, functions or barriers.

B.15.2 Use

ETA can be used for modelling, calculating and ranking (from a risk point of view) different accident scenarios following the initiating event

ETA can be used at any stage in the life cycle of a product or process. It may be used qualitatively to help brainstorm potential scenarios and sequences of events following an initiating event and how outcomes are affected by various treatments, barriers or controls intended to mitigate unwanted outcomes.

The quantitative analysis lends itself to consider the acceptability of controls. It is most often used to model failures where there are multiple safeguards.

ETA can be used to model initiating events which might bring loss or gain. However, circumstances where pathways to optimize gain are sought are more often modelled using a decision tree.

B.15.3 Inputs

Inputs include:

- a list of appropriate initiating events;
- information on treatments, barriers and controls, and their failure probabilities (for quantitative analyses);
- understanding of the processes whereby an initial failure escalates.

B.15.4 Process

An event tree starts by selecting an initiating event. This may be an incident such as a dust explosion or a causal event such as a power failure. Functions or systems which are in place to mitigate outcomes are then listed in sequence. For each function or system, a line is drawn to represent their success or failure. A particular probability of failure can be assigned to each line, with this conditional probability estimated e.g. by expert judgement or a fault tree analysis. In this way, different pathways from the initiating event are modelled.

Note that the probabilities on the event tree are conditional probabilities, for example the probability of a sprinkler functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under conditions of fire caused by an explosion.

Each path through the tree represents the probability that all of the events in that path will occur. Therefore, the frequency of the outcome is represented by the product of the individual conditional probabilities and the frequency of the initiation event, given that the various events are independent.

B.15.5 Outputs

Outputs from ETA include the following:

- qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events;
- quantitative estimates of event frequencies or probabilities and relative importance of various failure sequences and contributing events;
- lists of recommendations for reducing risks;
- quantitative evaluations of recommendation effectiveness.

B.15.6 Strengths and limitations

Strengths of ETA include the following:

- ETA displays potential scenarios following an initiating event, are analysed and the influence of the success or failure of mitigating systems or functions in a clear diagrammatic way;
- it accounts for timing, dependence and domino effects that are cumbersome to model in fault trees;
- it graphically represent sequences of events which are not possible to represent when using fault trees.

Limitations include:

- in order to use ETA as part of a comprehensive assessment, all potential initiating events need to be identified. This may be done by using another analysis method (e.g. HAZOP, PHA), however, there is always a potential for missing some important initiating events;
- with event trees, only success and failure states of a system are dealt with, and it is difficult to incorporate delayed success or recovery events;
- any path is conditional on the events that occurred at previous branch points along the path. Many dependencies along the possible paths are therefore addressed. However, some dependencies, such as common components, utility systems and operators, may be overlooked if not handled carefully, may lead to optimistic estimations of risk.

B.16 Cause-consequence analysis

B.16.1 General

Cause-consequence analysis is a combination of fault tree and event tree analysis. It starts from a critical event and analyses consequences by means of a combination of YES/NO logic gates which represent conditions that may occur or failures of systems designed to mitigate the consequences of the initiating event. The causes of the conditions or failures are analysed by means of fault trees (see Clause B.15)

B.16.2 Use

Cause-consequence analysis was originally developed as a reliability tool for safety critical systems to give a more complete understanding of system failures. Like fault tree analysis, it is used to represent the failure logic leading to a critical event but it adds to the functionality of a fault tree by allowing time sequential failures to be analysed. The method also allows time delays to be incorporated into the consequence analysis which is not possible with event trees.

The method is used to analyse the various paths a system could take following a critical event and depending on the behaviour of particular subsystems (such as emergency response systems). If quantified they will give an estimate of the probability of different possible consequences following a critical event.

As each sequence in a cause-consequence diagram is a combination of sub-fault trees, the cause-consequence analysis can be used as a tool to build big fault trees.

Diagrams are complex to produce and use and tend to be used when the magnitude of the potential consequence of failure justifies intensive effort.

B.16.3 Inputs

An understanding of the system and its failure modes and failure scenarios is required.

B.16.4 Process

Figure B.4 shows a conceptual diagram of a typical cause-consequence analysis.

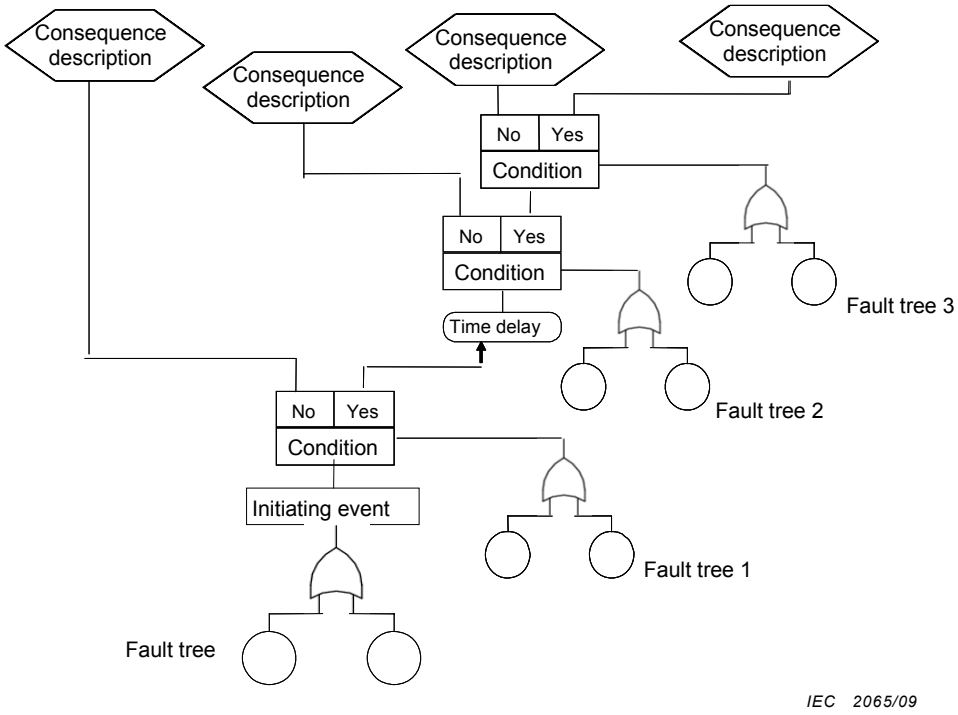

Figure B.4 – Example of cause-consequence analysis

The procedure is as follows:

a) Identify the critical (or initiating) event (equivalent to the top event of a fault tree and the initiating event of an event tree).

b) Develop and validate the fault tree for causes of the initiating event as described in Clause B.14. The same symbols are used as in conventional fault tree analysis.

c) Decide the order in which conditions are to be considered. This should be a logical sequence such as the time sequence in which they occur.

d) Construct the pathways for consequences depending on the different conditions. This is similar to an event tree but the split in pathways of the event tree is shown as a box labelled with the particular condition that applies.

e) Provided the failures for each condition box are independent, the probability of each consequence can be calculated. This is achieved by first assigning probabilities to each output of the condition box (using the relevant fault trees as appropriate) The probability of any one sequence leading to a particular consequence is obtained by multiplying the probabilities of each sequence of conditions which terminates in that particular consequence. If more than one sequence ends up with the same consequence, the probabilities from each sequence are added. If there are dependencies between failures of conditions in a sequence (for example a power failure may cause several conditions to fail) then the dependencies should be dealt with prior to calculation.

B.16.5 Output

The output of cause-consequence analysis is a diagrammatic representation of how a system may fail showing both causes and consequences. An estimation of the probability of occurrence of each potential consequence based on analysis of probabilities of occurrence of particular conditions following the critical event.

B.16.6 Strengths and limitations

The advantages of cause-consequence analysis are the same as those of event trees and fault trees combined. In addition, it overcomes some of the limitations of those techniques by

being able to analyse events that develop over time. Cause-consequence analysis provides a comprehensive view of the system.

Limitations are that it is more complex than fault tree and event tree analysis, both to construct and in the manner in which dependencies are dealt with during quantification.

B.17 Cause-and-effect analysis

B.17.1 Overview

Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. The information is organized in either a Fishbone (also called Ishikawa) or sometimes a tree diagram (see B.17.4).

B.17.2 Use

Cause-and-effect analysis provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.

It is used to enable consideration of all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes which can then be tested empirically or by evaluation of available data. It is most valuable at the beginning of an analysis to broaden thinking about possible causes and then to establish potential hypotheses that can be considered more formally.

Constructing a cause-and-effect diagram can be undertaken when there is need to:

- identify the possible root causes, the basic reasons, for a specific effect, problem or condition;
- sort out and relate some of the interactions among the factors affecting a particular process;
- analyse existing problems so that corrective action can be taken.

Benefits from constructing a cause-and-effect diagram include:

- concentrates review members' attention on a specific problem;
- to help determine the root causes of a problem using a structured approach;
- encourages group participation and utilizes group knowledge for the product or process;
- uses an orderly, easy-to-read format to diagram cause-and-effect relationships;
- indicates possible causes of variation in a process;
- identifies areas where data should be collected for further study.

Cause-and-effect analysis can be used as a method in performing root cause analysis (see Clause B.12).

B.17.3 Input

The input to a cause-and-effect analysis may come from expertise and experience from participants or a previously developed model that has been used in the past.

B.17.4 Process

The cause-and-effect analysis should be carried out by a team of experts knowledgeable with the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

- establish the effect to be analysed and place it in a box. The effect may be positive (an objective) or negative (a problem) depending on the circumstances;
- determine the main categories of causes represented by boxes in the Fishbone diagram. Typically, for a system problem, the categories might be people, equipment, environment, processes, etc. However, these are chosen to fit the particular context;
- fill in the possible causes for each major category with branches and sub-branches to describe the relationship between them;
- keep asking “why?” or “what caused that?” to connect the causes;
- review all branches to verify consistency and completeness and ensure that the causes apply to the main effect;
- identify the most likely causes based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone or Ishikawa diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone) with branches and sub-branches that describe more specific causes in those categories.

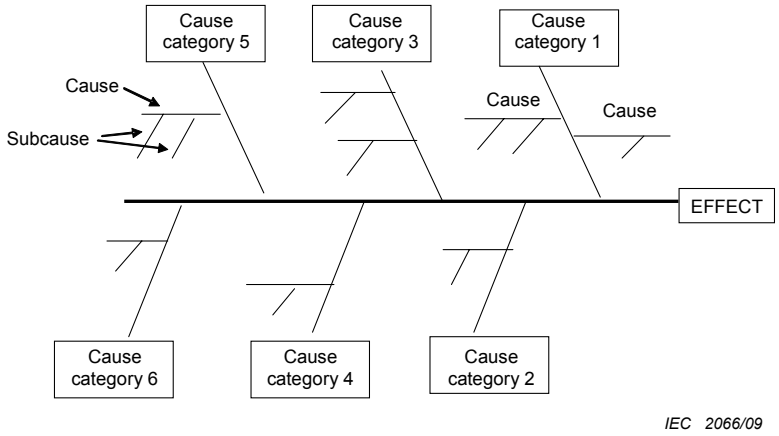

Figure B.5 – Example of Ishikawa or Fishbone diagram

The tree representation is similar to a fault tree in appearance, although it is often displayed with the tree developing from left to right rather than down the page. However, it cannot be quantified to produce a probability of the head event as the causes are possible contributory factors rather than failures with a known probability of occurrence

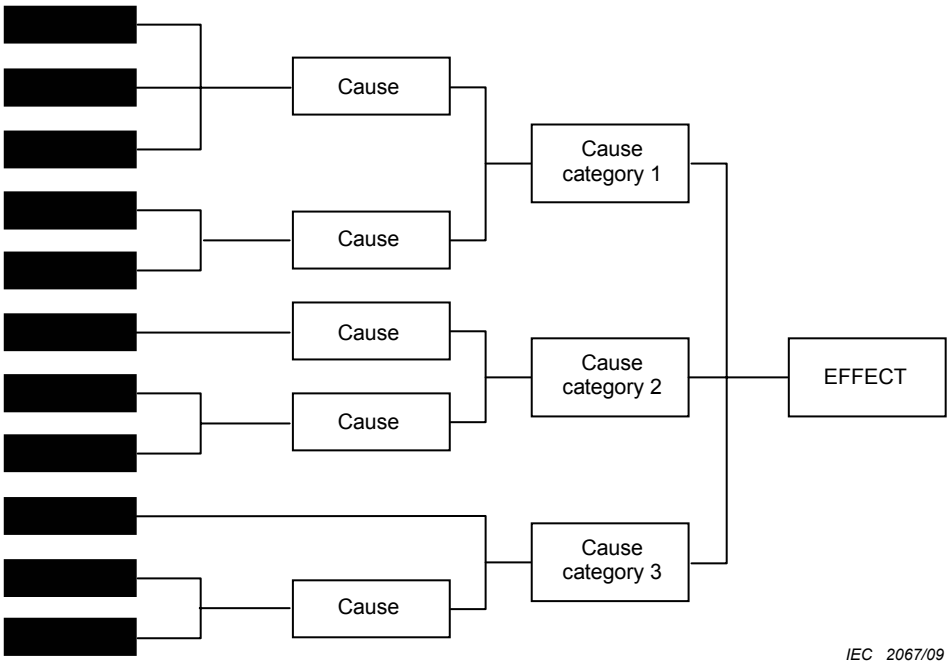

Figure B.6 – Example of tree formulation of cause-and-effect analysis

Cause-and-effect diagrams are generally used qualitatively. It is possible to assume the probability of the problem is 1 and assign probabilities to generic causes, and subsequently to the sub-causes, on the basis of the degree of belief about their relevance. However, contributory factors often interact and contribute to the effect in complex ways which make quantification invalid

B.17.5 Output

The output from a cause-and-effect analysis is a Fishbone or tree diagram that shows the possible and likely causes. This has then to be verified and tested empirically before recommendations can be made.

B.17.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- graphical easy-to-read illustration of results;
- areas identified where further data is needed;
- can be used to identify contributory factors to wanted as well as unwanted effects. Taking a positive focus on an issue can encourage greater ownership and participation.

Limitations include:

- the team may not have the necessary expertise;
- it is not a complete process in itself and needs to be a part of a root cause analysis to produce recommendations;
- it is a display technique for brainstorming rather than a separate analysis technique;
- the separation of causal factors into major categories at the start of the analysis means that interactions between the categories may not be considered adequately, e.g. where

equipment failure is caused by human error, or human problems are caused by poor design.

B.18 Layers of protection analysis (LOPA)

B.18.1 Overview

LOPA is a semi-quantitative method for estimating the risks associated with an undesired event or scenario. It analyses whether there are sufficient measures to control or mitigate the risk.

A cause-consequence pair is selected and the layers of protection which prevent the cause leading to the undesired consequence are identified. An order of magnitude calculation is carried out to determine whether the protection is adequate to reduce risk to a tolerable level.

B.18.2 Uses

LOPA may be used qualitatively simply to review the layers of protection between a hazard or causal event and an outcome. Normally a semi-quantitative approach would be applied to add more rigour to screening processes for example following HAZOP or PHA.

LOPA provides a basis for the specification of independent protection layers (IPLs) and safety integrity levels (SIL levels) for instrumented systems, as described in the IEC 61508 series and in IEC 61511, in the determination of safety integrity level (SIL) requirements for safety instrumented systems. LOPA can be used to help allocate risk reduction resources effectively by analysing the risk reduction produced by each layer of protection.

B.18.3 Inputs

Inputs to LOPA include

- basic information on risks including hazards, causes and consequences such as provided by a PHA;
- information on controls in place or proposed;
- causal event frequencies, and protection layer failure probabilities, measures of consequence and a definition of tolerable risk;
- initiating cause frequencies, protection layer failure probabilities, measures of consequence and a definition of tolerable risk.

B.18.4 Process

LOPA is carried out using a team of experts who apply the following procedure:

- identify initiating causes for an undesired outcome and seek data on their frequencies and consequences;
- select a single cause-consequence pair;
- layers of protection which prevent the cause proceeding to the undesired consequence are identified and analysed for their effectiveness;
- identify independent protection layers (IPLs) (not all layers of protection are IPLs);
- estimate the probability of failure of each IPL;
- the frequency initiating cause is combined with the probabilities of failure of each IPL and the probabilities of any conditional modifiers (a conditional modifier is for example whether a person will be present to be impacted) to determine the frequency of occurrence of the undesired consequence. Orders of magnitude are used for frequencies and probabilities;

- the calculated level of risk is compared with risk tolerance levels to determine whether further protection is required.

An IPL is a device system or action that is capable of preventing a scenario proceeding to its undesired consequence, independent of the causal event or any other layer of protection associated with the scenario.

IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;
- post event physical protection;
- emergency response systems (procedures and inspections are not IPLs).

B.18.5 Output

Recommendations for any further controls and the effectiveness of these controls in reducing risk shall be given.

LOPA is one of the techniques used for SIL assessment when dealing with safety related/instrumented systems

B.18.6 Strengths and limitations

Strengths include:

- it requires less time and resources than a fault tree analysis or fully quantitative risk assessment but is more rigorous than qualitative subjective judgments;
- it helps identify and focus resources on the most critical layers of protection;
- it identifies operations, systems and processes for which there are insufficient safeguards;
- it focuses on the most serious consequences.

Limitations include:

- LOPA focuses on one cause-consequence pair and one scenario at a time. Complex interactions between risks or between controls are not covered;
- quantified risks may not account for common mode failures;
- LOPA does not apply to very complex scenarios where there are many cause-consequence pairs or where there are a variety of consequences affecting different stakeholders.

B.18.7 Reference documents

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

B.19 Decision tree analysis

B.19.1 Overview

A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made.

B.19.2 Use

A decision tree is used in managing project risks and in other circumstances to help select the best course of action where there is uncertainty. The graphical display can also help communicate reasons for decisions.

B.19.3 Input

A project plan with decision points. Information on possible outcomes of decisions and on chance events which might affect decisions.

B.19.4 Process

A decision tree starts with an initial decision, for example to proceed with project A rather than project B. As the two hypothetical projects proceed, different events will occur and different predictable decisions will need to be made. These are represented in tree format, similar to an event tree. The probability of the events can be estimated together with the cost or utility of the final outcome of the pathway.

Information concerning the best decision pathway is logically that which produces the highest expected value calculated as the product of all the conditional probabilities along the pathway and the outcome value.

B.19.5 Outputs

Outputs include:

- a logical analysis of the risk displaying different options that may be taken
- a calculation of the expected value for each possible path

B.19.6 Strengths and limitations

Strengths include:

- they provide a clear graphical representation of the details of a decision problem;
- they enable a calculation of the best pathway through a situation.

Limitations include:

- large decisions trees may become too complex for easy communication with others;
- there may be a tendency to oversimplify the situation so as to be able to represent it as a tree diagram.

B.20 Human reliability assessment (HRA)

B.20.1 Overview

Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system.

Many processes contain potential for human error, especially when the time available to the operator to make decisions is short. The probability that problems will develop sufficiently to become serious can be small. Sometimes, however, human action will be the only defence to prevent an initial failure progressing towards an accident.

The importance of HRA has been illustrated by various accidents in which critical human errors contributed to a catastrophic sequence of events. Such accidents are warnings against risk assessments that focus solely on the hardware and software in a system. They illustrate the dangers of ignoring the possibility of human error contribution. Moreover, HRAs are useful in highlighting errors that can impede productivity and in revealing ways in which these errors and other failures (hardware and software) can be "recovered" by the human operators and maintenance personnel.

B.20.2 Use

HRA can be used qualitatively or quantitatively. Qualitatively, it is used to identify the potential for human error and its causes so the probability of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

B.20.3 Input

Inputs to HRA include:

- information to define tasks that people should perform;
- experience of the types of error that occur in practice and potential for error;
- expertise on human error and its quantification.

B.20.4 Process

The HRA process is as follows:

- **Problem definition**, what types of human involvements are to be investigated/assessed?
- **Task analysis,** how will the task be performed and what type of aids will be needed to support performance?
- **Human error analysis**, how can task performance fail: what errors can occur and how can they be recovered?
- **Representation**, how can these errors or task performance failures be integrated with other hardware, software, and environmental events to enable overall system failure probabilities to be calculated?
- **Screening**, are there any errors or tasks that do not require detailed quantification?
- **Quantification**, how likely are individual errors and failures of tasks?
- **Impact assessment**, which errors or tasks are most important, i.e. which ones have the highest contribution to reliability or risk?
- **Error reduction**, how can higher human reliability be achieved?
- **Documentation**, what details of the HRA need to be documented?

In practice, the HRA process proceeds step-wise although sometimes with parts (e.g. tasks analysis and error identification) proceeding in parallel with one another.

B.20.5 Output

Outputs include:

- a list of errors that may occur and methods by which they can be reduced – preferably through redesign of the system;
- error modes, error types causes and consequences;

- a qualitative or quantitative assessment of the risk posed by the errors.

B.20.6 Strengths and limitations

Strengths of HRA include:

- HRA provides a formal mechanism to include human error in consideration of risks associated with systems where humans often play an important role;
- formal consideration of human error modes and mechanisms can help reduce the probability of failure due to error.

Limitations include:

- the complexity and variability of humans, which make defining simple failure modes and probabilities difficult;
- many activities of humans do not have a simple pass/fail mode. HRA has difficulty dealing with partial failures or failure in quality or poor decision-making.

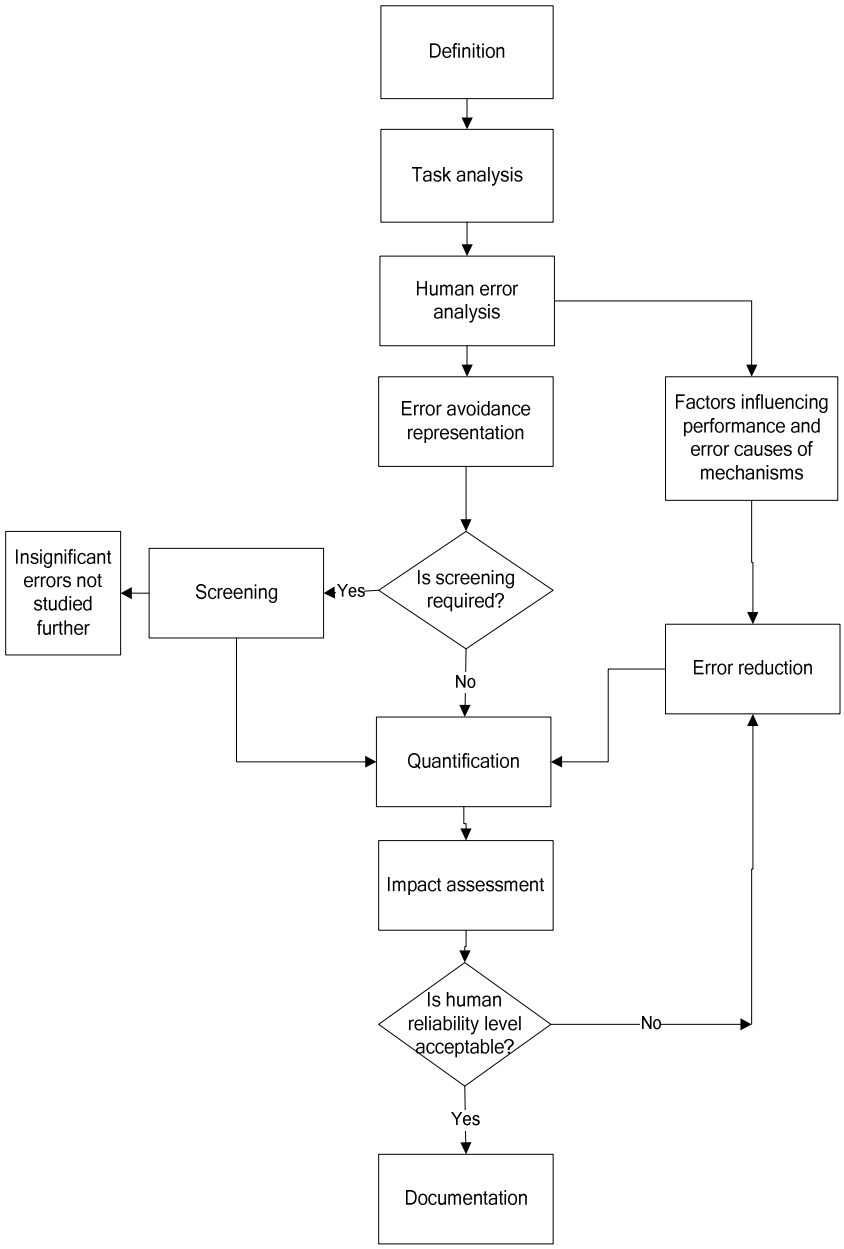

Figure B.7 – Example of human reliability assessment

B.21 Bow tie analysis

B.21.1 Overview

Bow tie analysis is a simple diagrammatic way of describing and analysing the pathways of a risk from causes to consequences. It can be considered to be a combination of the thinking of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences. However the focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences. Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly from a brainstorming session.

B.21.2 Use

Bow tie analysis is used to display a risk showing a range of possible causes and consequences. It is used when the situation does not warrant the complexity of a full fault tree analysis or when the focus is more on ensuring that there is a barrier or control for each failure pathway. It is useful where there are clear independent pathways leading to failure.

Bow tie analysis is often easier to understand than fault and event trees, and hence can be a useful communication tool where analysis is achieved using more complex techniques.

B.21.3 Input

An understanding is required of information on the causes and consequences of a risk and the barriers and controls which may prevent, mitigate or stimulate it.

B.21.4 Process

The bow tie is drawn as follows:

a) A particular risk is identified for analysis and represented as the central knot of a bow tie.

b) Causes of the event are listed considering sources of risk (or hazards in a safety context).

c) The mechanism by which the source of risk leads to the critical event is identified.

d) Lines are drawn between each cause and the event forming the left-hand side of the bow tie. Factors which might lead to escalation can be identified and included in the diagram.

e) Barriers which should prevent each cause leading to the unwanted consequences can be shown as vertical bars across the line. Where there were factors which might cause escalation, barriers to escalation can also be represented. The approach can be used for positive consequences where the bars reflect ‘controls’ that stimulate the generation of the event.

f) On the right-hand side of the bow tie different potential consequences of the risk are identified and lines drawn to radiate out from the risk event to each potential consequence.

g) Barriers to the consequence are depicted as bars across the radial lines. The approach can be used for positive consequences where the bars reflect ‘controls’ that support the generation of consequences.

h) Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification of a bow tie diagram may be possible where pathways are independent, the probability of a particular consequence or outcome is known and a figure can be estimated for the effectiveness of a control. However, in many situations, pathways and barriers are not independent and controls may be procedural and hence the effectiveness unclear. Quantification is often more appropriately carried out using FTA and ETA.

B.21.5 Output

The output is a simple diagram showing main risk pathways and the barriers in place to prevent or mitigate the undesired consequences or stimulate and promote desired consequences.

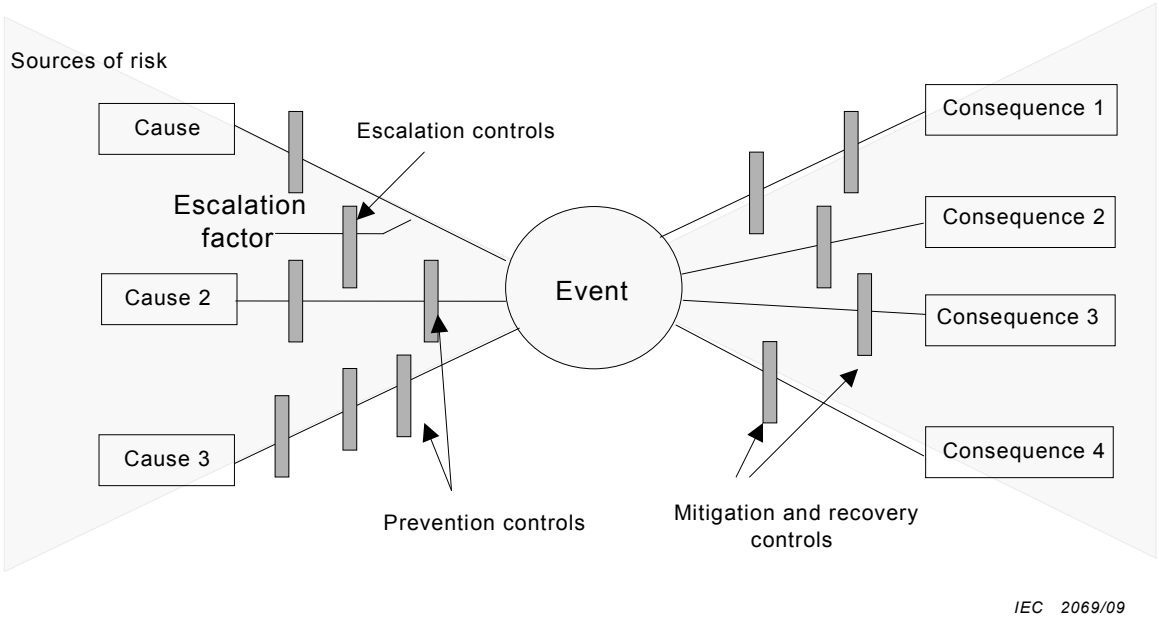

Figure B.8 – Example bow tie diagram for unwanted consequences

B.21.6 Strengths and limitations

Strengths of bow tie analysis:

- it is simple to understand and gives a clear pictorial representation of the problem;
- it focuses attention on controls which are supposed to be in place for both prevention and mitigation and their effectiveness;
- it can be used for desirable consequences;
- it does not need a high level of expertise to use.

Limitations include:

- it cannot depict where multiple causes occur simultaneously to cause the consequences (i.e. where there are AND gates in a fault tree depicting the left-hand side of the bow);
- it may over-simplify complex situations, particularly where quantification is attempted.

B.22 Reliability centred maintenance

B.22.1 Overview

Reliability centred maintenance (RCM) is a method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.

RCM is now a proven and accepted methodology used in a wide range of industries.

RCM provides a decision process to identify applicable and effective preventive maintenance requirements for equipment in accordance with the safety, operational and economic consequences of identifiable failures, and the degradation mechanism responsible for those failures. The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes. Details regarding the use and application of RCM are provided in IEC 60300-3-11.

B.22.2 Use

All tasks are based on safety in respect of personnel and environment, and on operational or economic concerns. However, it should be noted that the criteria considered will depend on the nature of the product and its application. For example, a production process will need to be economically viable, and may be sensitive to strict environmental considerations, whereas an item of defence equipment should be operationally successful, but may have less stringent safety, economic and environmental criteria. Greatest benefit can be achieved through targeting of the analysis to where failures would have serious safety, environmental, economic or operational effects.

RCM is used to ensure that applicable and effective maintenance is performed, and is generally applied during the design and development phase and then implemented during operation and maintenance.

B.22.3 Input

Successful application of RCM needs a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems and items of equipment, together with the possible failures, and the consequences of those failures.

B.22.4 Process

The basic steps of an RCM programme are as follows:

- initiation and planning;
- functional failure analysis;
- task selection;
- implementation;
- continuous improvement.

RCM is risk based since it follows the basic steps in risk assessment. The type of risk assessment is a failure mode, effect and criticality analysis (FMECA) but requires a specific approach to analysis when used in this context.

Risk identification focuses on situations where potential failures may be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. It is performed by identifying required functions and performance standards and failures of equipment and components that can interrupt those functions

Risk analysis consists of estimating the frequency of each failure without maintenance being carried out. Consequences are established by defining failure effects. A risk matrix that combines failure frequency and consequences allows categories for levels of risk to be established.

Risk evaluation is then performed by selecting the appropriate failure management policy for each failure mode.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

B.22.5 Output

RCM provides a definition of maintenance tasks such as condition monitoring, scheduled restoration, scheduled replacement, failure-finding or non preventive maintenance. Other possible actions that can result from the analysismay include redesign, changes to operating

or maintenance procedures or additional training. Task intervals and required resources are then identified.

B.22.6 Reference documents

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 Sneak analysis (SA)and sneak circuit analysis (SCI)

B.23.1 Overview

Sneak analysis (SA) is a methodology for identifying design errors. A sneak condition is a latent hardware, software or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel.

B.23.2 Use

Sneak circuit analysis (SCA) was developed in the late 1960s for NASA to verify the integrity and functionality of their designs. It served as a useful tool for discovering unintentional electrical circuit paths, and assisted in devising solutions to isolate each function. However, as technology advanced, the tools for sneak circuit analysis also had to advance. Sneak analysis includes and far exceeds the coverage of sneak circuit analysis. It can locate problems in both hardware and software using any technology. The sneak analysis tools can integrate several analyses such as fault trees, failure mode and effects analysis (FMEA), reliability estimates, etc. into a single analysis saving time and project expenses.

B.23.3 Input

Sneak analysis is unique from the design process in that it uses different tools (network trees, forests, and clues or questions to help the analyst identify sneak conditions) to find a specific type of problem. The network trees and forests are topological groupings of the actual system. Each network tree represents a sub-function and shows all inputs that may affect the sub-function output. Forests are constructed by combining the network trees that contribute to a particular system output. A proper forest shows a system output in terms of all of its related inputs. These, along with others, become the input to the analysis.

B.23.4 Process

The basic steps in performing a sneak analysis consist of:

- data preparation;
- construction of the network tree;
- evaluation of network paths;
- final recommendations and report.

B.23.5 Output

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system, coded into the software program, or triggered by human error. There are four categories of sneak circuits:

a) sneak paths: unexpected paths along which current, energy, or logical sequence flows in an unintended direction;

b) sneak timing: events occurring in an unexpected or conflicting sequence;

c) sneak indications: ambiguous or false displays of system operating conditions that may cause the system or an operator to take an undesired action;

d) sneak labels: incorrect or imprecise labelling of system functions, e.g. system inputs, controls, display buses that may cause an operator to apply an incorrect stimulus to the system.

B.23.6 Strengths and limitations

Strengths include:

- sneak analysis is good for identifying design errors;
- it works best when applied in conjunction with HAZOP;
- it is very good for dealing with systems which have multiple states such as batch and semi-batch plant.

Limitations may include:

- the process is somewhat different depending on whether it is applied to electrical circuits, process plants, mechanical equipment or software;
- the method is dependent on establishing correct network trees.

B.24 Markov analysis

B.24.1 Overview

Markov analysis is used where the future state of a system depends only upon its present state. It is commonly used for the analysis of repairable systems that can exist in multiple states and the use of a reliability block analysis would be unsuitable to adequately analyse the system. The method can be extended to more complex systems by employing higher order Markov processes and is only restricted by the model, mathematical computations and the assumptions.

The Markov analysis process is a quantitative technique and can be discrete (using probabilities of change between the states) or continuous (using rates of change across the states).

While a Markov analysis can be performed by hand, the nature of the techniques lends itself to the use of computer programmes, many of which exist in the market.

B.24.2 Use

The Markov analysis technique can be used on various system structures, with or without repair, including:

- independent components in parallel;
- independent components in series;
- load-sharing system;
- stand-by system, including the case where switching failure can occur;
- degraded systems.

The Markov analysis technique can also be used for calculating availability, including taking into account the spares components for repairs.

B.24.3 Input

The inputs essential to a Markov analysis are as follows:

- list of various states that the system, sub-system or component can be in (e.g. fully operational, partially operation (i.e. a degraded state), failed state, etc);
- a clear understanding of the possible transitions that are necessary to be modelled. For example, failure of a car tyre needs to consider the state of the spare wheel and hence the frequency of inspection;
- rate of change from one state to another, typically represented by either a probability of change between states for discrete events, or failure rate (λ) and/or repair rate (μ) for continuous events.

B.24.4 Process

The Markov analysis technique is centred around the concept of "states", e.g. "available" and "failed", and the transition between these two states over time based on a constant probability of change. A stochastic transitional probability matrix is used to describe the transition between each of the states to allow the calculation of the various outputs.

To illustrate the Markov analysis technique, consider a complex system that can be in only three states; functioning, degraded and failed, defined as states S1, S2, S3 respectively. Each day, the system exists in one of these three states. Table B.3 shows the probability that tomorrow, the system is in state S*i* where *i* can be 1, 2 or 3.

Table B.2 – Markov matrix

		State today		
		S1	S2	S3
State tomorrow	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

This array of probabilities is called a Markov matrix, or transition matrix. Notice that the sum for each of the columns is 1 as they are the sum of all the possible outcomes in each case. The system, can also be represented by a Markov diagram where the circles represent the states, and the arrows represent the transition, together with the accompanying probability.

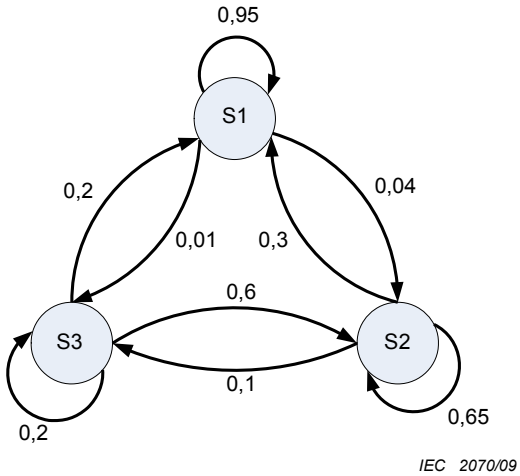

Figure B.9 – Example of system Markov diagram

The arrows from a state to itself are not usually shown, but are shown within these examples for completeness.

Let P*i* represent the probability of finding the system in state *i* for *i* = 1, 2, 3, then the simultaneous equations to be solved are:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B.3)}$$

These three equations are not independent and will not solve the three unknowns. The following equation should be used and one of the above equations discarded.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

The solution is 0,85, 0,13, and 0.02 for the respective states 1, 2, 3. The system is fully functioning for 85 % of the time, in the degraded state for 13 % of the time and failed for 2 % of the time.

Consider two items operating in parallel with either required to be operational for the system to function. The items can either be operational or failed and the availability of the system is dependent upon the status of the items.

The states can be considered as:

State 1 Both items are functioning correctly;

State 2 One item has failed and is undergoing repair, the other is functioning;

State 3 Both items have failed and one is undergoing repair.

If the continuous failure rate for each item is assumed to be λ and the repair rate to be μ, then the state transition diagram is:

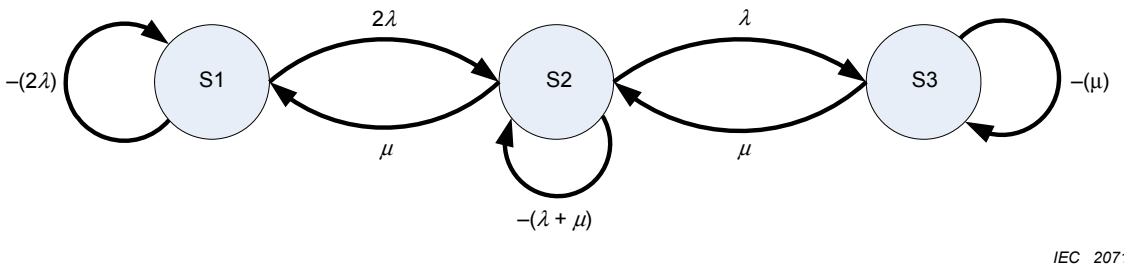

Figure B.10 – Example of state transition diagram

Note that the transition from state 1 to state 2 is 2λ as failure of either of the two items will take the system to state 2.

Let P*i*(*t*) be the probability of being in an initial state *i* at time *t*; and

Let P*i*(*t* + *δt*) be the probability of being in a final state at time *t* + *δt*

The transition probability matrix becomes:

Table B.3 – Final Markov matrix

		Initial state		
		P1(t)	P2(t)	P3(t)
	P1($t + \delta t$)	-2λ	μ	0
Final state	P2($t + \delta t$)	2λ	$-(\lambda + \mu)$	μ
	P3($t + \delta t$)	0	λ	$-\mu$

It is worth noting that the zero values occur as it is not possible to move from state 1 to state 3 or from state 3 to state 1. Also, the columns sum to zero when specifying rates.

The simultaneous equations become:

$$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda\, P1(t) + -(\lambda + \mu)\, P2(t) + \mu\, P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda\, P2(t) + -\mu\, P3(t) \quad \text{(B.7)}$$

For simplicity, it will be assumed that the availability required is the steady state availability.

When δt tends to infinity, dPi/dt will tend to zero and the equations become easier to solve. The additional equation as shown in Equation (B.4) above should also be used:

Now the equation $A(t) = P1(t) + P2(t)$ can be expressed as:

$A = P1 + P2$

Hence $A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Output

The output from a Markov analysis is the various probabilities of being in the various states, and therefore an estimate of the failure probabilities and/or availability, one of the essential components of a system.

B.24.6 Strengths and limitations

Strengths of a Markov analysis include:

- ability to calculate the probabilities for systems with a repair capability and multiple degraded states.

Limitations of a Markov analysis include:

- assumption of constant probabilities of change of state; either failure or repairs;
- all events are statistically independent since future states are independent of all past states, except for the state immediately prior;
- needs knowledge of all probabilities of change of state;
- knowledge of matrix operations;
- results are hard to communicate with non-technical personnel.

B.24.7 Comparisons

Markov analysis is similar to a Petri-Net analysis by being able to monitor and observe system states, although different since Petri-Net can exist in multiple states at the same time.

B.24.8 Reference documents

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts)*, Software and systems engineering – High-level Petri nets*

B.25 Monte Carlo simulation

B.25.1 Overview

Many systems are too complex for the effects of uncertainty on them to be modelled using analytical techniques, but they can be evaluated by considering the inputs as random variables and running a number N of calculations (so-called simulations) by sampling the input in order to obtain N possible outcomes of the wanted result.

This method can address complex situations that would be very difficult to understand and solve by an analytical method. Systems can be developed using spreadsheets and other conventional tools, but more sophisticated tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. When the technique was first developed, the number of iterations required for Monte Carlo simulations made the process slow and time consuming, but advances in computers and theoretical developments, such as Latin-hypercube sampling, have made processing time almost insignificant for many applications.

B.25.2 Use

Monte Carlo simulation provides a means of evaluating the effect of uncertainty on systems in a wide range of situations. It is typically used to evaluate the range of possible outcomes and the relative frequency of values in that range for quantitative measures of a system such as cost, duration, throughput, demand and similar measures. Monte Carlo simulation may be used for two different purposes:

- uncertainty propagation on conventional analytical models;
- probabilistic calculations when analytical techniques do not work.

B.25.3 Input

The input to a Monte Carlo simulation is a good model of the system and information on the types of inputs, the sources of uncertainty that are to be represented and the required output. Input data with uncertainty is represented as random variables with distributions which are more or less spread according to the level of uncertainties. Uniform, triangular, normal and log normal distributions are often used for this purpose.

B.25.4 Process

The process is as follows:

a) A model or algorithm is defined which represents as closely as possible the behaviour of the system being studied.

b) The model is run multiple times using random numbers to produce outputs of the model (simulations of the system); Where the application is to model the effects of uncertainty

the model is in the form of an equation providing the relationship between input parameters and an output. The values selected for the inputs are taken from appropriate probability distributions that represent the nature of the uncertainty in these parameters.

c) In either case a computer runs the model multiple times (often up to 10,000 times) with different inputs and produces multiple outputs. These can be processed using conventional statistics to provide information such as average values, standard deviation, confidence intervals.

An example of a simulation is given below.

Consider the case of two items operating in parallel and only one is required for the system to function. The first item has a reliability of 0,9 and the other 0,8.

It is possible to construct a spreadsheet with the following columns.

Table B.4 – Example of Monte Carlo simulation

	Item 1		Item 2		
Simulation number	Random number	Functions?	Random number	Functions?	System
1	0,577 243	YES	0,059 355	YES	1
2	0,746 909	YES	0,311 324	YES	1
3	0,541 728	YES	0,919 765	NO	1
4	0,423 274	YES	0,643 514	YES	1
5	0,917 776	NO	0,539 349	YES	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	YES	0,950 241	NO	1
8	0,661 418	YES	0,919 868	NO	1
9	0,213 376	YES	0,367 555	YES	1
10	0,565 657	YES	0,119 215	YES	1

The random generator creates a number between 0 and 1 which is used to compare with the probability of each item to determine if the system is operational. With just 10 runs, the result of 0,9 should not be expected to be an accurate result. The usual approach is to build in a calculator to compare the total result as the simulation progresses to achieve the level of accuracy required. In this example, a result of 0,979 9 was achieved after 20 000 iterations.

The above model can be extended in a number of ways. For example:

- by extending the model itself (such as considering the second item becoming immediately operational only when the first item fails);
- by changing the fixed probability to a variable (a good example is the triangular distribution) when the probability cannot be accurately defined;
- using failure rates combined with the randomizer to derive a time of failure (exponential, Weibull, or other suitable distribution) and building in repair times.

Applications include, amongst other things, the assessment of uncertainty in financial forecasts, investment performance, project cost and schedule forecasts, business process interruptions and staffing requirements.

Analytical techniques are not able to provide relevant results or when there is uncertainty in the input data and so in the outputs.

B.25.5 Output

The output could be a single value, as determined in the above example, it could be a result expressed as the probability or frequency distribution or it could be the identification of the main functions within the model that has the greatest impact on the output.

In general, a Monte Carlo simulation will be used to assess either the entire distribution of outcomes that could arise or key measures from a distribution such as:

- the probability of a defined outcome arising;
- the value of an outcome in which the problem owners have a certain level of confidence that it will not be exceeded or beaten, a cost that there is less than a 10 % chance of exceeding or a duration that is 80 % certain to be exceeded.

An analysis of the relationships between inputs and outputs can throw light on the relative significance of the factors at work and identify useful targets for efforts to influence the uncertainty in the outcome.

B.25.6 Strengths and limitations

Strengths of the Monte Carlo analysis include the following:

- the method can, in principle, accommodate any distribution in an input variable, including empirical distributions derived from observations of related systems;
- models are relatively simple to develop and can be extended as the need arises;
- any influences or relationships arising in reality can be represented, including subtle effects such as conditional dependencies;
- sensitivity analysis can be applied to identify strong and weak influences;
- models can be easily understood as the relationship between inputs and outputs is transparent;
- efficient behavioural models such as Petri Nets (future IEC 62551) are available which prove to be very efficient for Monte Carlo simulation purposes;
- provides a measure of the accuracy of a result;
- software is readily available and relatively inexpensive.

Limitations are as follows:

- the accuracy of the solutions depends upon the number of simulations which can be performed (this limitation is becoming less important with increased computer speeds);
- it relies on being able to represent uncertainties in parameters by a valid distribution;
- large and complex models may be challenging to the modeller and make it difficult for stakeholders to engage with the process;
- the technique may not adequately weigh high-consequence/low probability events and therefore not allow an organization’s risk appetite to be reflected in the analysis.

B.25.7 Reference documents

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*[1]

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*

---

1 Currently under consideration.

B.26 Bayesian statistics and Bayes Nets

B.26.1 Overview

Bayesian statistics are attributed to the Reverend Thomas Bayes. Its premise is that any already known information (the Prior) can be combined with subsequent measurement (the Posterior) to establish an overall probability. The general expression of the Bayes Theorem can be expressed as:

$$P(A \mid B) = \{P(A)P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

where

the probability of X is denoted by $P(X)$;

the probability of X on the condition that Y has occurred is denoted by $P(X|Y)$; and

E_i is the ith event.

In its simplest form this reduces to $P(A|B) = \{P(A)P(B|A)\} /P(B)$.

Bayesian statistics differs from classical statistics in that is does not assume that all distribution parameters are fixed, but that parameters are random variables. A Bayesian probability can be more easily understood if it is considered as a person's degree of belief in a certain event as opposed to the classical which is based upon physical evidence. As the Bayesian approach is based upon the subjective interpretation of probability, it provides a ready basis for decision thinking and the development of Bayesian nets (or Belief Nets, belief networks or Bayesian networks).

Bayes nets use a graphical model to represent a set of variables and their probabilistic relationships. The network is comprised of nodes that represent a random variable and arrows which link a parent node to a child node, (where a parent node is a variable that directly influences another (child) variable).

B.26.2 Use

In recent years, the use of Bays' theory and Nets has become widespread partly because of their intuitive appeal and also because of the availability of software computing tools. Bayes nets have been used on a wide range of topics: medical diagnosis, image modelling, genetics, speech recognition, economics, space exploration and in the powerful web search engines used today. They can be valuable in any area where there is the requirement for finding out about unknown variables through the utilization of structural relationships and data. Bayes nets can be used to learn causal relationships to give an understanding about a problem domain and to predict the consequences of intervention.

B.26.3 Input

The inputs are similar to the inputs for a Monte Carlo model. For a Bayes net, examples of the steps to be taken include the following:

- define system variables;
- define causal links between variables;
- specify conditional and prior probabilities;
- add evidence to net;
- perform belief updating;
- extract posterior beliefs.

B.26.4 Process

Bayes theory can be applied in a wide variety of ways. This example will consider the creation of a Bayes table where a medical test is used to determine if the patient has a disease. The belief before taking the test is that 99 % of the population do not have this disease and 1 % have the disease, i.e the Prior information. The accuracy of the test has shown that if the person has the disease, the test result is positive 98 % of the time. There is also a probability that if you do not have the disease, the test result is positive 10 % of the time. The Bayes table provides the following information:

Table B.5 – Bayes' table data

	PRIOR	PROBABILITY	PRODUCT	POSTERIOR
Have disease	0,01	0,98	0,009 8	0,090 1
No disease	0,99	0,10	0,099 0	0,909 9
SUM	1		0,108 8	1

Using Bayes rule, the product is determined by combining the prior and probability. The posterior is found by dividing the product value by the product total. The output shows that a positive test result indicates that the prior has increased from 1 % to 9 % . More importantly, there is a strong chance that even with a positive test, having the disease is unlikely. Examining the equation (0,01×0,98)/((0,01×0,98)+(0,99×0,1)) shows that the 'no disease-positive result' value plays a major role in the posterior values.

Consider the following Bayes net:

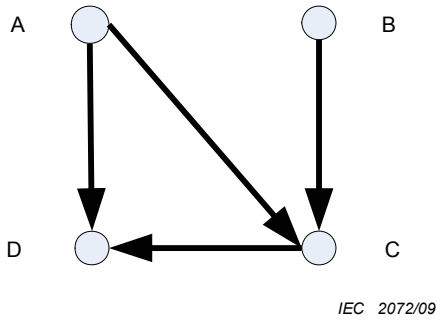

Figure B.11 – Sample Bayes' net

With the conditional prior probabilities defined within the following tables and using the notation that Y indicates positive and N indicates negative, the positive could be "have disease" as above, or could be High and N could be Low.

Table B.6 – Prior probabilities for nodes A and B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Table B.7 – Conditional probabilities for node C with node A and node B defined

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8

N	*N*	0,7	0,3

Table B.8 – Conditional probabilities for node D with node A and node C defined

A	*C*	P(*D* = *Y*)	P(*D* = *N*)
Y	*Y*	0,6	0,4
Y	*N*	1,0	0,0
N	*Y*	0,2	0,8
N	*N*	0,6	0,4

To determine the posterior probability of P(*A*|*D*=*N*,*C*=*Y*), it is necessary to first calculate P(*A*,*B*|*D*=*N*,*C*=*Y*).

Using Bayes' rule, the value P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*) is determined as shown below and the last column shows the normalized probabilities which sum to 1 as derived in the previous example (result rounded).

Table B.9 – Posterior probability for nodes A and B with node D and node C defined

A	*B*	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A*,*B*|*D*=*N*,*C*=*Y*)
Y	*Y*	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0,4
Y	*N*	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0,48
N	*Y*	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0,04
N	*N*	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0,08

To derive P(*A*|*D*=*N*,*C*=*Y*), all values of *B* need to be summed:

Table B.10 – Posterior probability for node A with node D and node C defined

P(*A*=*Y*|*D*=*N*,*C*=*Y*)	P(*A*=*N*|*D*=*N*,*C*=*Y*)
0,88	0,12

This shows that the prior for P(*A*=*N*) has increased from 0,1 to a posterior of 0,12 which is only a small change. On the other hand, P(*B*=*N*|*D*=*N*,*C*=*Y*) has changed from 0,4 to 0,56 which is a more significant change.

B.26.5 Outputs

The Bayesian approach can be applied to the same extent as classical statistics with a wide range of outputs, e.g. data analysis to derive point estimators and confidence intervals. Its recent popularity is in relation to Bayes nets to derive posterior distributions. The graphical output provides an easily understood model and the data can be readily modified to consider correlations and sensitivity of parameters.

B.26.6 Strengths and limitations

Strengths:

- all that is needed is knowledge on the priors;
- inferential statements are easy to understand;
- Bayes' rule is all that is required;
- it provides a mechanism for using subjective beliefs in a problem.

Limitations:

- defining all interactions in Bayes nets for complex systems is problematic;
- Bayesian approach needs the knowledge of a multitude of conditional probabilities which are generally provided by expert judgment. Software tools can only provide answers based on these assumptions.

B.27 FN curves

B.27.1 Overview

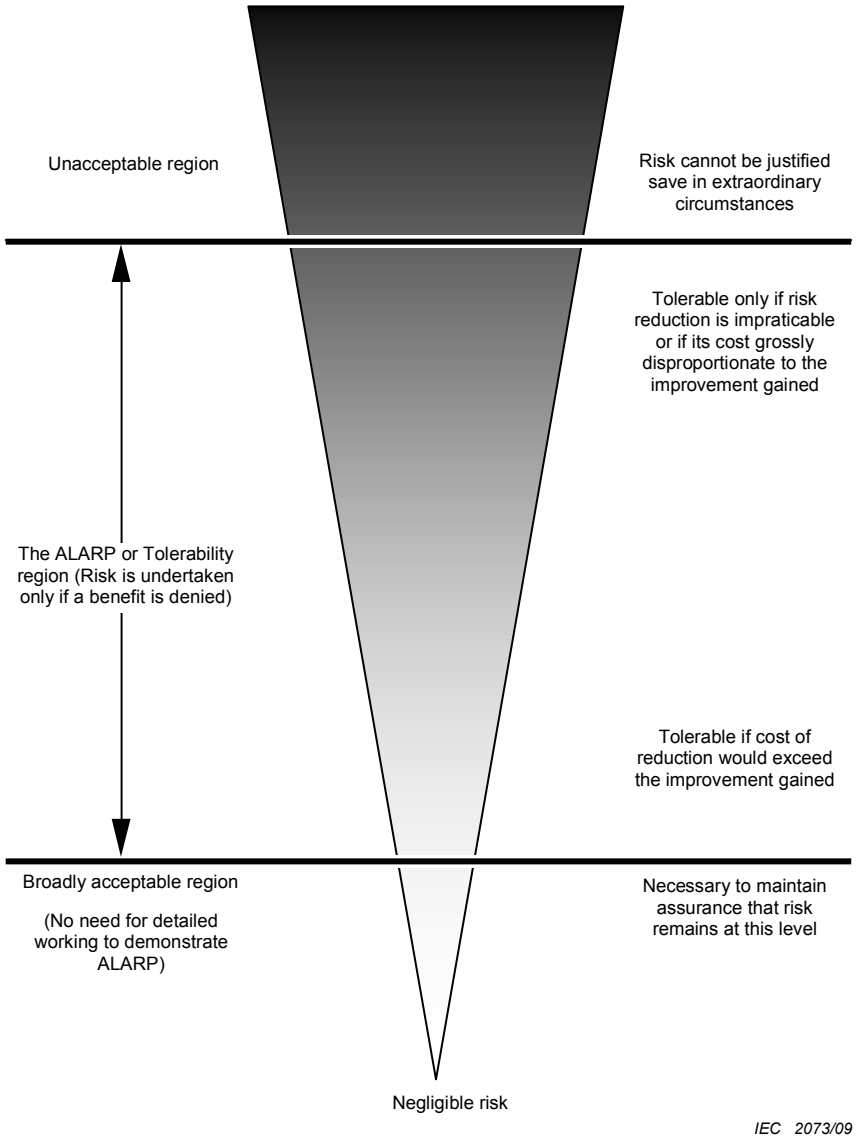

Figure B.12 – The ALARP concept

FN curves are a graphical representation of the probability of events causing a specified level of harm to a specified population. Most often they refer to the frequency of a given number of casualties occurring.

FN curves show the cumulative frequency (*F*) at which *N* or more members of the population that will be affected. High values of *N* that may occur with a high frequency *F* are of significant interest because they may be socially and politically unacceptable.

B.27.2 Use

FN curves are a way of representing the outputs of risk analysis. Many events have a high probability of a low consequence outcome and a low probability of a high consequence outcome. The FN curves provide a representation of the level of risk that is a line describing this range rather than a single point representing one consequence probability pair.

FN curves may be used to compare risks, for example to compare predicted risks against criteria defined as an FN curve, or to compare predicted risks with data from historical incidents, or with decision criteria (also expressed as an F/N curve).

FN curves can be used either for system or process design, or for management of existing systems.

B.27.3 Input

The inputs are either:

- sets of the probability consequence pairs over a given period of time;
- the output of data from a quantitative risk analysis giving estimated probabilities for specified numbers of casualties;
- data from both historical records and a quantitative risk analysis.

B.27.4 Process

The available data is plotted onto a graph with the number of casualties (to a specified level of harm, i.e. death) forming the abscissa with the probability of *N* or more casualties forming the ordinate. Because of the large range of values, both axes are normally on logarithmic scales.

FN curves may be constructed statistically using “real” numbers from past losses or they can be calculated from simulation model estimates. The data used and assumptions made may mean that these two types of FN curve give different information and should be used separately and for different purposes. In general, theoretical FN curves are most useful for system design, and statistical FN curves are most useful for management of a particular existing system.

Both derivation approaches can be very time-consuming so it is not uncommon to use a mixture of both. Empirical data will then form fixed points of precisely known casualties that occurred in known accidents/incident in a specified period of time and the quantitative risk analysis providing other points by extrapolation or interpolation.

The need to consider low-frequency, high-consequence accidents may require consideration of long periods of time to gather enough data for a proper analysis. This in turn may make the available data suspect if the initiating events happen to change over time.

B.27.5 Output

A line representing risk across a range of values of consequence that can be compared with criteria that are appropriate for the population being studied and the specified level of harm.

B.27.6 Strengths and limitations

FN curves are a useful way of presenting risk information that can be used by managers and system designers to help make decisions about risk and safety levels. They are a useful way of presenting both frequency and consequence information in an accessible format.

FN curves are appropriate for comparison of risks from similar situations where sufficient data is available. They should not be used to compare risks of different types with varying characteristics in circumstances where quantity and quality of data varies.

A limitation of FN curves is that they do not say anything about the range of effects or outcomes of incidents other than the number of people impacted, and there is no way of identifying the different ways in which the level of harm may have occurred. They map a particular consequence type, usually harm to people. FN curves are not a risk assessment method, but one way of presenting the results of risk assessment.

They are a well established method for presenting risk assessment results but require preparation by skilled analysts and are often difficult for non specialists to interpret and evaluate

B.28 Risk indices

B.28.1 Overview

A risk index is a semi-quantitative measure of risk which is an estimate derived using a scoring approach using ordinal scales. Risk indices can be used to rate a series of risks using similar criteria so that they can be compared. Scores are applied to each component of risk, for example contaminant characteristics (sources), the range of possible exposure pathways and the impact on the receptors.

Risk indices are essentially a qualitative approach to ranking and comparing risks. While numbers are used, this is simply to allow for manipulation. In many cases where the underlying model or system is not well known or not able to be represented, it is better to use a more overtly qualitative approach.

B.28.2 Use

Indices can be used for classifying different risks associated with an activity if the system is well understood. They permit the integration of a range of factors which have an impact on the level of risk into a single numerical score for level of risk

Indices are used for many different types of risk usually as a scoping device for classifying risk according to level of risk. This may be used to determine which risks need further in-depth and possibly quantitative assessment.

B.28.3 Input

The inputs are derived from analysis of the system, or a broad description of the context. This requires a good understanding of all the sources of risk, the possible pathways and what might be affected. Tools such as fault tree analysis, event tree analysis and general decision analysis can be used to support the development of risk indices.

Since the choice of ordinal scales is, to some extent, arbitrary, sufficient data is needed to validate the index.

B.28.4 Process

The first step is to understand and describe the system. Once the system has been defined, scores are developed for each component in such a way that they can be combined to provide a composite index. For example, in an environmental context, the sources, pathway and receptor(s) will be scored, noting that in some cases there may be multiple pathways and receptors for each source. The individual scores are combined according to a scheme that takes account of the physical realities of the system. It is important that the scores for each part of the system (sources, pathways and receptors) are internally consistent and maintain their correct relationships. Scores may be given for components of risk (e.g. probability, exposure, consequence) or for factors which increase risk.

Scores may be added, subtracted, multiplied and/or divided according to this high level model. Cumulative effects can be taken into account by adding scores (for example, adding scores for different pathways). It is strictly not valid to apply mathematical formulae to ordinal scales. Therefore, once the scoring system has been developed, the model should be validated by applying it to a known system. Developing an index is an iterative approach and several different systems for combining the scores may be tried before the analyst is comfortable with the validation.

Uncertainty can be addressed by sensitivity analysis and varying scores to find out which parameters are the most sensitive.

B.28.5 Output

The output is a series of numbers (composite indices) that relate to a particular source and which can be compared with indices developed for other sources within the same system or which can be modelled in the same way.

B.28.6 Strengths and limitations

Strengths:

- indices can provide a good tool for ranking different risks;
- they allow multiple factors which affect the level of risk to be incorporated into a single numerical score for the level of risk.

Limitations:

- if the process (model) and its output are not well validated, the results may be meaningless. The fact that the output is a numerical value for risk may be misinterpreted and misused, for example in subsequent cost/benefit analysis;
- in many situations where indices are used, there is no fundamental model to define whether the individual scales for risk factors are linear, logarithmic or of some other form, and no model to define how factors should be combined. In these situations, the rating is inherently unreliable and validation against real data is particularly important.

B.29 Consequence/probability matrix

B.29.1 Overview

The consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating.

The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances.

B.29.2 Use

A consequence/probability matrix is used to rank risks, sources of risk or risk treatments on the basis of the level of risk. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis, which risks need treatment first, or which need to be referred to a higher level of management. It may also be used to select which risks need not be considered further at this time. This kind of risk matrix is also widely used to determine if a given risk is broadly acceptable, or not acceptable (see 5.4) according to the zone where it is located on the matrix.

The consequence/probability matrix may also be used to help communicate a common understanding for qualitative levels of risks across the organization. The way risk levels are set and decision rules assigned to them should be aligned with the organization's risk appetite.

A form of consequence/probability matrix is used for criticality analysis in FMECA or to set priorities following HAZOP. It may also be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more quantitative analysis

B.29.3 Input

Inputs to the process are customized scales for consequence and probability and a matrix which combines the two.

The consequence scale (or scales) should cover the range of different types of consequence to be considered (for example: financial loss; safety; environment or other parameters, depending on context) and should extend from the maximum credible consequence to the lowest consequence of concern. A part example is shown in Figure B.6.

The scale may have any number of points. 3, 4 or 5 point scales are most common.

The probability scale may also have any number of points. Definitions for probability need to be selected to be as unambiguous as possible. If numerical guides are used to define different probabilities, then units should be given. The probability scale needs to span the range relevant to the study in hand, remembering that the lowest probability must be acceptable for the highest defined consequence, otherwise all activities with the highest consequence are defined as intolerable. A part example is shown in Figure B.7.

A matrix is drawn with consequence on one axis and probability on the other. Figure B.8 shows part of an example matrix with a 6 point consequence and 5 point probability scales.

The risk levels assigned to the cells will depend on the definitions for the probability/ consequence scales. The matrix may be set up to give extra weight to consequences (as shown) or to probability, or it may be symmetrical, depending on the application. The levels of risk may be linked to decision rules such as the level of management attention or the time scale by which response is needed.

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro • Pressu	• Major litigation costing $10m+ • Investigation by regulator body resulting in lon Interruption to
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or Irrevers	• Major spi		
3	$100k – $90 loss or gain					
2	$10 lo					
1						

IEC 2074/09

Figure B.13 – Part example of a consequence criteria table

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mo
Unlikely	- may occur but not - could occur in "
Rare	- occurrence re - exceptional' - only occ
Remote	- theor - fr

IEC 2075/09

Figure B.14 – Part example of a risk ranking matrix

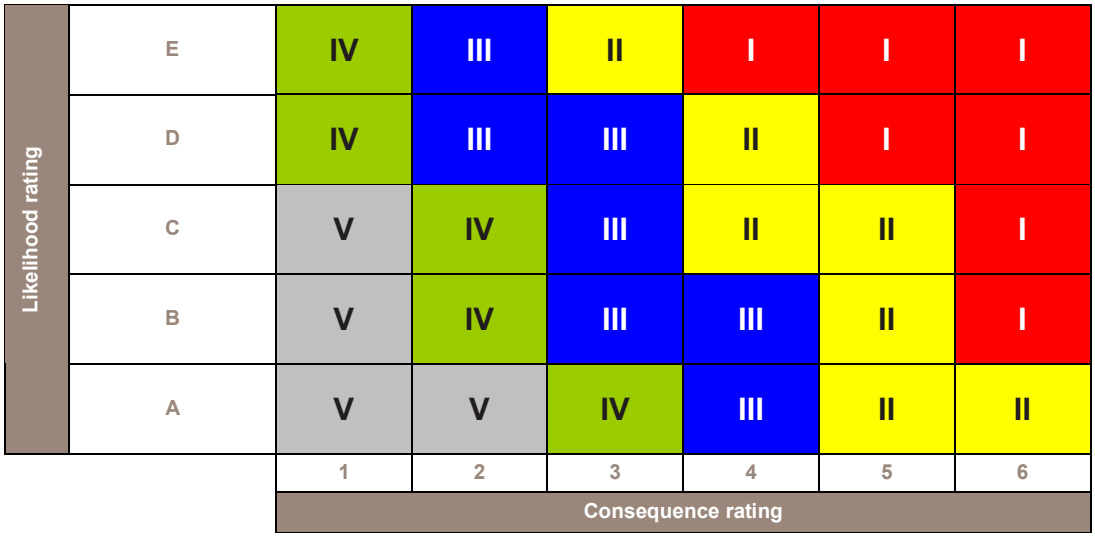

Figure B.15 – Part example of a probability criteria matrix

Rating scales and a matrix may be set up with quantitative scales. For example, in a reliability context the probability scale could represent indicative failure rates and the consequence scale the dollar cost of failure.

Use of the tool needs people (ideally a team) with relevant expertise and such data as is available to help in judgements of consequence and probability.

B.29.4 Process

To rank risks, the user first finds the consequence descriptor that best fits the situation then defines the probability with which those consequences will occur. The level of risk is then read off from the matrix.

Many risk events may have a range of outcomes with different associated probability. Usually, minor problems are more common than catastrophes. There is therefore a choice as to whether to rank the most common outcome or the most serious or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as these pose the largest threat and are often of most concern. In some cases, it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important that the probability relevant to the selected consequence is used and not the probability of the event as a whole.

The level of risk defined by the matrix may be associated with a decision rule such as to treat or not to treat the risk.

B.29.5 Output

The output is a rating for each risk or a ranked list of risk with significance levels defined.

B.29.6 Strengths and limitations

Strengths:

- relatively easy to use;
- provides a rapid ranking of risks into different significance levels.

Limitations:

- a matrix should be designed to be appropriate for the circumstances so it may be difficult to have a common system applying across a range of circumstances relevant to an organization;
- it is difficult to define the scales unambiguously;
- use is very subjective and there tends to be significant variation between raters;
- risks cannot be aggregated (i.e. one cannot define that a particular number of low risks or a low risk identified a particular number of times is equivalent to a medium risk);
- it is difficult to combine or compare the level of risk for different categories of consequences.

Results will depend of the level of detail of the analysis, i.e. the more detailed the analysis, the higher the number of scenarios, each with a lower probability. This will underestimate the actual level of risk. The way in which scenarios are grouped together in describing risk should be consistent and defined at the start of the study.

B.30 Cost/benefit analysis (CBA)

B.30.1 Overview

Cost/benefit analysis can be used for risk evaluation where total expected costs are weighed against the total expected benefits in order to choose the best or most profitable option. It is an implicit part of many risk evaluation systems. It can be qualitative or quantitative or involve a combination of quantitative and qualitative elements. Quantitative CBA aggregates the monetary value of all costs and all benefits to all stakeholders that are included in the scope and adjusts for different time periods in which costs and benefits accrue. The net present value (NPV) which is produced becomes an input into to decisions about risk. A positive NPV associated with an action would normally mean the action should occur. However, for some negative risks, particularly those involving risks to human life or damage to the environment the ALARP principle may be applied. This divides risks into three regions: a level above which negative risks are intolerable and should not be taken except in extraordinary circumstances; a level below which risks are negligible and need only to be monitored to ensure they remain low; and a central band where risks are made as low as reasonably practicable (ALARP). Towards the lower risk end of this region, a strict cost benefit analysis may apply but where risks are close to intolerable, the expectation of the ALARP principle is that treatment will occur unless the costs of treatment are grossly disproportionate to the benefit gained.

B.30.2 Uses

Cost/benefit analysis can be used to decide between options which involve risk.

For example

- as input into a decision about whether a risk should be treated,
- to differentiate between and decide on the best form of risk treatment,
- to decide between different courses of action.

B.30.3 Inputs

Inputs include information on costs and benefits to relevant stakeholders and on uncertainties in those costs and benefits. Tangible and intangible costs and benefits should be considered. Costs include resources expended and negative outcomes, benefits include positive outcomes, negative outcomes avoided and resources saved.

B.30.4 Process

The stakeholders who may experience costs or receive benefits are identified. In a full cost benefit analysis all stakeholders are included.

The direct and indirect benefits and costs to all relevant stakeholders of the options being considered are identified. Direct benefits are those which flow directly from the action taken, while indirect or ancillary benefits are those which are coincidental but might still contribute significantly to the decision. Examples of indirect benefits include reputation improvement, staff satisfaction and “peace of mind”. (These are often weighted heavily in decision-making).

Direct costs are those that are directly associated with the action. Indirect costs are those additional, ancillary and sunk costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments. When applying a cost benefit analysis to a decision on whether to treat a risk, costs and benefits associated with treating the risk, and with taking the risk, should be included

In quantitative cost/benefit analysis, when all tangible and intangible costs and benefits have been identified, a monetary value is assigned to all costs and benefits (including intangible costs and benefits). There are a number of standard ways of doing this including the ‘willingness to pay’ approach and using surrogates. If, as often happens, the cost is incurred over a short period of time (e.g. a year) and the benefits flow for a long period thereafter, it is normally necessary to discount the benefits to bring them into “today’s money” so that a valid comparison can be obtained. All costs and benefits are expressed as a present value. The present value of all costs and all benefits to all stakeholders can be combined to produce a net present value (NPV). A positive NPV implies that the action is beneficial. Benefit cost ratios are also used see B30.5

If there is uncertainty about the level of costs or benefits, either or both terms can be weighted according to their probabilities.

In qualitative cost benefit analysis no attempt is made to find a monetary value for intangible costs and benefits and, rather than providing a single figure summarizing the costs and benefits, relationships and trade-offs between different costs and benefits are considered qualitatively.

A related technique is a cost-effectiveness analysis. This assumes that a certain benefit or outcome is desired, and that there are several alternative ways to achieve it. The analysis looks only at costs and which is the cheapest way to achieve the benefit.

B.30.5 Output

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions. This may be expressed quantitatively as a net present value (NPV) an internal rate of return (IRR) or as the ratio of the present value of benefits to the present value of costs. Qualitatively the output is usually a table comparing costs and benefits of different types of cost and benefit, drawing attention to trade offs.

B.30.6 Strengths and limitations

Strengths of cost benefit analysis:

- it allows costs and benefits to be compared using a single metric (money);
- it provides transparency of decision making;
- it requires detailed information to be collected on all possible aspects of the decision. This can be valuable in revealing ignorance as well as communicating knowledge.

Limitations:

- quantitative CBA can yield dramatically different numbers, depending on the methods used to assign economic values to non-economic benefits;
- in some applications it is difficult to define a valid discounting rate for future costs and benefits;

- benefits which accrue to a large population are difficult to estimate, particularly those relating to public good which is not exchanged in markets;
- the practice of discounting means that benefits gained in the long term future have negligible influence on the decision depending on the discounting rate chosen. The method becomes unsuitable for consideration of risks affecting future generations unless very low or zero discount rates are set.

B.31 Multi-criteria decision analysis (MCDA)

B.31.1 Overview

The objective is to use a range of criteria to objectively and transparently assess the overall worthiness of a set of options. In general, the overall goal is to produce a preference of order between the available options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.

B.31.2 Use

MCDA can be used for

- comparing multiple options for a first pass analysis to determine preferred and potential options and inappropriate option,
- comparing options where there are multiple and sometimes conflicting criteria,
- reaching a consensus on a decision where different stakeholders have conflicting objectives or values.

B.31.3 Inputs

A set of options for analysis. Criteria, based on objectives that can be used equally across all options to differentiate between them.

B.31.4 Process

In general a group of knowledgeable stakeholders undertakes the following process:

a) define the objective(s);
b) determine the attributes (criteria or performance measures) that relate to each objective;
c) structure the attributes into a hierarchy;
d) develop options to be evaluated against the criteria;
e) determine the importance of the criteria and assign corresponding weights to them;
f) evaluate the alternatives with respect to the criteria. This may be represented as a matrix of scores.
g) combine multiple single-attribute scores into a single aggregate multi attribute score;
h) evaluate the results.

There are different methods by which the weighting for each criteria can be elicited and different ways of aggregating the criteria scores for each option into a single multi-attribute score. For example, scores may be aggregated as a weighted sum or a weighted product or using the analytic hierarchy process, an elicitation technique for the weights and scores based on pairwise comparisons. All these methods assume that the preference for any one criterion does not depend on the values of the other criteria. Where this assumption is not valid, different models are used.

Since scores are subjective, sensitivity analysis is useful to examine the extent to which the weights and scores influence overall preferences between options.

B.31.5 Outputs

Rank order presentation of the options goes from best to least preferred. If the process produces a matrix where the axes of the matrix are criteria weighted and the criteria score for each option, then options that fail highly weighted criteria can also be eliminated.

B.31.6 Strengths and limitations

Strengths:

- provides a simple structure for efficient decision-making and presentation of assumptions and conclusions;
- can make complex decision problems, which are not amenable to cost/benefit analysis, more manageable;
- can help rationally consider problems where tradeoffs need to be made;
- can help achieve agreement when stakeholders have different objectives and hence criteria.

Limitations:

- can be affected by bias and poor selection of the decision criteria;
- most MCDA problems do not have a conclusive or unique solution;
- aggregation algorithms which calculate criteria weights from stated preferences or aggregate differing views can obscure the true basis of the decision.

Bibliography

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

IEC 61649, *Weibull analysis*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*[2]

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

_____

2 Currently under consideration.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DES RISQUES – TECHNIQUES D'ÉVALUATION DES RISQUES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). 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 les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI 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/ISO 31010 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement et le groupe de travail «Gestion des risques» de l'ISO TMB.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1329/FDIS	56/1346/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. A l'ISO, la norme a été approuvée par 17 comités membres sur 18 ayant votés.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les organisations de tout type et de toute taille font face à un éventail de risques susceptibles d'avoir un impact sur la réalisation de leurs objectifs.

Il peut s'agir de leurs activités (de leurs initiatives stratégiques à leurs opérations, processus et projets) qui peuvent avoir des conséquences en termes de résultats sociétaux, environnementaux, technologiques, de sécurité et sûreté, de mesures commerciales, financières et économiques, et avoir des impacts sociaux, culturels, politiques et toucher à la réputation de l'organisation.

Toute activité d'une organisation implique des risques qu'il convient de gérer. Le processus de gestion des risques facilite la prise de décision. Il s'agit en effet de tenir compte de l'incertitude, d'éventuels événements ou de certaines circonstances (prévus ou imprévus) et de leurs effets sur les objectifs fixés.

La gestion des risques comprend l'application de méthodes logiques et systématiques permettant:

- de communiquer et de consulter tout au long de ce processus;
- d'établir le contexte de l'organisation afin d'identifier, d'analyser, d'évaluer et de traiter le risque lié à une activité, un processus, une fonction ou un produit;
- de surveiller et d'examiner l'évolution des risques;
- de rapporter et de consigner les résultats de manière appropriée.

L'évaluation des risques fait partie intégrante de la gestion des risques. Elle consiste à fournir un processus structuré permettant d'identifier dans quelle mesure les objectifs peuvent être affectés, et d'analyser les conséquences et la probabilité d'occurrence des risques avant de décider s'il est nécessaire de procéder à un traitement supplémentaire.

L'évaluation des risques tente de répondre aux questions essentielles suivantes:

- que se passe-t-il et pourquoi (par identification des risques) ?
- quelles sont les conséquences ?
- quelle est la probabilité d'occurrence ?
- existe-t-il des facteurs permettant de limiter la conséquence du risque ou de réduire la probabilité d'occurrence du risque ?

Le niveau de risque est-il tolérable ou acceptable et nécessite-t-il un traitement supplémentaire ? La présente norme est destinée à refléter les bons usages actuels en matière de choix et d'utilisation des techniques d'évaluation des risques et ne fait pas référence à des notions nouvelles ou en cours de développement n'ayant 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'évaluation pour des applications particulières. Si ces normes ont été élaborées en harmonie avec la présente norme, les normes spécifiques seront généralement suffisantes.

GESTION DES RISQUES – TECHNIQUES D'ÉVALUATION DES RISQUES

1 Domaine d’application

La présente Norme internationale est une norme d’accompagnement de l’ISO 31000 et fournit des lignes directrices permettant de choisir et d'appliquer des techniques systématiques d'évaluation des risques.

L'évaluation des risques réalisée conformément à la présente norme contribue aux autres activités de gestion des risques.

L'application de certaines techniques est présentée, avec des références spécifiques à d'autres normes internationales dans lesquelles la notion et l'application des techniques sont décrites plus en détail.

La présente norme n’est pas destinée à être utilisée à des fins de certification, de réglementation ou contractuelles.

La présente norme ne fournit pas de critères particuliers permettant d'identifier s'il est nécessaire de procéder à une évaluation des risques. Elle ne précise pas non plus la méthode d'évaluation des risques nécessaire pour une application donnée.

La présente norme ne spécifie pas toutes les techniques et de ce fait l’absence d’une technique n’implique pas qu’elle n’est pas valable. Le fait qu’une méthode soit applicable à une circonstance particulière n’implique pas qu’il convient nécessairement de l’appliquer.

NOTE La présente norme ne traite pas spécifiquement de la sécurité. C'est une norme générale de gestion des risques et toute référence à la sécurité est purement de nature informative. Les lignes directrices sur l'introduction des aspects de sécurité dans les normes CEI est définie dans le Guide ISO/CEI 51.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Guide ISO/CEI 73, *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes*

ISO 31000, *Management du risque – Principes et lignes directrices*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions du Guide ISO/CEI 73 s'appliquent.

4 Concepts d'évaluation des risques

4.1 Objet et avantages

L'évaluation des risques a pour objet de fournir des informations et une analyse factuelles permettant de prendre des décisions avisées sur la manière de traiter des risques particuliers et faire un choix parmi différentes options.

L'évaluation des risques présente certains des principaux avantages suivants:

- compréhension du risque et de son impact potentiel sur les objectifs;
- apport d'informations pour la prise de décision;
- participation à la compréhension des risques afin de faciliter la sélection des options de traitement;
- identification des principaux facteurs contribuant aux risques et des maillons faibles d'un système ou d'une organisation;
- comparaison des risques avec ceux d'autres systèmes, technologies ou approches;
- communication sur les risques et incertitudes;
- aide à l'établissement de priorités;
- prévention des accidents fondée sur une enquête post-accidentelle;
- choix entre différentes formes de traitement du risque;
- satisfaction à des exigences réglementaires;
- apport d'informations permettant d'évaluer le niveau de tolérance au risque en fonction de critères préalablement définis;
- évaluation des risques liés à la mise au rebut en fin de vie.

4.2 Évaluation des risques et cadre de gestion des risques

La présente norme suppose que l'évaluation des risques est réalisée dans le cadre et le processus de gestion des risques décrit dans l'ISO 31000.

Un cadre de gestion des risques fournit les règles, les procédures et les dispositions organisationnelles intégrant la gestion des risques à tous les niveaux de l'organisation.

Dans ce cadre, il convient que l'organisation dispose de règles ou d'une stratégie permettant de décider du moment et de la manière dont il convient d'évaluer les risques.

En particulier, il convient que les responsables chargés de l'évaluation des risques soient bien informés des éléments suivants:

- le contexte et les objectifs de l'organisation;
- l'étendue et le type de risques tolérables et la manière dont doivent être traités les risques inacceptables;
- la manière dont l'évaluation des risques est intégrée dans les processus de l'organisation;
- les méthodes et techniques à utiliser pour évaluer les risques et leur contribution au processus de gestion des risques;
- le rapporteur, la responsabilité et l'autorité en matière d'évaluation des risques;
- les ressources disponibles pour évaluer les risques;
- la manière dont l'évaluation des risques sera rapportée et examinée.

4.3 Evaluation des risques et processus de gestion des risques

4.3.1 Généralités

L'évaluation des risques reprend les éléments fondamentaux du processus de gestion des risques définis dans l'ISO 31000, et traite des éléments suivants:

- communication et consultation;
- établissement du contexte;
- évaluation des risques (comprenant leur identification, leur analyse et leur évaluation);
- traitement des risques;
- contrôle et examen.

L'évaluation des risques n'est pas une activité autonome. Il convient qu'elle soit totalement intégrée aux autres composantes du processus de gestion des risques.

4.3.2 Communication et consultation

Le succès de l'évaluation des risques dépend de l'efficacité de la communication et de la consultation avec les différents acteurs.

L'implication des acteurs dans le processus de gestion des risques est nécessaire pour

- développer un plan de communication,
- définir le contexte de manière appropriée,
- s'assurer de la bonne compréhension et prise en compte des intérêts des acteurs,
- rassembler différents domaines d'expertise pour identifier et analyser les risques,
- s'assurer de la bonne prise en compte des différents points de vue dans l'évaluation des risques,
- faciliter l'identification appropriée des risques,
- l'application et la prise en charge sécurisée d'un plan de traitement.

Il convient que les acteurs jouent le rôle d'interface entre le processus d'évaluation des risques et des autres disciplines de gestion, notamment pour modifier la gestion, le projet et la gestion du programme, ainsi que la gestion financière.

4.3.3 Etablissement du contexte

L'établissement du contexte permet de définir les paramètres de base en matière de gestion des risques, ainsi que le domaine d'application et les critères pour le reste du processus. Il s'agit de tenir compte des paramètres internes et externes liés à l'ensemble de l'organisation, ainsi que du retour d'expérience relatif aux risques particuliers en cours d'évaluation.

Dans ce cadre, les objectifs d'évaluation des risques, les critères de risque et le programme d'évaluation des risques sont déterminés et font l'objet d'un accord.

Pour évaluer un risque particulier, il convient que l'établissement du contexte intègre la définition des contextes externe, interne et de gestion des risques ainsi que la classification des critères de risque:

a) L'établissement du contexte externe implique de se familiariser avec l'environnement dans lequel l'organisation et le système évoluent, notamment:

   - les facteurs d'environnement culturels, politiques, juridiques, réglementaires, financiers, économiques et compétitifs, internationaux, nationaux, régionaux ou locaux;

- les principaux éléments et tendances ayant un impact sur les objectifs de l'organisation; et
- les perceptions et valeurs des acteurs externes.

b) L'établissement du contexte interne implique la compréhension

- des capacités de l'organisation en termes de ressources et de connaissance,
- des flux d'informations et des processus de prise de décision,
- des acteurs internes,
- des objectifs et des stratégies en place pour les atteindre,
- des perceptions, des valeurs et de la culture,
- des règles et des processus,
- des normes et des modèles de référence adoptés par l'organisation, et
- des structures (gouvernance, rôles et responsabilités, par exemple).

c) L'établissement du contexte du processus de gestion des risques implique:

- de définir les rapporteurs et les responsabilités;
- de définir l'étendue des activités de gestion des risques à réaliser, y compris les inclusions et exclusions spécifiques;
- de définir l'étendue du projet, du processus, des fonctions ou de l'activité en termes de durée et de lieu;
- de définir les relations entre un projet ou activité particulier et d'autres projets ou activités de l'organisation;
- de définir les méthodologies d'évaluation des risques;
- de définir les critères de risque;
- de définir les moyens d'évaluation de la gestion des risques;
- d'identifier et de préciser les décisions à prendre et les actions à entreprendre et
- d'identifier les études de définition ou de cadrage nécessaires, leur étendue, leurs objectifs et les ressources requises.

d) La phase de définition des critères de risque comprend :

- la nature et les types de conséquences à inclure et la manière de les mesurer,
- la manière d'exprimer la probabilité,
- la manière de déterminer un niveau de risque,
- les critères permettant de décider s'il est nécessaire de traiter un risque,
- les critères permettant de décider si un risque est acceptable et/ou tolérable,
- si des combinaisons de risques seront prises en compte et la manière dont elles le seront.

Les critères peuvent reposer sur des sources telles que

- les objectifs fixés du processus,
- les critères identifiés dans les spécifications,
- les sources de données générales,
- les critères industriels communément acceptés (les niveaux d'intégrité de la sécurité, par exemple),
- la volonté de prise de risque de l'organisation,

- les exigences juridiques, entre autres, pour les équipements ou applications particulières.

4.3.4 Evaluation des risques

L'évaluation des risques est le processus global d'identification, d'analyse et d'évaluation des risques.

Les risques peuvent être évalués au niveau de l'organisation, au niveau inférieur (départemental), pour des projets, des activités individuelles ou des risques particuliers. Différents outils et différentes techniques peuvent être adaptés à différents contextes.

L'évaluation des risques permet de bien appréhender les risques, leurs causes, leurs conséquences et la probabilité d'occurrence. Elle offre des éléments de décisions sur les éléments suivants:

- la nécessité de réaliser ou non une activité;
- la manière d'optimiser les opportunités;
- la nécessité de traiter les risques;
- le choix entre différentes options aux risques différents;
- les priorités des options de traitement;
- le choix des stratégies appropriées de traitement des risques visant à ramener les risques à un niveau tolérable.

4.3.5 Traitement des risques

L'évaluation des risques étant réalisée, le traitement des risques implique de choisir et d'accepter une ou plusieurs options pertinentes visant à modifier la probabilité d'occurrence, les effets des risques, ou les deux, et de mettre en place ces options.

Cette étape est suivie d'un processus cyclique de réévaluation du nouveau niveau de risque, en veillant à déterminer son niveau de tolérance par rapport aux critères préalablement définis, afin de décider de la nécessité de la mise en place d'un traitement approfondi.

4.3.6 Contrôle et examen

Dans le cadre du processus de gestion des risques, il convient de surveiller et d'examiner régulièrement les risques et leur surveillance pour s'assurer que

- les hypothèses concernant les risques sont toujours valides;
- les hypothèses sur lesquelles repose l'évaluation des risques (le contexte externe et interne, en particulier) sont toujours valides;
- les résultats prévus sont sur le point d'être atteints;
- les résultats de l'évaluation des risques sont en accord avec l'expérience réelle;
- les techniques d'évaluation des risques sont correctement appliquées;
- les traitements des risques sont efficaces.

Il convient d'établir la responsabilité du contrôle et des examens.

5 Processus d'évaluation des risques

5.1 Présentation

L'évaluation des risques permet aux décideurs et aux responsables de mieux appréhender les risques susceptibles d'avoir un impact sur les objectifs, ainsi que la pertinence et l'efficacité

des contrôles déjà en place. Cela permet de décider de l'approche la plus pertinente pour traiter les risques. Les résultats de l'évaluation des risques doivent être utilisés pour alimenter les processus de prise de décision de l'organisation.

L'évaluation des risques est le processus global d'identification, d'analyse et d'évaluation des risques (voir la Figure 1). La manière d'appliquer ce processus ne dépend pas seulement du contexte du processus de gestion des risques, mais également des méthodes et des techniques utilisées pour évaluer les risques.

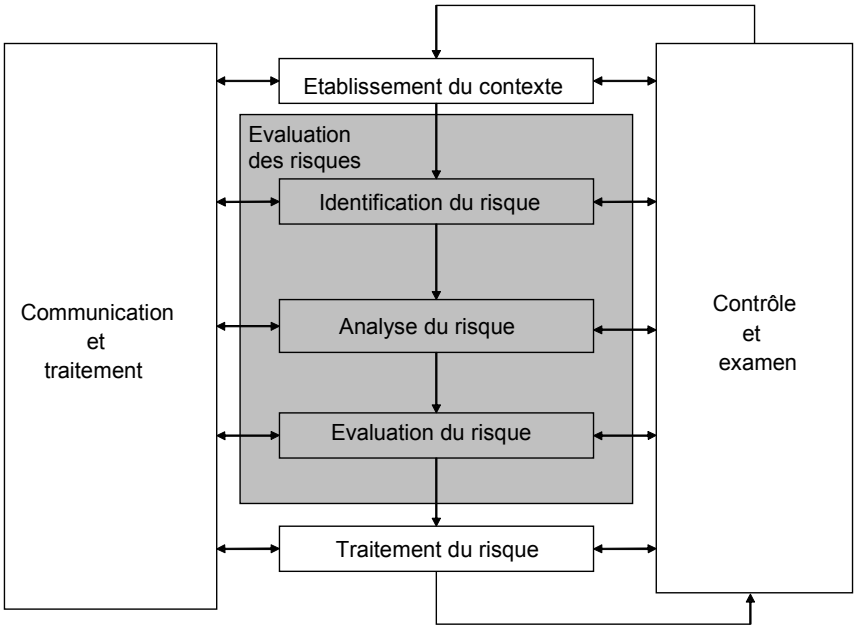

Figure 1 – Contribution de l'évaluation des risques au processus de gestion des risques

L'évaluation des risques peut nécessiter une approche pluridisciplinaire étant donné que les risques peuvent couvrir un large éventail de causes et de conséquences.

5.2 Identification des risques

L'identification des risques est le processus de recherche, de reconnaissance et d'enregistrement des risques.

L'identification des risques a pour objet d'identifier les raisons pour lesquelles les objectifs du système ou de l'organisation pourraient ne pas être atteints. Une fois les risques identifiés, il convient que l'organisation identifie tous les contrôles existants tels que les fonctions, les personnes, les processus et les systèmes.

Le processus d'identification des risques comprend l'identification des causes et de l'origine des risques (risque dans le contexte d'une blessure), des événements, des situations ou des circonstances susceptibles d'avoir un impact matériel sur les objectifs et la nature de cet impact.

Les méthodes d'identification des risques peuvent inclure:

- des méthodes reposant sur la preuve (des listes de contrôle et des examens des données historiques, par exemple);

- les approches systématiques en équipe, dans laquelle une équipe d'experts suit un processus systématique d'identification des risques au moyen d'un ensemble structuré d'invites ou de questions;
- des techniques de raisonnement inductif, telles que HAZOP[1].

Différentes techniques peuvent être utilisées pour améliorer la précision et l'exhaustivité de l'identification des risques, notamment le «brainstorming» et la méthodologie Delphi.

Quelles que soient les techniques actuelles utilisées, il est important, dans le processus global d'identification des risques, d'accorder une importance particulière aux facteurs humains et organisationnels. Par conséquent, il convient d'inclure les variations humaines et organisationnelles dans le processus d'identification des risques, conjointement aux éléments «matériels» ou «logiciels».

5.3 Analyse des risques

5.3.1 Généralités

L'analyse des risques consiste à comprendre et à étudier profondément les risques. Elle constitue une donnée d'entrée de l'évaluation des risques et dans la prise de décision sur la nécessité de traiter les risques et sur les stratégies ou méthodes de traitement les plus appropriées.

L'analyse des risques consiste à déterminer les conséquences et les probabilités pour les risques identifiés en tenant compte de la présence (ou non) et de l'efficacité des contrôles existants. Probabilité et conséquence associée sont alors combinées pour déterminer le niveau de risque.

L'analyse des risques implique de tenir compte des causes et des sources du risque ainsi que de leurs conséquences et de la probabilité de leur occurrence. Il convient d'identifier les facteurs ayant un effet sur les conséquences et la probabilité. Un événement peut avoir plusieurs conséquences et peut affecter plusieurs objectifs. Il convient de tenir compte des contrôles de risque existants et de leur efficacité. Différentes méthodes d'analyse sont présentées dans l'Annexe B. Pour des applications complexes, il peut se révéler nécessaire d'appliquer plusieurs techniques.

En règle générale, l'analyse des risques comprend une estimation de l'ensemble des conséquences potentielles susceptibles de résulter d'un événement, d'une situation ou d'une circonstance, et des probabilités associées, afin de mesurer le niveau de risque. Cependant, dans certains cas, par exemple lorsque les conséquences sont probablement négligeables ou que la probabilité prévue est extrêmement faible, il peut être suffisant de n'estimer qu'un seul paramètre pour prendre une décision.

Dans certaines circonstances, une conséquence peut résulter d'un ensemble de différents événements ou de différentes conditions, ou lorsqu'un événement particulier n'est pas identifié. Dans ce cas, l'évaluation des risques porte sur l'analyse de l'importance et de la vulnérabilité des composants du système afin de définir les traitements associés aux niveaux de protection ou aux stratégies de remise en état.

Les méthodes utilisées dans l'analyse des risques peuvent être qualitatives, semi-quantitatives ou quantitatives. Le degré de précision requis dépend de l'application particulière, de la disponibilité de données fiables et des besoins de prise de décision de l'organisation. Certaines méthodes et le degré de précision de l'analyse peuvent être déterminés par la loi.

---

1 HAZOP = *Hazard and Operability Studies*

L'évaluation qualitative définit les conséquences, la probabilité et le niveau de risque par des termes comme «élevé», «moyen» et «faible» et peut combiner conséquence et probabilité pour évaluer le niveau de risque qui en découle en fonction de critères qualitatifs.

Les méthodes semi-quantitatives utilisent des échelles d'évaluation numérique de probabilité et de conséquence et les combinent pour obtenir un niveau de risque grâce à une formule. Les échelles peuvent être linéaires ou logarithmiques ou faire l'objet d'autres relations, les formules utilisées pouvant également varier.

L'analyse quantitative estime les conséquences et la probabilité liées à des valeurs réalistes et produit des valeurs de niveau de risque dans des unités spécifiques définies lors du développement du contexte. Il n'est pas toujours possible ou souhaitable de procéder à une analyse quantitative complète en raison d'informations insuffisantes relatives au système ou à l'activité en cours d'analyse, du manque de données, de l'influence de facteurs humains, etc. ou parce que le résultat de l'analyse quantitative n'est pas garanti ou nécessaire. Dans ces circonstances, il peut s'avérer judicieux de faire appel à des spécialistes reconnus dans leurs domaines respectifs pour procéder à un classement semi-quantitatif ou qualitatif, comparatif des risques.

Dans le cas d'une analyse qualitative, il convient que tous les termes utilisés soient clairement expliqués et que la base de tous les critères soit enregistrée.

Même si une quantification exhaustive a été réalisée, il faut admettre que tous les niveaux de risque calculés ne sont que des estimations. Il convient de veiller à s'assurer que leur niveau de précision et d'exactitude n'est pas incompatible avec la précision des données et méthodes d'analyse utilisées.

Il convient d’exprimer les niveaux de risque dans les termes les plus adaptés au type de risque et d'une manière facilitant l'évaluation des risques. Dans certains cas, un risque peut être exprimé sous la forme d'une distribution de probabilité sur un ensemble de conséquences.

5.3.2 Evaluation des contrôles

Le niveau de risque dépend de l’adéquation et de l’efficacité des contrôles existants. Cela implique de répondre aux questions suivantes:

- quels sont les contrôles existants liés à un risque particulier?
- ces contrôles sont-ils en mesure de traiter le risque de manière à le maintenir à un niveau tolérable?
- dans la pratique, les contrôles fonctionnent-ils comme prévu et leur efficacité peut-elle être démontrée, le cas échéant?

Il est possible de répondre à ces questions avec certitude uniquement s’il existe une documentation pertinente et si un processus d’assurance adapté a été mis en place.

Le niveau d’efficacité d’un contrôle particulier ou d’une suite de contrôles connexes peut être exprimé de manière qualitative, semi-quantitative ou quantitative. Dans la plupart des cas, un niveau élevé de précision n’est pas garanti. Toutefois, il peut être intéressant d’exprimer et d’enregistrer la mesure de l’efficacité du contrôle des risques de manière à pouvoir émettre un avis sur l’effort à porter pour améliorer le contrôle ou par un traitement différent des risques.

5.3.3 Analyse des conséquences

L'analyse des conséquences permet de déterminer la nature et le type d’impact susceptible de se produire, en supposant que des événements ou des circonstances particuliers se sont produits. Un événement peut avoir une série d’impacts de gravité différente et affecter un

ensemble d'objectifs et d'acteurs différents. Les types de conséquence à analyser et les acteurs concernés auront été définis lors de l'établissement du contexte.

L'analyse des conséquences peut s'étendre d'une simple description des résultats à une modélisation quantitative détaillée ou une analyse de vulnérabilité.

Les impacts peuvent avoir une conséquence faible mais une probabilité élevée, ou une conséquence élevée et une faible probabilité, ou des résultats intermédiaires. Dans certains cas, il est pertinent de mettre l'accent sur les risques présentant des résultats potentiellement très variés donc faisant souvent l'objet d'une attention particulière de la part des décideurs. Dans d'autres cas, il peut être important d'analyser les risques à conséquence élevée et faible de manière séparée. Par exemple, un problème fréquent mais à faible impact (ou chronique) peut avoir des effets cumulés ou à long terme importants. Par ailleurs, les traitements appliqués à ces deux différents types de risques sont souvent tout à fait différents, ce qui justifie donc de les analyser séparément.

L'analyse des conséquences peut impliquer:

- de tenir compte de considérations liées aux contrôles existants afin de traiter les conséquences avec tous les facteurs contributifs pertinents ayant un effet sur les conséquences;
- d'associer les conséquences du risque aux objectifs d'origine;
- de tenir compte des conséquences immédiates et de celles susceptibles de survenir ultérieurement, si cela est cohérent avec le domaine d'application de l'évaluation;
- de tenir compte des conséquences secondaires comme celles ayant un impact sur les systèmes, activités, équipements ou organisations connexes.

5.3.4 Analyse de vraisemblance et estimation de la probabilité

Trois approches générales sont couramment utilisées pour estimer la probabilité. Elles peuvent être utilisées individuellement ou conjointement:

a) Utilisation de données historiques pertinentes afin d'identifier des événements ou des situations qui se sont produits dans le passé et ainsi extrapoler la probabilité de leur occurrence dans le futur. Il convient que les données utilisées soient adaptées au type de système, d'installation, d'organisation ou d'activité considéré et aux normes de fonctionnement de l'organisation considérée. Si, du point de vue historique, la fréquence d'occurrence est très faible, il peut s'avérer impossible d'estimer la probabilité. Cela concerne particulièrement les occurrences nulles, lorsque personne ne suppose que l'événement, la situation ou la circonstance va se produire dans le futur.

b) Prévision des probabilités à l'aide de techniques prédictives telles que l'analyse par arbre de panne et l'analyse par arbre d'événements (voir Annexe B). Si les données historiques ne sont pas disponibles ou appropriées, il est nécessaire de déduire les probabilités par une analyse du système, de l'activité, de l'équipement ou de l'organisation ainsi que l'échec ou la réussite qui en découle. Les données numériques liées aux équipements, personnes, organisations et systèmes sur la base d'expériences opérationnelles ou de sources de données publiées sont alors combinées pour produire une estimation de la probabilité de l'événement de tête. Lorsque des techniques prédictives sont utilisées, il est important d'assurer que, lors de l'analyse, il a été dûment tenu compte de l'éventualité de défaillance de mode commun qui implique la défaillance de plusieurs pièces ou composants différents du système. Des techniques de simulation peuvent s'avérer nécessaires pour estimer la probabilité 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'avis d'un expert peut être utilisé dans un processus systématique et structuré pour estimer la probabilité. Il convient que ces avis experts se fondent sur toutes les informations disponibles applicables, y compris les données historiques, spécifiques au système et à l'organisation, expérimentales, de conception, etc. Il existe un certain nombre de méthodes formelles permettant d'obtenir des avis experts qui fournissent une

aide à la formulation de questions appropriées. Les méthodes disponibles comprennent l'approche Delphi, les méthodes de comparaison par paires, de catégorisation et de probabilité absolue.

5.3.5 Analyse préliminaire (dépistage des risques)

Il est possible de procéder à un dépistage des risques pour identifier les risques les plus significatifs, ou pour exclure les risques insignifiants ou mineurs de l'analyse ultérieure. L'objectif est d'assurer que les ressources sont concentrées sur les risques les plus importants. Il convient de ne pas négliger le dépistage des risques faibles qui surviennent fréquemment et qui ont un effet cumulé significatif.

Il convient que le dépistage repose sur des critères définis dans le contexte. L'analyse préliminaire permet de déterminer l'une des suites d'actions suivantes:

- décision de traiter les risques sans évaluation supplémentaire;
- définition de risques non significatifs collatéraux ne justifiant pas de traitement;
- poursuite par une évaluation plus détaillée des risques.

Il convient de documenter les hypothèses initiales et les résultats.

5.3.6 Incertitudes et sensibilités

Des incertitudes considérables sont souvent associées à l'analyse des risques. Il est nécessaire de bien cerner ces incertitudes pour interpréter et communiquer de manière efficace les résultats de l'analyse des risques. L'analyse des incertitudes liées aux données, aux méthodes et aux modèles utilisés pour identifier et analyser les risques joue un rôle important dans leur application. L'analyse de l'incertitude implique de déterminer la variation ou l'imprécision des résultats, à la suite de la variation collective des paramètres et des hypothèses utilisés pour définir les résultats. L'analyse de sensibilité est étroitement liée à **l'analyse de l'incertitude.**

L'analyse de sensibilité implique de déterminer l'importance et la signification du niveau de risque liées à la modification de paramètres d'entrée individuels. Elle permet de distinguer les données qui doivent être précises, de celles qui sont moins sensibles et dont les effets sur l'exactitude générale sont par conséquent moins importants.

Il convient d'établir l'exhaustivité et l'exactitude de l'analyse des risques de manière aussi complète que possible. Le cas échéant, il convient d'identifier les sources d'incertitude et il convient que cela concerne les incertitudes liées aux données et au modèle/méthode. Il convient de définir les paramètres auxquels l'analyse est sensible et le degré de sensibilité.

5.4 Evaluation des risques

Afin de déterminer l'importance du niveau et du type de risque, l'évaluation des risques implique de comparer des niveaux estimés de risque en fonction de critères de risque définis lors de l'établissement du contexte.

Cette évaluation s'appuie sur la compréhension des risques découlant de leur analyse afin de prendre des décisions portant sur des actions à venir. Les considérations éthiques, juridiques et financières, entre autres (notamment la perception des risques), sont également des éléments de décision.

Les décisions peuvent inclure les éléments suivants:

- la nécessité de traiter le risque;
- les priorités de traitement;
- s'il convient ou non de réaliser une activité;

- le nombre de cheminements qu'il convient de suivre.

La nature des décisions à prendre et les critères pris en compte dans ce cadre ont été choisis lors de l'établissement du contexte. Mais ces éléments doivent être approfondis à cette étape, les risques particuliers identifiés étant à présent mieux connus.

Le cadre le plus simple de définition des critères de risque est composé d'un seul niveau qui distingue les risques devant faire l'objet d'un traitement de ceux à ignorer. Cette méthode donne des résultats simples intéressants, mais ne reflète pas les incertitudes implicites en matière d'estimation des risques et de séparation entre les risques à traiter et ceux à ignorer.

La décision relative à l'éventuel traitement du risque et à la manière de l'appliquer peut dépendre des coûts et des avantages liés à la prise de risque et des coûts et avantages liés à la mise en œuvre de contrôles améliorés.

Une approche commune consiste à diviser les risques en trois bandes:

a) une bande supérieure dans laquelle le niveau de risque est considéré comme intolérable, quel que soit le bénéfice retiré de l'activité, et dans laquelle le traitement du risque est primordial quel que soit son coût;
b) une bande moyenne (ou zone «grise») dans laquelle les coûts et avantages sont pris en compte et les opportunités équilibrées en fonction des éventuelles conséquences;
c) une bande inférieure dans laquelle le niveau de risque est considéré comme négligeable ou si minime qu'aucun traitement n'est envisagé.

Le système de critères ALARP (aussi faible que possible de manière raisonnable)[2], utilisé dans des applications de sécurité se conforme à cette approche dans laquelle la bande moyenne comporte une échelle mobile correspondant aux risques faibles et permettant de comparer directement les coûts et les avantages, compte tenu du fait que pour les risques élevés, le potentiel de nuisance doit être réduit jusqu'à ce que le coût d'une réduction supplémentaire soit totalement disproportionné par rapport à l'avantage de sécurité obtenu.

5.5 Documentation

Il convient que le processus d'évaluation des risques soit documenté avec les résultats de l'évaluation. Il convient que les risques soient exprimés en termes compréhensibles et que les unités dans lesquelles est exprimé le niveau de risque soient claires.

La portée du rapport dépendra des objectifs et du domaine d'application de l'évaluation. Sauf pour les estimations très simples, la documentation peut comporter:

- les objectifs et le domaine d'application;
- la description des parties correspondantes du système et leurs fonctions;
- un résumé du contexte externe et interne de l'organisation et de la manière dont il est lié à la situation, au système ou aux circonstances objet de l'évaluation;
- les critères de risque appliqués et leur justification;
- les limitations, hypothèses et la justification des hypothèses;
- la méthodologie d'évaluation;
- les résultats d'identification des risques;
- les données, hypothèses, leurs sources et la validation;
- les résultats de l'analyse des risques et leur évaluation;
- l'analyse de sensibilité et d'incertitude;

---

2 ALARP = *As Low As Reasonably Practicable*

- les hypothèses critiques et autres facteurs devant faire l'objet d'une surveillance;
- la discussion des résultats;
- les conclusions et recommandations;
- les références.

Si l'évaluation des risques est requise pour appuyer un processus continu de gestion des risques, il convient qu'elle soit réalisée et documentée de façon à ce qu'elle puisse être maintenue tout au long du cycle de vie du système, de l'organisation, de l'équipement ou de l'activité. Il convient que l'évaluation soit tenue à jour au fur et à mesure de la disponibilité de nouvelles informations importantes et des modifications du contexte, conformément aux besoins du processus de gestion.

5.6 Contrôle et examen de l'évaluation des risques

Le processus d'évaluation des risques met en évidence le contexte et d'autres facteurs susceptibles de varier dans le temps et de modifier ou invalider l'évaluation des risques. Il convient de spécifiquement identifier ces facteurs pour contrôle et examen continus afin de pouvoir actualiser l'évaluation des risques si nécessaire.

Il convient également d'identifier et de recueillir les données à contrôler afin de pouvoir affiner l'évaluation des risques.

Il convient également de contrôler et de documenter l'efficacité des contrôles pour fournir des données à utiliser pour l'analyse des risques. Il convient de définir les responsabilités pour ce qui concerne la création et l'examen des preuves et de la documentation.

5.7 Application de l'évaluation des risques au cours du cycle de vie

Il est possible de considérer que le cycle de vie de la plupart des activités, projets et produits commence au concept et à la définition initiaux et se poursuit jusqu'à l'achèvement, qui peut inclure le déclassement et la mise au rebut du matériel.

Les risques peuvent être évalués à toutes les étapes du cycle de vie. D'une manière générale, ils le sont plusieurs fois à différents niveaux de détail, de manière à faciliter la prise de décision à chaque phase.

Les phases du cycle de vie répondent à différentes exigences et nécessitent d'appliquer différentes techniques. Par exemple, lors de la phase de conception et de définition, si une opportunité est identifiée, les risques peuvent être évalués pour décider de la poursuite ou de l'interruption.

Si plusieurs options sont disponibles, les risques peuvent être évalués pour mesurer d'autres concepts et déterminer plus facilement lequel offre le meilleur rapport entre les risques positifs et négatifs.

Lors de la phase de conception et de développement, l'évaluation des risques permet:

- d'assurer que les risques liés au système sont tolérables;
- de participer au processus d'amélioration de la conception;
- de participer aux études de rentabilité;
- d'identifier les risques ayant un impact sur les phases suivantes du cycle de vie.

Au fur et à mesure du déroulement de l'activité, il est possible d'évaluer les risques pour apporter des informations facilitant les procédures de développement pour les conditions normales et d'urgence.

6 Sélection des techniques d'évaluation des risques

6.1 Généralités

Le présent article explique comment sélectionner les techniques d'évaluation des risques. Les annexes répertorient et expliquent plus en détail l'ensemble des outils et techniques qu'il est possible d'utiliser pour réaliser ou faciliter le processus d'évaluation des risques. Il peut être parfois nécessaire d'utiliser plusieurs méthodes d'évaluation.

6.2 Sélection des techniques

L'évaluation des risques peut être réalisée à divers degrés de profondeur et de détail et par de nombreuses méthodes, de la plus simple à la plus complexe. Il convient que la forme de l'évaluation et son résultat soient cohérents avec les critères de risque développés dans le cadre de l'établissement du contexte. L'Annexe A illustre les relations conceptuelles entre les différentes catégories de techniques d'évaluation des risques et les facteurs liés à une situation à risque donnée. Elle donne des exemples sur la manière dont les organisations peuvent sélectionner les techniques d'évaluation des risques appropriées pour une situation particulière.

De manière générale, il convient qu'une technique adaptée possède les caractéristiques suivantes:

- il convient qu'elle soit justifiée et adaptée à la situation ou à l'organisation considérée;
- il convient 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 traités;
- il convient qu'elle soit utilisée de telle sorte qu'elle soit traçable, reproductible et vérifiable.

Il convient de justifier du choix des techniques en tenant compte de leur pertinence et de leur convenance. Lorsqu'il s'agit d'intégrer les résultats de diverses études, il convient que les techniques et les données obtenues en sortie soient comparables.

Une fois prise la décision d'effectuer une évaluation des risques et une fois définis les objectifs et le domaine d'application, il convient de choisir la ou les techniques sur la base de facteurs applicables, tels que:

- les objectifs de l'étude. Les objectifs de l'évaluation des risques auront un effet direct sur les techniques utilisées. Par exemple, s'il est entrepris une étude comparative entre différentes options, il peut être acceptable d'utiliser des modèles de conséquence moins détaillés pour les parties du système qui ne sont pas affectées par les différences d'options;
- les besoins des décideurs. Dans certains cas, un niveau de détail élevé est nécessaire pour prendre une bonne décision, alors que dans d'autres cas, une compréhension plus générale est suffisante;
- le type et l'ensemble des risques en cours d'analyse;
- l'amplitude potentielle des conséquences. Il convient que la décision prise quant au niveau de profondeur de l'évaluation des risques reflète la perception initiale des conséquences (même s'il peut s'avérer nécessaire de la modifier après réalisation d'une évaluation préliminaire);
- le degré de compétence, ainsi que les besoins en ressources humaines et autres. Une méthode simple, correctement mise en œuvre, peut souvent donner de meilleurs résultats qu'une procédure plus sophistiquée d'application médiocre, si elle satisfait aux objectifs et au domaine d'application de l'évaluation. En général, il convient que l'investissement dans l'évaluation soit cohérent avec le niveau potentiel de risque analysé;

- la disponibilité des informations et des données. Certaines techniques nécessitent plus d'informations et de données que d'autres;
- la modification/mise à jour nécessaire de l'évaluation des risques. Il est admis que l'évaluation puisse nécessiter des modifications/mises à jour futures et qu'à cet égard, certaines techniques soient, plus que d'autres, susceptibles d'être modifiées;
- toutes exigences réglementaires et contractuelles.

Différents facteurs influencent le choix d'une approche de l'évaluation des risques, comme les ressources disponibles, la nature et le degré d'incertitude des données et informations disponibles, ainsi que la complexité de l'application (voir Tableau A.2).

6.3 Disponibilité des ressources

Les ressources et capacités pouvant avoir un impact sur le choix des techniques d'évaluation des risques comprennent:

- les compétences, l'expérience, la capacité et les aptitudes de l'équipe d'évaluation des risques;
- les contraintes liées au temps et aux autres ressources de l'organisation;
- le budget disponible si des ressources externes sont requises.

6.4 Nature et degré d'incertitude

La nature et le degré d'incertitude exigent une bonne connaissance de la qualité, de la quantité et de l'intégrité des informations disponibles relatives au risque considéré. Il s'agit de savoir dans quelle mesure les informations suffisantes relatives au risque, à leurs sources et à leurs causes, ainsi que leurs conséquences sur l'atteinte des objectifs sont disponibles. L'incertitude peut provenir de la qualité médiocre des données ou de l'absence de données essentielles et fiables. A titre d'illustration, les méthodes utilisées pour rassembler des données peuvent changer, de même que la manière dont les organisations utilisent ces méthodes, ou l'organisation peut ne pas avoir de méthode particulière pour rassembler des données relatives au risque identifié.

L'incertitude peut également être inhérente au contexte externe et interne de l'organisation. Les données disponibles ne constituent pas toujours une base fiable de prédiction de l'avenir. Pour les types uniques de risques, les données historiques peuvent ne pas être disponibles, ou celles qui le sont peuvent faire l'objet de différentes interprétations par différents acteurs. Cette évaluation des risques entreprise doit cerner le type et la nature de l'incertitude et apprécier les implications quant à la fiabilité des résultats de l'évaluation. Il convient de toujours communiquer ces éléments aux décideurs.

6.5 Complexité

Les risques peuvent être complexes par nature, par exemple, dans les systèmes complexes dont les risques doivent être évalués dans le cadre du système plutôt qu'en traitant chaque composant séparément et en ignorant les synergies. Dans d'autres cas, le traitement d'un seul risque peut avoir des implications ailleurs et avoir un impact sur d'autres activités. Les impacts importants et dépendances du risque doivent être compris pour s'assurer que de la gestion d'un seul risque ne découle pas une situation intolérable ailleurs. Il est essentiel de comprendre la complexité d'un seul risque ou d'un ensemble de risques d'une organisation pour choisir la méthode ou la technique adaptée à l'évaluation des risques.

6.6 Application de l'évaluation des risques au cours du cycle de vie

Il est possible de considérer que le cycle de vie de la plupart des activités, projets et produits commence au concept et à la définition initiaux et se poursuit jusqu'à l'achèvement, qui peut inclure le déclassement et la mise au rebut du matériel.

Les risques peuvent être évalués à toutes les étapes du cycle de vie. D'une manière générale, ils le sont plusieurs fois à différents niveaux de détail, de manière à faciliter la prise de décision à chaque phase.

Les phases du cycle de vie répondent à différentes exigences et nécessitent d'appliquer différentes techniques. Par exemple, lors de la phase de conception et de définition, si une opportunité est identifiée, les risques peuvent être évalués pour décider de la poursuite ou de l'interruption.

Si plusieurs options sont disponibles, les risques peuvent être évalués pour mesurer d'autres concepts et déterminer plus facilement lequel offre le meilleur rapport entre les risques positifs et négatifs.

Lors de la phase de conception et de développement, l'évaluation des risques permet

- d'assurer que les risques liés au système sont tolérables,
- de participer au processus d'amélioration de la conception,
- de participer aux études de rentabilité,
- d'identifier les risques ayant un impact sur les phases suivantes du cycle de vie.

Au fur et à mesure du déroulement de l'activité, il est possible d'évaluer les risques pour apporter des informations facilitant les procédures de développement pour les conditions normales et d'urgence.

6.7 Types de techniques d'évaluation des risques

Les techniques d'évaluation des risques peuvent être classées de différentes manières afin de faciliter la compréhension de leurs forces et faiblesses relatives. A titre d'illustration, les différents tableaux de l'Annexe A mettent en corrélation les techniques potentielles et ces catégories.

Chaque technique est approfondie dans l'Annexe B quant à la nature de l'évaluation qu'elle propose et les lignes directrices en matière d'applicabilité dans certaines situations.

Annexe A
(informative)

Comparaison des techniques d'évaluation des risques

A.1 Types de techniques

Le premier classement montre dans quelle mesure la technique s'applique à chaque étape du processus d'évaluation des risques, comme suit:

- identification du risque;
- analyse du risque – analyse des conséquences;
- analyse du risque – estimation de probabilité qualitative, semi-quantitative ou quantitative:
- analyse du risque – évaluation de l'efficacité des contrôles existants;
- analyse du risque – estimation du niveau de risque;
- évaluation des risques.

Pour chaque étape du processus d'évaluation des risques, l'application de la méthode est présentée comme étant parfaitement applicable, applicable ou inapplicable (voir Tableau A.1).

A.2 Facteurs influençant le choix des techniques d'évaluation des risques

Ensuite, les attributs des méthodes sont décrits en termes de

- complexité du problème et méthodes nécessaires à son analyse,
- nature et degré d'incertitude de l'évaluation des risques reposant sur la quantité d'informations disponibles et sur les éléments nécessaires à la satisfaction des objectifs,
- étendue des ressources nécessaires en termes de durée et de niveau des expertises, de données nécessaires ou de coût,
- possibilité pour la méthode de fournir des résultats quantitatifs.

Des exemples de types de méthodes d'évaluation des risques disponibles sont répertoriés dans le Tableau A.2, dans lequel chaque méthode est classée selon que ses attributs sont élevés, moyens ou faibles.

Tableau A.1 – Applicabilité des outils utilisés pour l'évaluation des risques

Outils et techniques	Processus d'évaluation des risques					Voir Annexe
	Identification des risques	Analyse des risques			Evaluation des risques	
		Conséquence	Probabilité	Niveau de risque		
« Brainstorming »	SA[1)]	NA[2)]	NA	NA	NA	B 01
Entretiens structurés ou semi-structurés	SA	NA	NA	NA	NA	B 02
Techniques Delphi	SA	NA	NA	NA	NA	B 03
Listes de contrôle	SA	NA	NA	NA	NA	B 04
Analyse préliminaire du danger	SA	NA	NA	NA	NA	B 05
Etudes de danger et d'exploitabilité (HAZOP)	SA	SA	A[3)]	A	A	B 06
HACCP[3]	SA	SA	NA	NA	SA	B 07
Evaluation des risques environnementaux	SA	SA	SA	SA	SA	B 08
SWIFT[4]	SA	SA	SA	SA	SA	B 09
Analyse de scénario	SA	SA	A	A	A	B 10
Analyse d'impact sur l'activité	A	SA	A	A	A	B 11
Analyse de causes profondes	NA	SA	SA	SA	SA	B 12
Analyse des modes de défaillance et de leurs effets	SA	SA	SA	SA	SA	B 13
Analyse par arbre de panne	A	NA	SA	A	A	B 14
Analyse par arbre d'événements	A	SA	A	A	NA	B 15
Analyse causes-conséquences	A	SA	SA	A	A	B 16
Analyse des causes et de leurs effets	SA	SA	NA	NA	NA	B 17
Analyse des niveaux de protection (LOPA)[5]	A	SA	A	A	NA	B 18
Arbre de décision	NA	SA	SA	A	A	B 19
Analyse de fiabilité humaine	SA	SA	SA	SA	A	B 20
Analyse «nœud papillon»	NA	A	SA	SA	A	B 21
Maintenance basée sur la fiabilité	SA	SA	SA	SA	SA	B 22
Analyse des conditions insidieuses (Analyse transitoire)	A	NA	NA	NA	NA	B 23
Analyse de Markov	A	SA	NA	NA	NA	B 24
Simulation de Monte-Carlo	NA	NA	NA	NA	SA	B 25
Analyse bayésienne et réseaux de Bayes	NA	SA	NA	NA	SA	B 26
Courbes FN	A	SA	SA	A	SA	B 27
Indices de risque	A	SA	SA	A	SA	B 28
Matrice conséquence/probabilité	SA	SA	SA	SA	A	B 29
Analyse coût/bénéfice	A	SA	A	A	A	B 30
Analyse de décision à critères multiples (ADCM)	A	SA	A	SA	A	B 31

3 HACCP = *Hazard Analysis and Critical Control Points*

4 SWIFT = *Structured "What-if" Techniques*

5 LOPA = *Layer of Protection Analysis*

Outils et techniques	Processus d'évaluation des risques					Voir Annexe
	Identification des risques	Analyse des risques			Evaluation des risques	
		Conséquence	Probabilité	Niveau de risque		
[1] Parfaitement applicable. [2] Inapplicable. [3] Applicable.						

Tableau A.2 – Attributs d'un choix d'outils d'évaluation des risques

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
MÉTHODES DE RECHERCHE					
Listes de contrôle	Formulaire simple d'identification des risques. Technique proposant un répertoire d'incertitudes usuelles qu'il convient de prendre en compte. Les utilisateurs se rapportent à une liste, à des codes et à des normes préalablement établis	Faible	Faible	Faible	Non
Analyse préliminaire du danger	Une méthode d'analyse inductive simple consistant à identifier les dangers, ainsi que les situations et événements dangereux, pouvant nuire à une activité, une installation ou un système donné	Faible	Élevé	Moyen	Non
MÉTHODES DE SOUTIEN					
Entretien structuré et «brainstorming»	Moyen de rassembler un grand nombre d'idées et d'évaluations en les classant dans un groupe. Le «brainstorming» peut être stimulé par des invites ou par des techniques d'entretien en tête à tête ou seul contre tous	Faible	Faible	Faible	Non
Technique Delphi	Moyen permettant de combiner les avis d'un expert susceptibles de soutenir la source et d'avoir un impact sur l'identification, la probabilité et les conséquences et l'évaluation des risques. Il s'agit d'une technique collaborative permettant de prévoir un consensus. Implique l'analyse et le vote indépendants d'experts	Moyen	Moyen	Moyen	Non
Méthode ("que se passerait-il si ?")	Système incitant une équipe à identifier les risques. Il est en principe utilisé dans un atelier formel. En principe lié à une analyse des risques et une technique d'évaluation	Moyen	Moyen	Toutes	Non
Analyse de fiabilité humaine (AFH)	L'analyse de fiabilité humaine (AFH) porte sur l'impact des personnes sur les performances du système. Elle peut être utilisée pour évaluer les influences de l'erreur humaine sur le système	Moyen	Moyen	Moyen	Oui

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ANALYSE DU SCÉNARIO					
Analyse de causes profondes (analyse la perte unique)	Une seule perte a été analysée afin de comprendre les causes concourantes et la manière dont le système ou le processus peut être amélioré pour éviter des pertes de ce type à l'avenir. L'analyse doit tenir compte des contrôles en place au moment de la perte et de la manière dont ils peuvent être améliorés	Moyen	Faible	Moyen	Non
Analyse du scénario	Les futurs scénarii possibles sont imaginés ou extrapolés à partir des risques actuels et différents considérés, en supposant que ces scénarii soient susceptibles de se produire. Il peut s'agir de scénarii formels ou informels, qualitatifs ou quantitatifs	Moyen	Élevé	Moyen	Non
Évaluation des risques toxicologiques	Les dangers sont identifiés et analysés, et les possibles vecteurs d'exposition au danger d'une cible spécifiée sont identifiés. Les informations relatives au niveau d'exposition et à la nature de la nuisance provoquée par un niveau d'exposition donné sont combinées pour donner une mesure de la probabilité d'occurrence de la nuisance spécifiée	Élevé	Élevé	Moyen	Oui
Analyse d'impact sur l'activité	Propose d'analyser la manière dont les principaux risques de perturbation pourraient avoir un impact sur les opérations d'une organisation et d'identifier et de quantifier les aptitudes nécessaires à leur gestion	Moyen	Moyen	Moyen	Non
Analyse par arbre de panne	Technique commençant par l'événement indésirable (événement de tête) et déterminant toutes les manières dont il pourrait se produire. Ces éléments sont présentés graphiquement sous la forme d'une arborescence logique. Une fois l'arbre de panne développé, il convient de considérer les manières de réduire ou d'éliminer les causes/sources potentielles	Élevé	Élevé	Moyen	Oui
Analyse par arbre d'événements	Utilisation du raisonnement inductif pour traduire la probabilité d'événements initiateurs différents en résultats possibles	Moyen	Moyen	Moyen	Oui
Analyse causes/ conséquences	Combinaison de l'analyse par arbre de panne et par arbre d'événements permettant d'inclure des actions différées. Les causes et les conséquences d'un événement initiateur sont considérées	Élevé	Moyen	Élevé	Oui
Analyse de cause à effet	Un effet peut avoir un certain nombre de facteurs contributifs pouvant être regroupés en différentes catégories. Les facteurs contributifs sont souvent identifiés par «brainstorming» et présentés sous forme d'arborescence ou de diagramme d'Ishikawa	Faible	Faible	Moyen	Non

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ANALYSE FONCTIONNELLE					
AMDE et AMDEC	L'AMDE (Analyse des modes de défaillance et de leurs effets) est une technique qui permet d'identifier les modes et les mécanismes de défaillance, et leurs effets. Il existe plusieurs types de méthode AMDE: L'AMDE Conception (ou produit), qui est utilisée pour les composants ou les produits, l'AMDE Système utilisée pour les systèmes, l'AMDE Processus utilisée pour les processus de fabrication et d'assemblage, l'AMDE Service et l'AMDE Logiciel. L'AMDE peut être suivie d'une analyse de criticité qui définit l'importance de chaque mode de défaillance de manière qualitative, semi-qualitative ou quantitative (AMDEC). L'analyse de criticité peut se fonder sur la probabilité qu'un mode de défaillance donnera lieu à la défaillance du système, ou sur le niveau de risque associé au mode de défaillance, ou sur un degré de priorité du risque	Moyen	Moyen	Moyen	Oui
Maintenance basée sur la fiabilité	Une méthode permettant d'identifier les règles qu'il convient de mettre en place pour gérer les défaillances et atteindre de manière efficace et efficiente le niveau de sécurité, de disponibilité et d'économie requis du fonctionnement pour tous les types d'équipement	Moyen	Moyen	Moyen	Oui
Analyse transitoire (Analyse de conditions insidieuses)	Une méthodologie permettant d'identifier les erreurs de conception. Une condition insidieuse est une condition matérielle, logicielle ou intégrée latente pouvant être à l'origine d'un événement indésirable ou pouvant gêner l'occurrence d'un événement souhaité, cette condition n'étant pas provoquée par la défaillance d'un composant. Ces conditions se caractérisent par leur nature aléatoire et leur aptitude à échapper à toute forme de détection lors d'essais normalisés les plus rigoureux du système. Les conditions insidieuses peuvent être à l'origine de fonctionnements inappropriés, de la perte de disponibilité du système, de retards de programmation, voire de mort ou de blessure	Moyen	Moyen	Moyen	Non
Méthode HAZOP (Etudes de danger et d'exploitabilité)	Un processus général d'identification des risques permettant de définir les écarts possibles par rapport aux performances prévues ou attendues. Elle utilise un système reposant sur des mots-guides La criticité des écarts est évaluée	Moyen	Élevé	Élevé	Non
Méthode HACCP (Analyse des dangers critiques pour leur maîtrise)	Une méthode systématique, proactive et préventive visant à assurer la qualité des produits ainsi que la fiabilité et la sécurité des processus par la mesure et le contrôle de caractéristiques particulières devant se trouver dans des limites définies	Moyen	Moyen	Moyen	Non

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ÉVALUATION DES CONTRÔLES					
Méthode LOPA (Analyse des niveaux de protection)	(Également appelée analyse de barrière). Elle permet d'évaluer les contrôles et leur efficacité	Moyen	Moyen	Moyen	Oui
Analyse «nœud papillon»	Un moyen schématique simple permettant de décrire et d'analyser les chemins d'un risque en partant des dangers jusqu'aux conséquences et en examinant les moyens de contrôle. Elle peut être considérée comme la combinaison d'un arbre de panne permettant d'analyser la cause d'un événement et d'un arbre d'événements permettant d'analyser les conséquences. Elle est représentée graphiquement sous la forme d'un "noeud papillon"	Moyen	Élevé	Moyen	Oui
MÉTHODES STATISTIQUES					
Analyse de Markov	L'analyse de Markov, parfois appelée analyse de l'*espace des états*, est habituellement utilisée dans l'analyse des systèmes complexes réparables qui peuvent exister en plusieurs états, notamment divers états dégradés	Elevé	Faible	Elevé	Oui
Analyse de Monte-Carlo	La simulation de Monte-Carlo permet d'établir la variation d'agrégat résultant des variations, dans un système, d'un certain nombre d'entrées, dont chacune d'elles est répartie de manière définie et est liée au résultat par des relations définies. L'analyse peut être utilisée pour un modèle spécifique, dans lequel les interactions des différentes entrées peuvent être définies mathématiquement. Les entrées peuvent reposer sur une variété de types de distribution, selon la nature de l'incertitude qu'elles sont censées représenter. Dans le cas de l'évaluation des risques, les distributions triangulaires ou distributions bêta sont souvent utilisées	Elevé	Faible	Elevé	Oui
Analyse bayésienne	Un mode opératoire statistique qui utilise les données d'une distribution préalable pour évaluer la probabilité du résultat. L'analyse bayésienne dépend de l'exactitude de la distribution préalable pour déduire un résultat exact. Le modèle de réseaux de croyance bayésienne a un impact dans une variété de domaines en capturant les relations de probabilité des entrées variables pour déduire un résultat	Elevé	Faible	Elevé	Oui

Annexe B
(informative)

Techniques d'évaluation des risques

B.1 «Brainstorming»

B.1.1 Présentation

Le «brainstorming» implique de stimuler et d'encourager la libre conversation au sein d'un groupe de personnes compétentes afin d'identifier les modes de défaillance potentiels et les dangers, risques, critères de décision et/ou options de traitement associés. Le terme «brainstorming» est souvent utilisé très librement pour signifier tout type de discussion en groupe. Toutefois, le véritable «brainstorming» implique des techniques particulières dont l'objet est de stimuler l'imagination des personnes à l'aide des idées et déclarations des autres membres du groupe.

Une facilitation efficace est très importante dans cette technique. Elle comprend: la stimulation de la discussion au démarrage, l'encouragement périodique du groupe à évoquer d'autres domaines pertinents et la saisie des questions émanant de la discussion (qui est en général assez vivante).

B.1.2 Utilisation

Le «brainstorming» peut être utilisé avec d'autres méthodes d'évaluation des risques décrites ci-dessous. Il peut également être utilisé seul, comme une technique stimulant l'imagination à toutes les étapes du processus de gestion des risques et du cycle de vie d'un système. Il peut être utilisé dans le cadre de discussions de haut niveau dans lesquelles les problèmes sont identifiés, d'un examen plus détaillé ou d'un niveau approfondi lié à des problèmes particuliers.

Le «brainstorming» accorde une place prépondérante à l'imagination. Par conséquent, il est particulièrement utile lors de l'identification des risques liés à de nouvelles technologies, en l'absence de données ou lorsqu'il est nécessaire de trouver des solutions originales à des problèmes.

B.1.3 Entrées

Une équipe de personnes dont la connaissance de l'organisation, du système, du processus ou de l'application sont en cours d'évaluation.

B.1.4 Processus

Le «brainstorming» peut être formel ou informel. Le «brainstorming» formel est plus structuré avec des participants préparés à l'avance, l'objectif et le résultat de la session étant définis, et des moyens étant prévus pour évaluer les idées avancées. Le «brainstorming» informel est moins structuré et souvent plus approprié.

Dans un processus formel:

- avant la session, le facilitateur prépare les éléments de réflexion correspondant au contexte;
- les objectifs de la session sont définis et les règles expliquées;
- le facilitateur avance une série d'éléments de réflexion. Chacun explore des idées en identifiant autant de problèmes que possible. A cette étape, aucune discussion n'est engagée, car il ne s'agit pas de savoir s'il convient que tel ou tel élément fasse partie

d'une liste ou ce que signifie une déclaration particulière, ce type de situation ayant tendance à bloquer la fluidité de la réflexion. Toutes les entrées sont acceptées, aucune ne faisant l'objet de critiques. Le groupe avance rapidement pour développer des pensées latérales;

- le facilitateur peut engager les personnes sur de nouvelles pistes lorsque la réflexion a été poussée suffisamment loin ou qu'elle s'écarte trop du sujet. Toutefois, il s'agit de rassembler autant d'idées diverses que possible en vue d'une analyse ultérieure.

B.1.5 Résultats

Les résultats dépendent de l'étape du processus de gestion des risques dont il s'agit. Par exemple, à l'étape de l'identification, les résultats peuvent être une liste de risques et de contrôles actuels.

B.1.6 Avantages et limites

Les avantages du «brainstorming» sont les suivants:

- il stimule l'imagination et permet donc d'identifier de nouveaux risques et des solutions originales;
- il implique des acteurs clés et facilite donc la communication globale;
- il est relativement rapide et facile à mettre en place.

Les limites sont les suivantes:

- les participants peuvent manquer de compétences ou de connaissances pour être des contributeurs efficaces;
- étant donné qu'il est relativement peu structuré, il est difficile de démontrer que le processus est exhaustif (que tous les risques potentiels ont été identifiés, par exemple);
- il peut exister une dynamique de groupe variable, les personnes ayant des idées valables ne s'exprimant pas ou d'autres dominant la discussion. Cette situation peut être résolue par le «brainstorming» informatique, par l'intermédiaire d'un forum de discussion ou d'une technique de groupe nominal. Le «brainstorming» informatique peut être mis en place de manière anonyme, ce qui permet d'éviter les questions personnelles et politiques susceptibles de gêner le libre débat d'idées. Pour la technique de groupe nominal, les idées sont soumises de manière anonyme à un animateur et elles sont ensuite traitées par le groupe.

B.2 Entretiens structurés ou semi-structurés

B.2.1 Présentation

Dans un entretien structuré, un ensemble de questions préparées est posé aux personnes interrogées à partir d'une feuille de suggestions, les encourageant à aborder une situation selon différents points de vue et à identifier les risques selon ces perspectives. Un entretien semi-structuré est similaire, mais offre plus de liberté à la conversation pour explorer les questions soulevées.

B.2.2 Utilisation

Les entretiens structurés et semi-structurés sont utiles lorsqu'il est difficile de réunir les personnes pour une session de «brainstorming» ou qu'une libre discussion au sein d'un groupe n'est pas appropriée à la situation ou aux personnes concernées. Souvent, ils permettent d'identifier les risques ou d'évaluer l'efficacité des contrôles existants dans le cadre d'une analyse des risques. Ils peuvent être utilisés à toutes les étapes d'un projet ou d'un processus. Ils sont un moyen d'offrir aux acteurs une entrée pour l'évaluation des risques.

B.2.3 Entrées

Les entrées comprennent:

- une définition claire des objectifs des entretiens;
- une liste des personnes interrogées sélectionnées parmi les acteurs pertinents;
- un ensemble préparé de questions.

B.2.4 Processus

Un ensemble de questions pertinentes est créé pour orienter l'interrogateur. Dans la mesure du possible, il convient que les questions soient évolutives, simples, exprimées dans la langue de la personne interrogée et qu'elles ne couvrent qu'une seule question. Des questions complémentaires possibles pour obtenir des éclaircissements sont également préparées.

Les questions sont ensuite posées à la personne interrogée. Lors de la recherche d'élaboration, il convient que les questions soient évolutives. Il convient de veiller à ne pas influencer la personne interrogée.

Il convient de considérer les réponses selon un certain degré de souplesse afin d'offrir la possibilité à la personne interrogée d'explorer des domaines dans lesquels elle souhaite s'engager.

B.2.5 Résultats

Le résultat est l'opinion de la personne interrogée sur les questions faisant l'objet de l'entretien.

B.2.6 Avantages et limites

Les avantages des entretiens structurés sont les suivants:

- ils permettent aux personnes de prendre le temps de réfléchir sur une question;
- la communication en tête à tête peut permettre de considérer des questions de manière plus approfondie;
- les entretiens structurés permettent d'impliquer un plus grand nombre d'acteurs que le «brainstorming», qui utilise un groupe relativement réduit.

Les limites sont les suivantes:

- le facilitateur doit consacrer du temps pour rassembler plusieurs avis de cette manière;
- le parti pris est toléré et n'est pas éliminé de la discussion de groupe;
- il peut s’avérer impossible de stimuler l'imagination des personnes présentes, qui est un avantage significatif du «brainstorming».

B.3 Technique Delphi

B.3.1 Présentation

La technique Delphi est un mode opératoire permettant d'obtenir un consensus fiable sur les avis d'un groupe d'experts. Bien que le terme soit désormais largement utilisé pour signifier une forme de «brainstorming», l'une des fonctions essentielles de la technique Delphi, telle qu'elle a été formulée à l'origine, consistait à permettre à des experts d'exprimer leurs avis de manière individuelle et anonyme, tout en ayant accès aux avis de leurs homologues au fur et à mesure de l'avancée du processus.

B.3.2 Utilisation

La technique Delphi peut s'appliquer à toutes les étapes du processus de gestion des risques ou du cycle de vie d'un système, à chaque fois qu'un consensus d'avis d'experts est nécessaire.

B.3.3 Entrées

Un ensemble d'options pour lesquelles un consensus est requis.

B.3.4 Processus

Des questions sont posées à un groupe d'experts à l'aide d'un questionnaire semi-structuré. Les experts ne se connaissent pas. Leurs avis sont donc indépendants.

La procédure est la suivante:

- formation d'une équipe pour engager et surveiller le processus Delphi;
- sélection d'un groupe d'experts (il peut s'agir d'un ou de plusieurs groupes spécifiques d'experts);
- développement du questionnaire 1;
- essai du questionnaire;
- envoi du questionnaire à chaque membre du groupe;
- les informations provenant du premier jeu de réponses sont analysées et combinées, puis retransmises aux membres du groupe;
- les membres du groupe répondent, puis le processus est de nouveau enclenché tant que le consensus n'a pas été obtenu.

B.3.5 Résultats

Convergence vers un consensus sur les questions en cours.

B.3.6 Avantages et limites

Les avantages sont les suivants:

- compte tenu de leur caractère anonyme, les avis impopulaires sont plus susceptibles d'être exprimés;
- tous les points de vue sont pondérés de manière égale (il s'agit d'éviter tous les problèmes liés aux personnalités dominatrices);
- permet d'obtenir la propriété des résultats;
- il n'est pas utile que les personnes soient rassemblées en même temps au même endroit.

Les limites sont les suivantes:

- cela demande beaucoup de travail et de temps;
- les participants doivent être capables de s'exprimer correctement par écrit.

B.4 Listes de contrôle

B.4.1 Présentation

Les listes de contrôle répertorient les dangers, risques ou défaillances de contrôle qui ont été développés, en général par expérience, à la suite d'une précédente évaluation des risques ou des défaillances déjà survenues.

B.4.2 Utilisation

Une liste de contrôle peut être utilisée pour identifier les dangers et les risques ou pour évaluer l'efficacité des contrôles. Elle peut être utilisée à toutes les étapes du cycle de vie d'un produit, d'un processus ou d'un système. Elle peut également l'être dans le cadre d'autres techniques d'évaluation des risques. Toutefois, elle est le plus souvent utile lorsqu'elle permet de vérifier que tous les sujets ont été abordés à la suite de l'application d'une technique plus imaginative visant à identifier de nouveaux problèmes.

B.4.3 Entrées

Informations et expertise préalables sur la question, de manière à pouvoir sélectionner ou développer une liste de contrôle pertinente et de préférence validée.

B.4.4 Processus

La procédure est la suivante:

- le domaine d'application de l'activité est défini;
- une liste de contrôle est sélectionnée, couvrant tout le domaine d'application de manière appropriée. Les listes de contrôle doivent être sélectionnées avec soin pour l'objet. Par exemple, une liste de contrôles normalisés ne peut pas être utilisée pour identifier de nouveaux dangers ou risques;
- la personne ou l'équipe qui utilise la liste de contrôle passe en revue chaque élément du processus ou du système et regarde si les éléments de la liste sont présents.

B.4.5 Résultats

Les résultats dépendent de l'étape du processus de gestion des risques auquel ils sont appliqués. Par exemple, le résultat peut être une liste de contrôles insuffisants ou une liste de risques.

B.4.6 Avantages et limites

Les listes de contrôle présentent les avantages suivants:

- elles peuvent être utilisées par des profanes;
- si elles sont bien conçues, elles associent une expertise approfondie à un système d'utilisation facile;
- elles peuvent permettre de ne pas oublier les problèmes habituels.

Les limites sont les suivantes:

- elles ont tendance à entraver l'imagination en matière d'identification des risques;
- elles concernent les «connus connus», et pas les «inconnus connus» ou les « inconnus inconnus»;
- elles encouragent les comportements consistant à simplement cocher les cases;
- elles ont tendance à simplement reposer sur l'observation et donc à ignorer les problèmes qui n'ont pas été décelés.

B.5 Analyse préliminaire du danger (APD)

B.5.1 Présentation

L'analyse préliminaire du danger est une méthode d'analyse inductive simple consistant à identifier les dangers, ainsi que les situations et événements dangereux pouvant nuire à une activité, une installation ou un système donné.

B.5.2 Utilisation

En général, cette analyse est effectuée dès le développement d'un projet lorsque peu d'informations relatives aux détails de conception ou aux procédures de fonctionnement sont disponibles, et elle peut souvent être un précurseur à d'autres études ou fournir des informations de spécification sur la conception d'un système. Elle peut également être utile pour analyser des systèmes existants pour classer les dangers et les risques par priorité pour une analyse plus approfondie ou lorsque les circonstances ne permettent pas l'utilisation d'une technique plus poussée.

B.5.3 Entrées

Les entrées sont les suivantes:

- les informations sur le système à évaluer;
- les détails de la conception du système, en fonction de leurs disponibilité et pertinence.

B.5.4 Processus

Une liste de dangers et de situations dangereuses et risques génériques est formulée en tenant compte de caractéristiques telles que:

- les matériaux utilisés ou produits et leur réactivité;
- les appareils employés;
- l'environnement de fonctionnement;
- l'implantation;
- les interfaces entre composants du système, etc.

Il est possible de procéder à une analyse qualitative des conséquences d'un événement indésirable et de sa probabilité pour identifier les risques pour une évaluation supplémentaire.

Il convient de mettre à jour l'analyse APD au cours des phases de conception, de construction et d'essai afin de déceler tout nouveau danger, et si nécessaire, d'effectuer les corrections requises. Il est admis de présenter les résultats sous diverses formes, telles que tableaux et arbres.

B.5.5 Résultats

Les résultats sont les suivants:

- une liste de dangers et de risques;
- des recommandations sous la forme d'acceptation, de contrôles recommandés, de spécification de conception ou de requêtes pour une évaluation plus détaillée.

B.5.6 Avantages et limites

Les avantages sont les suivants:

- peut être utilisée lorsque les informations sont limitées;
- permet d'anticiper les risques très tôt dans le cycle de vie du système.

Les limites sont les suivantes:

- une analyse APD n'offre que des informations préliminaires. Elle n'est pas exhaustive ni ne donne des informations détaillées relatives aux risques et à la manière dont il est possible de les éviter au mieux.

B.6 Méthode HAZOP

B.6.1 Présentation

HAZOP est l'acronyme de **HA**zard and **OP**erability study (Etude de danger et d'exploitabilité). Il s'agit de l'examen structuré et systématique d'un produit, d'un processus, d'un mode opératoire ou d'un système planifié ou existant. Cette technique permet d'identifier les risques auxquels sont confrontés les personnes, les équipements, l'environnement et/ou les objectifs de l'organisation. L'équipe chargée de l'étude a également pour prérogative, dans la mesure du possible, d'apporter des solutions visant à éliminer le risque en question.

Le processus HAZOP est une technique qualitative reposant sur l'utilisation de mots-guides permettant de déterminer dans quelle mesure il n'est pas possible d'obtenir la conception ou les conditions de fonctionnement désirées à chaque étape de la conception, du processus, du mode opératoire ou du système. D'une manière générale, elle est mise en place par une équipe pluridisciplinaire à la suite de plusieurs réunions.

L'analyse HAZOP ressemble à l'analyse AMDE puisqu'elle identifie les modes de défaillance d'un processus, d'un système ou d'un mode opératoire, ainsi que leurs causes et leurs conséquences. La différence est que l'équipe tient compte des résultats et écarts indésirables par rapport aux résultats et conditions prévus, et revient aux causes et modes de défaillance possibles, tandis que l'analyse AMDE commence par identifier les modes de défaillance.

B.6.2 Utilisation

A l'origine, la technique HAZOP a été développée pour analyser les systèmes de production chimique mais elle a été étendue à d'autres types de systèmes et d'opérations complexes. Ceux-ci incluent, notamment, les systèmes mécaniques et électroniques, les modes opératoires, les systèmes logiciels. Elle a même été appliquée aux changements organisationnels et à la conception et l'examen de contrats juridiques.

Le processus HAZOP peut concerner toutes les formes d'écart par rapport à la conception prévue, à la suite de défaillances de conception, de composants, de modes opératoires et actions humaines planifiées.

Il est largement utilisé dans le cadre d'examens de conception logicielle. Lorsqu'il est appliqué au contrôle des appareils essentiels de sécurité et aux systèmes informatiques, il peut être connu sous le nom de CHAZOP (**C**ontrol **HAZ**ards and **OP**erability analysis – Analyse de danger et d'exploitabilité de commandes, ou **C**omputer **HAZ**ard and **OP**erability analysis – Analyse de danger et d'exploitabilité informatique).

D'une manière générale, une étude HAZOP est réalisée à l'étape de la conception détaillée, lorsqu'un diagramme exhaustif du processus prévu est disponible, mais que des modifications peuvent encore être apportées à la conception. Elle peut cependant être réalisée dans le cadre d'une approche progressive en appliquant différents mots-guides à chaque étape au fur et à mesure du développement de la conception. Une étude HAZOP peut également être réalisée lors du fonctionnement, mais les modifications nécessaires peuvent à cette étape s'avérer onéreuses.

B.6.3 Entrées

Les entrées essentielles d'une étude HAZOP sont des informations actuelles relatives au système, au processus ou au mode opératoire à examiner, ainsi qu'aux spécifications de conception et de performances prévues. Les entrées peuvent inclure: des dessins, des fiches techniques, des organigrammes, des diagrammes logiques et de contrôle de processus, des dessins de disposition, des modes opératoires de fonctionnement et de maintenance et des modes opératoires d'intervention d'urgence. Pour les éléments non matériels liés à l'analyse HAZOP, il peut s'agir de tout document décrivant les fonctions et éléments du système ou du mode opératoire en cours d'étude. Par exemple, les entrées peuvent être des

diagrammes organisationnels et des descriptions de poste, un projet de contrat, voire de mode opératoire.

B.6.4 Processus

L'analyse HAZOP traite de la conception et de la spécification du processus, du mode opératoire ou du système en cours d'étude et en examine chacune des parties afin de détecter les écarts susceptibles de se produire par rapport aux performances prévues, et ainsi déterminer les causes potentielles et les conséquences éventuelles. Pour ce faire, il s'agit d'examiner de manière systématique le comportement de chaque partie du système, du processus ou du mode opératoire lorsque des modifications sont apportées aux paramètres essentiels à l'aide de mots-guides pertinents. Il est possible de personnaliser les mots-guides en fonction d'un système, processus ou mode opératoire particulier, ou d'utiliser des mots génériques englobant tous les types d'écart. Le Tableau B.1 donne des exemples de mots-guides couramment utilisés pour des systèmes techniques. Des mots-guides similaires tels que « trop tôt », « trop tard », « trop - beaucoup», « trop peu – pas assez », « trop long », « trop court », « mauvaise direction », sur « mauvais objet », « mauvaise action » peuvent être utilisés pour identifier les modes d'erreur humaine.

La procédure normale d'une étude HAZOP est la suivante:

- nomination d'une personne responsable et disposant de toute la latitude nécessaire à la conduite de l'étude HAZOP, et en mesure d'appliquer toutes les actions qui en résultent;
- définition des objectifs et du domaine d'application de l'étude;
- établissement d'un ensemble de mots-clés ou de mots-guides correspondant à l'étude;
- constitution de l'équipe HAZOP. En principe, il s'agit d'une équipe pluridisciplinaire. Il convient qu'elle soit composée de personnel de conception et d'exploitation aux compétences techniques appropriées, afin d'évaluer les effets des écarts constatés par rapport à la conception prévue ou actuelle. Il est recommandé d'intégrer dans l'équipe des personnes n'étant pas directement impliquées dans la conception ou dans le système, le processus ou le mode opératoire en cours d'examen;
- collecte de la documentation requise.

Dans un atelier avec l'équipe d'étude:

- découpage du système, du processus ou du mode opératoire en éléments plus petits, en sous-systèmes, sous-processus ou sous-éléments afin d'assurer la tangibilité de l'examen;
- acceptation de la conception prévue pour chaque sous-système, sous-processus ou sous-élément, puis pour chacun de leurs éléments, en appliquant successivement les mots-guides, de manière à anticiper les écarts possibles qui produiront des résultats indésirables;
- en cas d'identification d'un résultat indésirable, acceptation de la cause et des conséquences dans chaque cas, puis suggestion de la manière dont ils peuvent être traités afin d'éviter qu'ils ne se reproduisent ou de limiter les conséquences, le cas échéant;
- documentation de la discussion et acceptation des actions spécifiques pour traiter les risques identifiés.

Tableau B.1 – Exemple de mots-guides HAZOP possibles

Termes	Définitions
Aucun ou non	Le résultat prévu ne s'est pas produit ni même partiellement, ou absence de la condition prévue
Plus (supérieur)	Accroissement quantitatif du résultat ou de la condition de fonctionnement
Moins (inférieur)	Diminution quantitative
Autant que	Accroissement quantitatif (matériau supplémentaire, par exemple)
En partie	Diminution quantitative (un ou deux composants uniquement dans un mélange donné, par exemple)
Inverse/opposé	Opposé (refoulement, par exemple)
Autre que	Rien de ce qui est prévu n'est réalisé, l'événement qui a lieu est totalement différent (écoulement du mauvais produit, par exemple)
Compatibilité	Matériaux; environnement
Les mots-guides sont appliqués à des paramètres tels que	
	Propriétés physiques d'un matériau ou d'un processus
	Conditions physiques (température ou vitesse, par exemple)
	Intention spécifiée d'un composant d'un système ou d'une conception (transfert d'informations, par exemple)
	Aspects fonctionnels

B.6.5 Résultats

Compte rendu des réunions HAZOP avec éléments enregistrés pour chaque point examiné. Il convient que cela comprenne: le mot-guide utilisé, le/les écart(s), les causes possibles, les actions à entreprendre pour résoudre les problèmes identifiés et la personne responsable de l'action.

Il convient que le risque lié à un écart qui ne peut pas être corrigé soit évalué.

B.6.6 Avantages et limites

Une analyse HAZOP présente les avantages suivants:

- offre le moyen d'examiner de manière systématique et rigoureuse un système, un processus ou un mode opératoire;
- implique la constitution d'une équipe pluridisciplinaire, composée de personnes aux compétences opérationnelles pragmatiques et en mesure de procéder à des opérations de traitement;
- génère des solutions et des moyens de traitement du risque;
- est applicable à un large éventail de systèmes, de processus et de modes opératoires;
- permet d'aborder de manière explicite les causes et conséquences d'une erreur humaine;
- permet d'enregistrer par écrit le processus qui peut être utilisé pour éviter les actes de négligence.

Les limites sont les suivantes:

- elle peut prendre beaucoup de temps et donc être onéreuse;
- elle nécessite un niveau élevé de documentation ou de spécification de système/processus et de mode opératoire;

- l'attention peut porter exclusivement sur la recherche de solutions plutôt que sur les raisons qui motivent une action (ceci peut être limité par une approche progressive);
- la discussion peut porter essentiellement sur des détails de conception et non sur des questions plus larges ou externes;
- elle est limitée par le projet de conception et la conception elle-même, ainsi que par le domaine d'application et les objectifs imposés à l'équipe;
- le processus s'appuie fortement sur l'expertise des concepteurs, ces derniers pouvant trouver difficile de rester suffisamment objectifs quant aux problèmes que peuvent présenter leurs conceptions.

B.6.7 Document de référence

CEI 61882, *Études de danger et d'exploitabilité (études HAZOP) – Guide d'application*

B.7 Méthode HACCP (Analyse des dangers – points critiques pour leur maîtrise)

B.7.1 Présentation

L'analyse HACCP offre une structure permettant d'identifier les dangers et de mettre des contrôles en place au niveau de toutes les parties importantes d'un processus, afin de se protéger contre les dangers et de maintenir la qualité, la fiabilité et la sécurité d'un produit. L'analyse HACCP prévoit de limiter les risques en procédant à des contrôles placés tout au long du processus, au lieu de procéder à une inspection du produit fini.

B.7.2 Utilisation

L'analyse HACCP a été développée pour garantir la qualité alimentaire dans le cadre des programmes spatiaux de la NASA. Elle est à présent utilisée par l'ensemble des organisations officiant dans toute la chaîne alimentaire pour contrôler les risques liés aux polluants physiques, chimiques ou biologiques dans la nourriture. Elle a également été développée pour la fabrication des produits pharmaceutiques et des appareils médicaux. Il est possible de généraliser à d'autres systèmes techniques, le principe d'identification des éléments pouvant avoir une influence sur la qualité des produits et de définition des étapes d'un processus dont les paramètres essentiels peuvent être surveillés et les dangers contrôlés.

B.7.3 Entrées

L'analyse HACCP débute par un organigramme de base ou un schéma de procédé et des informations relatives à des dangers susceptibles d'avoir un impact sur la qualité, la sécurité ou la fiabilité du produit ou sur le résultat du processus. Les informations relatives aux dangers, à leurs risques et aux moyens permettant de les contrôler représentent une entrée de l'analyse HACCP.

B.7.4 Processus

L'analyse HACCP repose sur les sept principes suivants:

- identification des dangers et mesures de prévention les concernant;
- détermination des étapes du processus dans lesquels les dangers peuvent être contrôlés ou éliminés (points de contrôle critiques ou PCC);
- définition des limites critiques nécessaires au contrôle des dangers. En d'autres termes, pour assurer le contrôle du danger, il convient que chaque PCC respecte un certain nombre de paramètres spécifiques;
- surveillance des limites critiques de chaque PCC à intervalles déterminés;
- mise en place d'actions correctives si le processus sort des limites établies;

- mise en place des procédures de vérification;
- tenue des archives et procédures de documentation correspondant à chacune des étapes.

B.7.5 Résultats

Enregistrements documentés comprenant une fiche de travail d'analyse de danger et un **plan** HACCP.

Les listes de fiches d'analyse de danger répertorient les éléments ci-dessous pour chaque étape du processus:

- les dangers susceptibles de se produire, d'être tenus sous contrôle ou aggravés à cette étape;
- si les dangers représentent un risque important (en tenant compte des conséquences et de la probabilité d'occurrence, déterminés en s'appuyant sur l'expérience, les données et une documentation technique);
- les raisons d'une telle importance;
- les possibles mesures de prévention pour chaque danger;
- si les mesures de surveillance ou de contrôle peuvent être appliquées à cette étape (en d'autres termes, s'il s'agit d'un PCC).

Le plan HACCP détermine la procédure à suivre pour contrôler une conception, un produit, un processus ou un mode opératoire spécifique. Le plan comprend une liste de tous les PCC, et pour chacun d'eux:

- les limites critiques correspondant à des mesures de prévention;
- les activités de surveillance et de contrôle continu (notamment, les éléments qui vont être surveillés et contrôlés, comment et quand ils vont l'être, et par qui);
- les actions correctives si des écarts par rapport aux limites critiques sont détectés;
- les activités de vérification et de tenue des archives.

B.7.6 Avantages et limites

Les avantages sont les suivants:

- processus structuré témoignant de la réalisation du contrôle de qualité ainsi que de l'identification et la réduction des risques;
- porte sur les aspects pratiques liés à la manière d'éviter les dangers et de contrôler les risques à différentes étapes du processus;
- encourage le contrôle des risques tout au long du processus, plutôt que le contrôle du produit fini;
- permet d'identifier les dangers liés aux actions humaines, et la manière de les contrôler à l'endroit même où ils peuvent se produire, ou ultérieurement.

Les limites sont les suivantes:

- la méthode HACCP nécessite d'identifier les dangers, les risques qu'ils représentent et leur importance, perçus comme des entrées dans le processus. Des contrôles appropriés doivent également être définis. Cela est nécessaire pour préciser les points de contrôle critiques et les paramètres de contrôle lors d'une analyse HACCP. A cette fin, ces différents éléments peuvent être combinés avec d'autres outils;
- les modifications progressives apportées aux paramètres de contrôle significatifs du point de vue statistique peuvent échapper à l'action entreprise lorsque ces paramètres dépassent les limites définies et qu'il convient, de ce fait, de réaliser.

B.7.7 Document de référence

ISO 22000, *Systèmes de management de la sécurité des denrées alimentaires – Exigences pour tout organisme appartenant à la chaîne alimentaire*

B.8 Evaluation de la toxicité

B.8.1 Présentation

L'évaluation des risques environnementaux porte ici sur le processus d'évaluation des risques auxquels sont exposés les végétaux, les animaux et les hommes à la suite d'une série de dangers environnementaux. La gestion des risques concerne la procédure de prise de décision, comprenant l'évaluation et le traitement des risques.

La méthode implique d'analyser le danger ou la source d'une nuisance et la mesure dans laquelle il affecte une population ciblée, ainsi que les différents vecteurs par lesquels il peut la toucher. Ces informations sont ensuite combinées pour donner une estimation de l'étendue et de la nature probables de la nuisance.

B.8.2 Utilisation

Le processus est utilisé pour évaluer les risques auxquels sont exposés les végétaux, les animaux et les hommes à la suite des dangers liés à des produits chimiques, des micro-organismes ou d'autres espèces.

Différents aspects de la méthodologie, par exemple l'analyse du cheminement, permettant d'explorer les différentes voies d'exposition d'une cible à une source de risque, peuvent être adaptés et utilisés dans de très nombreuses zones de risque différentes, outre la santé et l'environnement, et sont utiles pour identifier les traitements permettant de limiter les risques.

B.8.3 Entrées

La méthode implique la détention de données fiables quant à la nature et aux propriétés des dangers considérés, aux prédispositions de la/des population(s) ciblée(s) et à la manière dont ces deux facteurs interagissent. En général, ces données reposent sur une recherche en laboratoire ou épidémiologique.

B.8.4 Processus

Les étapes du processus sont les suivantes:

a) Formulation du problème – il s'agit de définir le domaine d'application de l'évaluation en définissant l'étendue des populations ciblées et les types de dangers considérés;

b) Identification des dangers – il s'agit d'identifier toutes les sources possibles de nuisance auxquelles est exposée la population ciblée par rapport aux dangers entrant dans le domaine d'application de l'étude. En principe, l'identification des dangers repose sur l'expertise et un examen de la documentation disponible;

c) Analyse de danger – il s'agit de bien cerner la nature du danger et la manière dont il interagit avec la cible. Par exemple, en cas d'exposition d'une personne à des effets chimiques, le danger peut inclure la toxicité aiguë et chronique, le risque de lésion de l'ADN ou de cancer ou malformations congénitales. Pour chaque effet dangereux, l'amplitude de l'effet (la réponse) est comparée à l'ampleur du danger auquel est exposée la cible (la dose), le mécanisme produisant l'effet étant, dans la mesure du possible, déterminé. La Dose Sans Effets (DSE) et la Dose Sans Effets Nocifs Observés (DSENO) sont notées. Ces éléments sont parfois utilisés comme critères d'acceptabilité du risque.

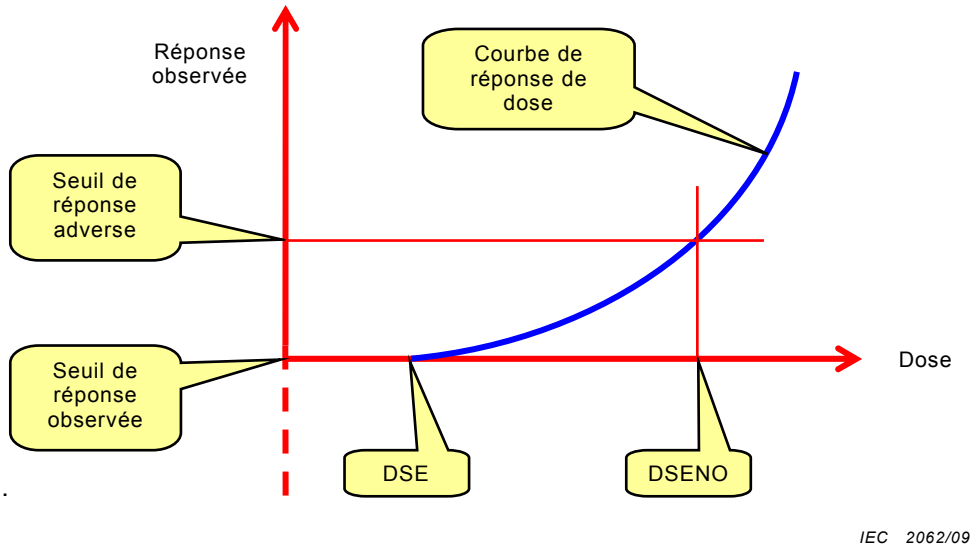

Figure B.1 – Courbe dose-effet

Dans le cas d'une exposition à un produit chimique, les résultats d'essai sont utilisés pour déduire les courbes dose-effet analogues à celle illustrée dans la Figure B.1. Ces courbes sont en général déduites des essais réalisés sur des animaux ou de systèmes expérimentaux (tissus ou cellules de culture, par exemple).

Les effets d'autres dangers (les micro-organismes ou les espèces introduites, par exemple) peuvent être déterminés à partir de données d'exploitation et d'études épidémiologiques. La nature de l'interaction entre les maladies ou organismes nuisibles et la cible est déterminée, la probabilité d'occurrence d'un niveau de nuisance particulier à la suite d'une exposition particulière au danger étant estimée.

d) Analyse de l'exposition – cette étape permet de comprendre comment, et dans quelle mesure, un danger ou ses suites résiduelles peuvent atteindre une population ciblée. Elle implique souvent une analyse du cheminement, qui tient compte des différents vecteurs de propagation du danger, des barrières qui pourraient protéger la cible et des facteurs pouvant influencer le niveau d'exposition. Par exemple, soit un risque provenant d'une projection chimique: l'analyse d'exposition tiendrait compte de facteurs comme l'ampleur de la projection, la manière et les conditions de sa survenue, déterminerait si des personnes ou des animaux ont été directement exposés, la quantité de résidu déposée sur les végétaux, l'évolution du produit dans l'environnement, s'il peut s'accumuler dans le corps des animaux ou s'il se diffuse dans les nappes phréatiques. En matière de biosécurité, l'analyse du cheminement peut tenir compte de la manière dont les organismes nuisibles entrant dans un pays peuvent envahir l'environnement, s'installer et se disperser.

e) Caractérisation du risque – à cette étape, les informations provenant de l'analyse de danger et de l'analyse de l'exposition sont rassemblées afin d'estimer la probabilité de conséquences particulières lorsque les effets de tous les cheminements sont combinés. En présence d'un grand nombre de dangers ou de cheminements, il est possible de procéder à un dépistage initial et à une analyse détaillée des dangers et de l'exposition, et de caractériser les risques afin de déterminer les scénarii les plus pessimistes.

B.8.5 Résultats

En principe, le résultat détermine le niveau de risque d'exposition d'une cible particulière à un danger particulier dans le contexte concerné. Le risque peut être exprimé de manière quantitative, semi-quantitative ou qualitative. Par exemple, le risque de cancer est souvent exprimé de manière quantitative comme la probabilité à laquelle est confrontée une personne de développer un cancer sur une période donnée, compte tenu d'une exposition spécifiée à un polluant. L'analyse semi-quantitative peut permettre de déduire un indice de risque pour un polluant ou un organisme nuisible particulier, le résultat qualitatif pouvant être un niveau de risque (élevé, moyen ou faible, par exemple) ou une description avec des données pratiques sur les effets probables.

B.8.6 Avantages et limites

L'avantage de cette analyse est qu'elle permet de bien comprendre la nature du problème et les facteurs augmentant le risque.

D'une manière générale, l'analyse du cheminement est un outil très utile, adapté à tous les domaines de risque, permettant d'identifier comment et dans quelle mesure il peut être possible d'améliorer les contrôles ou d'en introduire de nouveaux.

Toutefois, elle exige des données précises, qui ne sont pas toujours disponibles ou dont le niveau d'incertitude est souvent élevé. Par exemple, il convient d'extrapoler les courbes dose-effet déduites de l'exposition d'animaux à des niveaux élevés de danger afin d'estimer les effets de niveaux très faibles de polluant sur l'homme, de nombreux modèles étant à disposition à cet effet. Si la cible est l'environnement et pas l'homme, et que le danger n'est pas de nature chimique, les données se rapportant directement aux conditions particulières de l'étude peuvent être limitées.

B.9 Méthode SWIFT («Que Se Passerait-il Si ?»)

B.9.1 Présentation

A l'origine, la méthode SWIFT a été développée comme une alternative plus simple à la méthode HAZOP. Il s'agit d'une étude systématique réalisée par une équipe utilisant un ensemble de mots ou de phrases «à effet immédiat» que le facilitateur utilise dans un atelier pour stimuler les participants en matière d'identification des risques. Le facilitateur et l'équipe utilisent des phrases du type «que se passerait-il si ?», en combinaison avec les invites, pour déterminer l'impact des écarts par rapport aux fonctionnements et comportements normaux sur un système, un élément de l'installation, une organisation ou un mode opératoire. En principe, la méthode SWIFT s'applique à plusieurs niveaux du système, pour un niveau de détail moins élevé que celui de la méthode HAZOP.

B.9.2 Utilisation

Si, à l'origine, la méthode SWIFT a été développée pour les études des dangers liés aux usines chimiques et pétrochimiques, la technique est à présent largement appliquée aux systèmes, éléments de l'installation, modes opératoires et organisations. En particulier, elle permet d'examiner les conséquences de certains changements et les risques ainsi modifiés ou créés.

B.9.3 Entrées

Le système, le mode opératoire, l'élément de l'installation et/ou la modification doivent être soigneusement définis avant d'entamer l'étude. Les contextes externe et interne sont établis à la suite des entretiens et à l'étude de documents, de plans et de dessins menés par le facilitateur. En principe, l'élément, la situation ou le système étudié est divisé en nœuds ou éléments-clés afin de faciliter le processus d'analyse, mais cela se produit rarement au niveau de définition requis pour la méthode HAZOP.

Une autre entrée-clé est l'expertise et l'expérience dont bénéficie l'équipe chargée de l'étude, équipe qu'il convient de choisir avec soin. Dans la mesure du possible, il convient de partager l'expérience de tous les acteurs face à des éléments, systèmes, modifications ou situations analogues.

B.9.4 Processus

Le processus général suivi est le suivant:

a) Avant de commencer l'étude, le facilitateur prépare une liste de mots ou de phrases à effet immédiat pouvant reposer sur un ensemble de normes, ou donnant un aperçu exhaustif des dangers et des risques.

b) Au cours de l'atelier, les contextes externe et interne liés à l'élément, au système, à la modification ou à la situation et le domaine d'application de l'étude sont discutés et fixés.

c) Le facilitateur demande aux participants de relever et de présenter:

   – les risques et dangers connus;

   – les expériences et incidents précédents;

   – les contrôles et dispositifs de protection connus et existants;

   – les exigences et contraintes réglementaires.

d) La discussion est facilitée par une question du type «que se passerait-il si ?» et un mot ou sujet-guide. Les phrases du type «que se passerait-il si ?» à utiliser sont «que se passerait-il si», «quelqu'un ou quelque chose pourrait-il... ?», «quelqu'un ou quelque chose a-t-il déjà... ?». L'idée est d'inciter l'équipe chargée de l'étude à explorer des scénarii potentiels, leurs causes, leurs conséquences et leurs impacts.

e) Les risques sont résumés et l'équipe se penche sur les contrôles en place.

f) La description du risque, ses causes, ses conséquences et les contrôles prévus sont confirmés avec l'équipe, puis notés.

g) L'équipe étudie l'adéquation et l'efficacité des contrôles, puis convient d'une déclaration d'efficacité du contrôle des risques. Si elles ne sont pas satisfaisantes, les tâches de traitement des risques et les contrôles potentiels de l'équipe sont définis de manière plus approfondie.

h) Lors de la discussion, des questions du type «que se passerait-il si ?» plus précises sont posées pour identifier des risques supplémentaires.

i) Le facilitateur utilise la liste de mots-guides pour orienter la discussion et soumet des questions et scénarii supplémentaires à la réflexion de l'équipe.

j) Il est normal d'utiliser une méthode d'évaluation des risques qualitative ou semi-quantitative pour classer les actions créées en fonction de leur priorité. En principe, les risques sont évalués en tenant compte des contrôles existants et de leur efficacité.

B.9.5 Résultats

Les résultats comportent un registre dans lequel les actions ou les tâches sont classées en fonction du risque. Ces tâches peuvent ensuite être la base d'un plan de traitement.

B.9.6 Avantages et limites

Les avantages de la méthode SWIFT sont les suivants:

- elle peut être largement appliquée à toutes les formes d'installation ou de système, de situation ou de circonstance, d'organisation ou d'activité;
- elle demande peu de préparation par l'équipe;
- elle est relativement rapide et les principaux dangers et risques apparaissent rapidement au cours de l'atelier;
- l'étude est «orientée système» et permet aux participants de voir comment le système réagit aux écarts, plutôt que de simplement examiner les conséquences de la défaillance d'un composant;
- elle peut être utilisée pour identifier les opportunités d'amélioration des processus et des systèmes et, d'une manière générale, pour identifier les actions entraînant et augmentant les chances de conséquences favorables;
- elle permet d'impliquer dans l'atelier les personnes responsables des contrôles existants et des actions supplémentaires de traitement des risques, et d'accroître leurs responsabilités;

- elle permet de créer un registre des risques et un plan de traitement des risques sans effort supplémentaire;
- alors que, bien souvent, une forme qualitative ou semi-quantitative de classement des risques est utilisée pour évaluer les risques et attirer l'attention sur les actions qui en résultent, la méthode SWIFT peut être utilisée pour identifier les risques et dangers considérés dans une étude quantitative.

Les limites de la méthode SWIFT sont les suivantes:

- pour être efficace, le facilitateur doit être compétent;
- elle exige une préparation soignée, de sorte que l'équipe ne perde pas son temps;
- si l'expérience de l'équipe n'est pas suffisante ou si le système indicatif n'est pas cohérent, certains risques ou dangers peuvent ne pas être identifiés;
- l'application de la technique à haut niveau peut ne pas révéler les causes complexes, détaillées ou corrélées.

B.10 Analyse du scénario

B.10.1 Présentation

L'analyse du scénario est un nom donné au développement de modèles descriptifs de la manière dont l'avenir peut se présenter. Elle peut être utilisée pour identifier les risques en tenant compte des développements futurs possibles et en explorant leurs implications. Des ensembles de scénarii reflétant (par exemple) le « meilleur cas », le « pire cas » et le « cas prévu » peuvent être utilisés pour analyser les conséquences potentielles et leurs probabilités pour chaque scénario sous la forme d'une analyse de sensibilité dans le cadre de l'analyse des risques.

La puissance de l'analyse du scénario est illustrée en tenant compte des principales évolutions technologiques des 50 dernières années, des préférences des consommateurs, des attitudes sociales, etc. L'analyse du scénario ne permet pas de prévoir la probabilité de telles évolutions, mais elle permet de considérer leurs conséquences et d'aider les organisations à développer les forces et la résilience nécessaires pour s'adapter aux modifications prévisibles.

B.10.2 Utilisation

L'analyse du scénario peut être utilisée pour faciliter les prises de décision et la planification de futures stratégies, tout en tenant compte des activités existantes. Elle peut jouer un rôle dans les trois composants de l'évaluation des risques. Pour l'identification et l'analyse, des ensembles de scénarii reflétant, par exemple, le meilleur et le pire des cas, ainsi que les cas «prévus», peuvent permettre d'identifier les événements susceptibles de se produire dans des conditions particulières et d'analyser les conséquences potentielles et leur probabilité pour chaque scénario.

L'analyse du scénario peut être utilisée pour anticiper l'apparition de menaces et d'opportunités, et peut être utilisée pour tous les types de risque à court et long termes. Avec de courtes échéances et des données fiables, des scénarii potentiels peuvent être extrapolés depuis le présent. Pour les échéances plus longues ou des données moins fiables, l'analyse du scénario devient plus imaginative et peut faire référence à de futures analyses.

L'analyse du scénario peut être utile lorsqu'il existe d'importantes différences de répartition entre les résultats positifs et les résultats négatifs dans l'espace, le temps et les groupes d'une communauté ou une organisation.

B.10.3 Entrées

Une analyse du scénario exige de constituer une équipe de personnes ayant une bonne connaissance de la nature des évolutions (les avancées technologiques possibles, par exemple), et étant en mesure d'anticiper les événements à venir sans nécessairement les extrapoler en fonction d'événements passés. Il est également utile d'exploiter la documentation et les données relatives aux évolutions en cours.

B.10.4 Processus

La structure de l'analyse du scénario peut être formelle ou informelle.

Après avoir constitué une équipe et déterminé les canaux de communication adaptés, puis défini le contexte du problème et des questions à considérer, l'étape suivante consiste à identifier la nature des changements susceptibles de se produire. Il s'agira de faire des recherches sur les principales tendances, de déterminer le moment probable des changements de tendance, et d'anticiper l'avenir.

Les changements à prendre en compte peuvent inclure:

- les changements extérieurs (évolutions technologiques, par exemple);
- les décisions à prendre dans un futur proche, mais qui peuvent produire différents résultats;
- les besoins des différents acteurs et la manière dont ils peuvent changer;
- les changements macro-environnementaux (réglementation, caractéristiques socio-démographiques, etc.). Certains seront inévitables et d'autres incertains.

Parfois, un changement peut être le résultat des conséquences d'un autre risque. Par exemple, le risque de changement climatique modifie la demande des consommateurs en fonction des distances des approvisionnements alimentaires. Cela permettra de distinguer les aliments qui pourront être utilement exportés de ceux qui pourront être cultivés localement.

Il est désormais possible de répertorier les facteurs ou tendances locaux et macro et de les classer en fonction (1) de leur importance et (2) de leur incertitude. Une attention particulière est accordée aux facteurs les plus importants et les plus incertains. Les facteurs ou tendances-clés sont mis en correspondance avec d'autres pour déterminer les zones dans lesquelles des scénarii peuvent être développés.

Une série de scénarii est proposée, chacun d'eux portant sur un changement plausible des paramètres.

Une «histoire» est alors écrite pour chaque scénario, racontant le processus de passage immédiat au scénario documentaire. Ces histoires peuvent contenir des détails plausibles apportant de la valeur aux scénarii.

Les scénarii peuvent désormais être utilisés pour évaluer la question originale. L'essai tient compte de tous les facteurs significatifs prévisibles (les modes d'emploi, par exemple), détermine dans quelle mesure la règle (l'activité) pourrait aboutir dans le cadre de ce nouveau scénario, puis procède à un «essai préalable» des résultats à l'aide des questions du type «que se passerait-il si ?» en fonction d'hypothèses de modèle.

Si la question ou la proposition a été évaluée en fonction de chaque scénario, des modifications peuvent s'imposer pour la renforcer ou la rendre moins risquée. Il convient qu'il soit également possible d'identifier certains indicateurs avancés mettant en évidence le moment du changement. La surveillance et la réponse aux indicateurs avancés peuvent offrir une opportunité de changement dans les stratégies planifiées.

Etant donné que les scénarii ne sont que des «couches» définies de futurs possibles, il est important de veiller à tenir compte de la probabilité d'un résultat particulier (scénario) se produisant, c'est-à-dire d'adopter un cadre de risque. Par exemple, si des scénarii de meilleur des cas, de pire des cas et de cas prévus sont utilisés, il convient de tenter de qualifier ou d'exprimer la probabilité de survenue de chaque scénario.

B.10.5 Résultats

Il peut ne pas y avoir de meilleur scénario, mais il convient d'avoir un meilleur aperçu de l'étendue des options et de la manière de modifier le déroulement choisi des actions au fur et à mesure du déplacement des indicateurs.

B.10.6 Avantages et limites

L'analyse de scénario tient compte d'un éventail d'événements à venir possibles. Elle peut s'avérer préférable à l'approche traditionnelle consistant à s'appuyer sur des prévisions à court, moyen et long termes supposant, par l'utilisation de données historiques, que les événements futurs seront susceptibles d'être conformes aux tendances passées. Cet élément est important lorsque les connaissances actuelles sur lesquelles reposent les prévisions sont limitées, ou lorsque les risques sont pris en compte à plus long terme.

Toutefois, cet avantage comporte un inconvénient, en ce sens que les scénarii peuvent être peu réalistes lorsque l'incertitude est élevée.

Les principales difficultés de l'utilisation d'une analyse de scénario sont liées à la disponibilité des données, et à l'aptitude des analystes et des décideurs à développer des scénarii réalistes et à examiner les résultats possibles.

Les dangers de l'utilisation d'une analyse de scénario comme outil de prise de décision sont que les fondements des scénarii utilisés peuvent ne pas être adaptés, que les données peuvent s'avérer spéculatives et que les résultats irréalistes peuvent ne pas être interprétés comme tels.

B.11 Analyse d'impact sur l'activité (AIA)

B.11.1 Présentation

L'analyse d'impact sur l'activité, également appelée évaluation d'impact sur l'activité, propose d'analyser la manière dont les principaux risques de perturbation pourraient avoir un impact sur les opérations d'une organisation, puis d'identifier et de quantifier les aptitudes nécessaires à leur gestion. De manière spécifique, l'AIA propose une compréhension convenue de:

- l'identification et le caractère critique des processus métier-clés, des fonctions et des ressources associées et les principales interdépendances qui existent au sein d'une organisation;
- l'impact d'un sinistre sur la capacité et la possibilité d'atteindre des objectifs commerciaux essentiels;
- la capacité et les aptitudes nécessaires pour gérer l'impact d'un sinistre et aider l'organisation à retrouver des volumes d'opérations acceptables.

B.11.2 Utilisation

L'analyse d'impact sur l'activité permet de déterminer le caractère critique et les calendriers de relance des processus et ressources de soutien (personnes, équipement, technologies d'information afin de garantir l'atteinte des objectifs. En outre, elle facilite la détermination des interdépendances et des relations entre les processus, les parties internes et externes et les liens de la chaîne logistique.

B.11.3 Entrées

Les entrées sont les suivantes:

- une équipe pour réaliser l'analyse et développer un plan;
- une bonne compréhension des objectifs, de l'environnement, des opérations et des interdépendances de l'organisation;
- les caractéristiques des activités et opérations de l'organisation, y compris les processus, les ressources de soutien, les relations avec les autres organisations, les conventions d'externalisation, les différents acteurs;
- les conséquences financières et opérationnelles de la perte de processus critiques;
- le questionnaire préparé;
- la liste des personnes interrogées dans les services pertinents de l'organisation et/ou les différents acteurs à contacter.

B.11.4 Processus

Une analyse d'impact sur l'activité peut être réalisée sur la base de questionnaires, d'entretiens, d'ateliers structurés, ou sur une combinaison de ces trois paramètres, afin de bien appréhender les processus critiques, les effets liés à leur perte et les calendriers de reprise et ressources de soutien nécessaires.

Les étapes clés comprennent:

- à la suite de l'évaluation des risques et de la vulnérabilité, la confirmation des processus-clés et des résultats de l'organisation pour déterminer le caractère critique des processus;
- la détermination des conséquences d'un sinistre sur les processus critiques identifiés, en termes financiers et/ou opérationnels, sur des périodes définies;
- l'identification des interdépendances avec les différents acteurs-clés internes et externes. Il peut s'agir de mettre en correspondance la nature des interdépendances tout au long de la chaîne logistique;
- la détermination des ressources disponibles réelles et du niveau essentiel des ressources requises pour poursuivre l'activité à un niveau minimal acceptable, à la suite de la survenue d'un sinistre;
- l'identification d'autres solutions palliatives et processus en cours d'utilisation ou dont le développement est prévu. Il peut s'avérer nécessaire de développer d'autres solutions palliatives et processus lorsque les ressources ou capacités sont inaccessibles ou insuffisantes lors de la survenue du sinistre;
- la détermination de la durée maximale d'indisponibilité (DMI) pour chaque processus en fonction des conséquences identifiées et des facteurs de succès critiques de la fonction. La durée maximale d'indisponibilité représente le délai maximal au cours duquel l'organisation peut tolérer la perte de capacité;
- la détermination des objectifs de temps de remise en état (OTR) pour un équipement spécialisé ou une infrastructure de technologies d'information. L'objectif de temps de remise en état est la durée au cours de laquelle l'organisation a pour objectif de recouvrer la capacité de l'équipement spécialisé de l'infrastructure de technologies d'information;
- la confirmation du niveau de préparation actuel des processus critiques pour gérer un sinistre. Il peut s'agir d'évaluer le niveau de redondance au sein du processus (les équipements de rechange, par exemple) ou l'existence d'autres fournisseurs.

B.11.5 Résultats

Les résultats sont les suivants:

- une liste de priorités des processus critiques et des interdépendances associées;
- les impacts financiers et opérationnels documentés à la suite d'une perte des processus critiques;
- les ressources de soutien nécessaires pour les processus critiques identifiés;
- les calendriers d'indisponibilité des processus critiques et les calendriers de remise en état des technologies d'information associés.

B.11.6 Avantages et limites

L'analyse d'impact sur l'activité présente les avantages suivants:

- bonne compréhension des processus critiques permettant à l'organisation de continuer à suivre ses objectifs prévus;
- bonne compréhension des ressources requises;
- opportunité de redéfinir les processus opérationnels d'une organisation afin de faciliter la résilience de l'organisation.

Les limites sont les suivantes:

- manque de connaissance des participants aux questionnaires, aux entretiens ou aux ateliers;
- la dynamique de groupe peut avoir un impact sur l'analyse exhaustive d'un processus critique;
- attentes simplistes ou surréalistes des exigences de reprise;
- difficulté à obtenir le niveau de compréhension adéquat des opérations et activités de l'organisation.

B.12 Analyse de causes profondes

B.12.1 Présentation

L'analyse d'une perte majeure pour empêcher qu'elle ne se reproduise est habituellement appelée Analyse de Causes Profondes (RCA[6]), Analyse des défaillances de Causes Profondes (RCFA[7]) ou analyse de perte. L'analyse RCA porte sur les pertes d'actifs à la suite de différents types de défaillance, alors que l'analyse de perte porte essentiellement sur les pertes financières ou économiques en raison de facteurs externes ou de catastrophes. Elle tente d'identifier les causes racines ou d'origine au lieu de ne traiter que les symptômes immédiatement évidents. Il est convenu que l'action corrective ne peut pas toujours être complètement efficace et qu'une amélioration continue peut s'avérer nécessaire. Le plus souvent, l'analyse RCA s'applique à l'évaluation d'une perte majeure, mais peut également être utilisée pour analyser les pertes d'un point de vue plus global afin de déterminer à quel niveau les améliorations peuvent être apportées.

B.12.2 Utilisation

L'analyse RCA s'applique dans différents contextes, avec les larges domaines d'utilisation suivants:

- l'analyse RCA basée sur la sécurité est utilisée dans le cadre d'enquêtes sur les accidents et de l'hygiène et la sécurité au travail;
- l'analyse des défaillances est utilisée dans les systèmes technologiques liés à la fiabilité et la maintenance;

---

6 RCA = *Root Cause Analysis*

7 RCFA = *Root Cause Failure Analysis*

- l'analyse RCA basée sur la production s'applique dans le domaine du contrôle de qualité de la fabrication industrielle;
- l'analyse RCA basée sur les processus porte sur les processus-métier;
- l'analyse RCA basée sur les systèmes a été développée comme une combinaison des domaines précédents. Il s'agit de traiter les systèmes complexes, trouvant leur application dans la gestion des changements, la gestion des risques et l'analyse des systèmes.

B.12.3 Entrées

L'entrée principale d'une analyse RCA est un regroupement de toutes les preuves de défaillance ou de perte. Les données provenant d'autres défaillances analogues peuvent également être prises en compte dans l'analyse. D'autres entrées peuvent être des résultats permettant de tester des hypothèses particulières.

B.12.4 Processus

Lorsqu'une analyse RCA s'avère nécessaire, un groupe d'experts est convoqué pour procéder à l'analyse et faire des recommandations. Le type d'expert dépend principalement de l'expertise particulière nécessaire à l'analyse de la défaillance.

Même s'il est possible d'utiliser différentes méthodes pour procéder à l'analyse, les procédures de base en matière d'analyse RCA sont similaires et comprennent:

- la constitution de l'équipe;
- la définition du domaine d'application et des objectifs de l'analyse RCA;
- la collecte de données et de preuves de défaillance ou de perte;
- la réalisation d'une analyse structurée visant à déterminer la cause profonde;
- le développement de solutions et la stipulation de recommandations;
- la mise en œuvre des recommandations;
- la vérification du succès des recommandations mises en œuvre.

Les techniques d'analyse structurée peuvent comporter l'un des éléments suivants:

- technique de «5 raisons» - c'est-à-dire poser la question « pourquoi ? » à plusieurs reprises pour détacher les couches de cause et sous-cause);
- l'analyse des modes de défaillance et de leurs effets;
- l'analyse par arbre de panne;
- les diagrammes d'Ishikawa;
- l'analyse de Pareto;
- la mise en correspondance de la cause profonde.

L'évaluation des causes commence souvent par l'analyse des causes physiques initialement évidentes et humaines, pour évoluer vers des causes liées à la gestion ou fondamentales. Les facteurs de causalité doivent pouvoir être contrôlés ou éliminés par les parties concernées afin d'assurer l'efficacité et l'intérêt de l'action corrective.

B.12.5 Résultats

Les résultats d'une analyse RCA sont les suivants:

- documentation des données et preuves collectées;
- hypothèses considérées;

- conclusion concernant les causes-racine les plus probables de la défaillance ou de la perte;
- recommandations d'une action corrective.

B.12.6 Avantages et limites

Les avantages sont les suivants:

- implication d'experts concernés travaillant en équipe;
- analyse structurée;
- prise en compte de toutes les hypothèses probables;
- documentation des résultats;
- nécessité de produire des recommandations finales.

Les limites d'une analyse RCA peuvent être les suivantes:

- les experts concernés peuvent ne pas être disponibles;
- des preuves essentielles peuvent avoir été détruites lors de la défaillance ou supprimées lors du nettoyage;
- l'équipe peut ne pas disposer d'assez de temps ou de ressources suffisantes pour évaluer complètement la situation;
- il peut ne pas être possible de mettre en œuvre les recommandations de manière convenable.

B.13 Analyse des modes de défaillance et de leurs effets (AMDE) et analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)

B.13.1 Présentation

L'analyse des modes de défaillance et de leurs effets (AMDE) est une technique permettant d'identifier dans quelles mesures les composants, les systèmes ou les processus peuvent tomber en panne pour exécuter la conception prévue.

L'AMDE permet d'identifier:

- tous les modes de défaillance potentiels des différentes parties d'un système (un mode de défaillance est l'observation d'une panne ou de ce qui ne fonctionne pas correctement);
- les effets que ces défaillances peuvent avoir sur le système;
- les causes de la défaillance;
- la manière d'éviter les défaillances et/ou de limiter leurs effets sur le système.

La méthode AMDEC développe une AMDE de sorte que chaque mode de défaillance identifié soit classé conformément à son importance ou criticité.

D'une manière générale, il s'agit d'une analyse qualitative ou semi-quantitative, mais qui peut être quantifiée à l'aide des taux de défaillance actuels.

B.13.2 Utilisation

Il existe plusieurs types de méthode AMDE: l'AMDE Conception (ou produit), qui est utilisée pour les composants et les produits, l'AMDE Système utilisée pour les systèmes, l'AMDE Processus utilisée pour les processus de fabrication et d'assemblage, l'AMDE Service et l'AMDE Logiciel.

L'AMDE/AMDEC peut être appliquée lors de la conception, de la fabrication ou du fonctionnement d'un système.

Toutefois, pour améliorer la sûreté de fonctionnement, il est généralement plus aisé de mettre en œuvre les modifications lors de la phase de conception. L'AMDE et l'AMDEC peuvent également être appliquées aux processus et aux procédures. Elle est par exemple utilisée pour identifier le potentiel d'erreur médicale dans les systèmes de soins de santé et de défaillances dans les procédures de maintenance.

L'AMDE/AMDEC peut être utilisée pour

- faciliter la sélection d'alternatives de conception à haute sûreté de fonctionnement,
- s'assurer que tous les modes de défaillance des systèmes et processus, et leurs effets sur le succès opérationnel ont été pris en compte,
- identifier les modes de défaillance humaine et leurs effets,
- fournir un socle de planification des essais et de la maintenance des systèmes physiques,
- améliorer la conception des procédures et des processus,
- fournir des informations qualitatives ou quantitatives pour les techniques d'analyse, telles que l'analyse par arbre de panne.

L'AMDE/AMDEC peut apporter des éléments d'entrée à d'autres techniques d'analyse (l'analyse par arbre de panne, par exemple) du point de vue qualitatif ou quantitatif.

B.13.3 Entrées

L'AMDE et l'AMDEC requièrent des informations suffisamment détaillées relatives aux composants du système pour permettre de procéder à une analyse significative des manières dont chaque composant peut tomber en panne. Pour une AMDE Conception détaillée, l'élément peut se situer au niveau détaillé de composant individuel alors que pour une AMDE Système de niveau supérieur, les éléments peuvent être définis à un niveau plus élevé.

Ces informations peuvent comprendre:

- des schémas ou un organigramme du système en cours d'analyse et de ses composants, ou les étapes d'un processus;
- une bonne compréhension de la fonction de chaque étape d'un processus ou d'un composant d'un système;
- les détails du processus et des paramètres environnementaux, susceptibles d'affecter le fonctionnement;
- une compréhension des résultats liés à des défaillances particulières;
- des informations historiques relatives aux défaillances, comprenant les taux de panne calculés, le cas échéant.

B.13.4 Processus

Les étapes de l'analyse AMDE sont les suivantes:

a) définition du domaine d'application et des objectifs de l'étude;

b) constitution de l'équipe;

c) compréhension du système/processus faisant l'objet de l'analyse AMDEC;

d) décomposition du système en ses composants ou en étapes;

e) définition de la fonction de chaque étape ou composant;

f) pour chaque composant ou étape, répondre aux questions suivantes:

   - est-il concevable qu'un composant tombe en panne?

- quels sont les mécanismes susceptibles de produire ces modes de défaillance?
- quels seraient les effets d'éventuelles défaillances?
- la défaillance est-elle anodine ou dangereuse?
- comment la défaillance a-t-elle été détectée?

g) Identifier des dispositions inhérentes dans la conception pour compenser la défaillance.

Pour l'analyse AMDEC, l'équipe chargée de l'étude classe chacun des modes de défaillance identifiés en fonction de sa criticité.

Ceci peut être réalisé de plusieurs manières. Les méthodes courantes sont les suivantes:

- l'indice de criticité du mode;
- le niveau de risque;
- le degré de priorité du risque.

Le modèle de criticité est une mesure de la probabilité que le mode considéré donnera lieu à une défaillance du système dans son ensemble; il est défini comme suit:

Probabilité d'effet de défaillance * Taux de défaillance de mode * Temps de fonctionnement du système

Il est le plus souvent appliqué aux défaillances d'équipement pour lesquelles chacun de ces termes peut être défini de manière quantitative et les modes de défaillance ont tous la même conséquence.

Le niveau de risque est obtenu en combinant les conséquences d'un mode de défaillance et la probabilité de défaillance. Il est utilisé lorsque les conséquences des différents modes de défaillance ne sont pas les mêmes et il peut être appliqué aux systèmes ou processus des équipements. Le niveau de risque peut être exprimé de manière qualitative, semi-quantitative ou quantitative.

Le degré de priorité du risque (NRP) est une mesure semi-quantitative de la criticité obtenue en multipliant les nombres des échelles de classement (généralement comprise entre 1 et 10) correspondant à la conséquence de la défaillance, probabilité de défaillance et aptitude à détecter le problème. (Une priorité élevée est attribuée à une défaillance en cas de difficulté de détection.) Cette méthode est le plus souvent utilisée dans des applications d'assurance de qualité.

Une fois identifiés les modes et mécanismes de défaillance, il est possible de définir et de mettre en œuvre des actions correctives pour les modes de défaillance les plus significatifs.

L'AMDE est documentée dans un rapport contenant:

- les caractéristiques du système analysé;
- la manière dont l'analyse a été réalisée;
- les hypothèses avancées dans l'analyse;
- les sources des données;
- les résultats, y compris les fiches de travail renseignées;
- la criticité (si traitée) et la méthodologie utilisée pour la définir;
- toutes les recommandations pour des analyses approfondies, des changements de conception ou des fonctions à intégrer dans les plans d'essai, etc.

Le système peut être réévalué par un autre cycle d'analyse AMDE, à l'issue des actions entreprises.

B.13.5 Résultats

Le principal résultat de l'analyse AMDE est une liste des modes de défaillance, des mécanismes de défaillance et des effets pour chaque composant d'un système ou étape d'un processus (qui peut inclure des informations sur la probabilité de défaillance). Des informations sont également données sur les causes de la défaillance et ses conséquences sur l'ensemble du système. Les résultats de l'analyse AMDEC incluent une évaluation de l'importance fondée sur la probabilité de défaillance du système, le niveau de risque résultant du mode de défaillance ou une combinaison du niveau de risque et de « l'aptitude à la détection » du mode de défaillance.

L'analyse AMDEC peut donner un résultat quantitatif lorsqu'on utilise des données de taux de défaillance appropriées et des conséquences quantitatives.

B.13.6 Avantages et limites

Les analyses AMDE/AMDEC présentent les avantages suivants:

- elles s'appliquent largement aux modes de défaillance humaine, d'équipements et de systèmes ainsi qu'aux matériels, logiciels et procédures;
- elles permettent d'identifier les modes de défaillance du composant, leurs causes et leurs effets sur le système, et de les présenter dans un format lisible;
- elles permettent d'éviter les modifications onéreuses de l'équipement en service par une identification précoce des problèmes dans le processus de conception;
- elles permettent d'identifier les modes de défaillance localisée et les exigences pour les systèmes redondants et de sécurité;
- elles offrent une entrée aux programmes d'essai de développement en mettant en évidence les fonctions essentielles à tester.

Les limites sont les suivantes:

- elles peuvent uniquement être utilisées pour identifier les modes de défaillance localisée, et pas les combinaisons de modes de défaillance;
- si les études ne sont pas convenablement contrôlées et mises au point, elles peuvent prendre du temps et être onéreuses;
- elles peuvent s'avérer difficiles et fastidieuses pour les systèmes complexes à plusieurs couches.

B.13.7 Document de référence

CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

B.14 Analyse par arbre de panne (AAP)

B.14.1 Présentation

La technique AAP permet d'identifier et d'analyser les facteurs qui peuvent contribuer à un événement indésirable spécifié (appelé «événement de tête»). Les facteurs de causalité sont identifiés de manière déductive et organisés de manière logique et graphique, sous la forme d'une arborescence décrivant les facteurs de causalité et leurs relations logiques à l'événement de tête.

Il peut s'agir d'événements associés à des défaillances matérielles de composants, à des erreurs humaines ou à tout autre événement pertinent donnant lieu à l'événement indésirable.

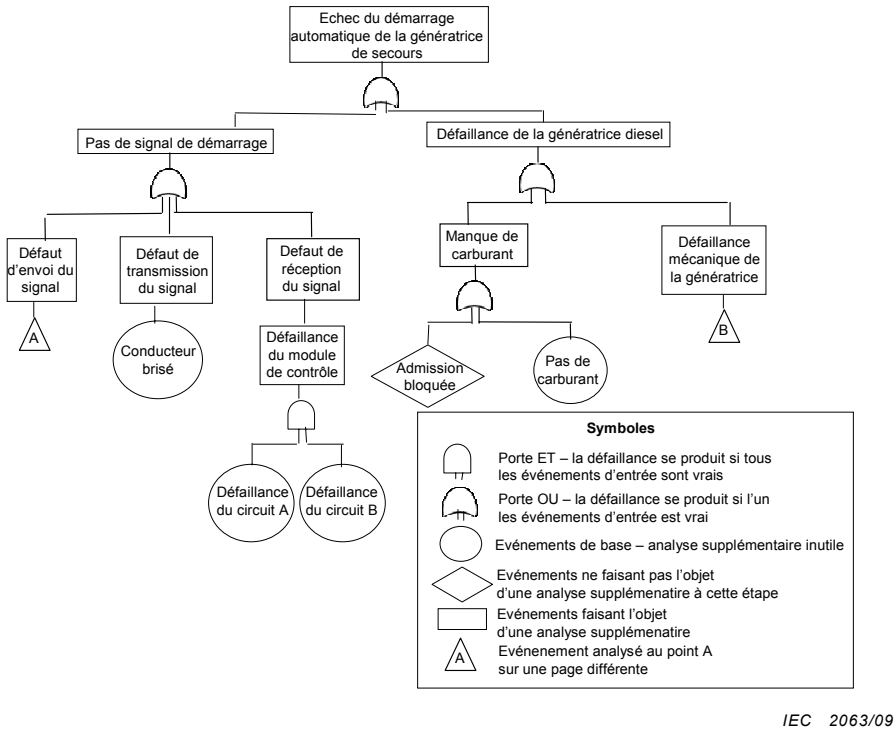

Figure B.2 – Exemple d'analyse par arbre de panne issu de la CEI 60300-3-9

B.14.2 Utilisation

Un arbre de panne peut être utilisé de manière qualitative pour identifier les causes et cheminements potentiels donnant lieu à une défaillance (l'événement de tête), ou de manière quantitative pour calculer la probabilité de l'événement de tête, compte tenu de la connaissance des probabilités des événements de causalité.

Il peut être utilisé à l'étape de la conception d'un système pour identifier les causes potentielles de défaillance et, par conséquent, faire un choix parmi les différentes options de conception. Il peut être utilisé à l'étape du fonctionnement pour identifier la manière dont les défaillances majeures peuvent se produire et l'importance relative des différents cheminements vers l'événement de tête. Un arbre de panne peut également être utilisé pour analyser une défaillance qui s'est produite afin d'afficher un graphique des différents événements à l'origine de la défaillance.

B.14.3 Entrées

Pour l'analyse qualitative, une bonne compréhension du système et des causes de la défaillance est requise ainsi qu'une compréhension technique de la manière dont le système peut tomber en panne. Des diagrammes détaillés sont utiles pour faciliter l'analyse.

Pour l'analyse quantitative, les taux de défaillance ou la probabilité d'être en état de défaillance pour tous les événements de base de l'arbre de panne sont requis.

B.14.4 Processus

La procédure de développement de l'arbre de panne est la suivante:

- L'événement de tête à analyser est défini. Il peut s'agir d'une défaillance ou du résultat plus général d'une défaillance. Si le résultat est analysé, l'arbre peut contenir une section portant sur la limitation de la défaillance réelle.

- En commençant par l'événement de tête, les causes possibles immédiates ou les modes de défaillance donnant lieu à l'événement de tête sont identifiés.
- Chacun de ces causes/modes de défaillance est analysé pour savoir comment la défaillance a pu se produire.
- En suivant progressivement l'identification du fonctionnement indésirable du système jusqu'aux niveaux système successivement inférieurs, l'analyse approfondie devient inutile. Dans un système matériel, il peut s'agir d'un niveau de défaillance du composant. Les événements et facteurs de causalité au niveau le plus bas du système analysé sont appelés événements de base.
- Si des probabilités peuvent être attribuées aux événements de base, il est possible de calculer la probabilité de l'événement de tête. Pour que la quantification soit valide, il doit être possible de démontrer que, pour chaque porte, toutes les entrées sont nécessaires et suffisantes pour produire l'événement de résultat. Si ce n'est pas le cas, l'arbre de panne n'est pas valide pour l'analyse de probabilité. Il peut néanmoins être un outil utile pour afficher les relations causales.

Dans le cadre de la quantification, il peut s'avérer nécessaire de simplifier l'arbre de panne à l'aide d'algèbre booléenne pour représenter les modes de défaillance en double.

Tout en fournissant une estimation de la probabilité de l'événement principal, des coupes minimales, faisant office de vecteurs individuels distincts vers l'événement principal, peuvent être identifiées et leur influence sur l'événement de tête calculée.

Sauf pour les arbres de panne simples, un progiciel est nécessaire pour réaliser correctement les calculs en présence d'événements répétés à plusieurs endroits dans l'arbre de panne, et pour calculer les coupes minimales. Les outils logiciels assurent la cohérence, l'exactitude et la vérifiabilité.

B.14.5 Résultats

Les résultats de l'analyse par arbre de panne sont les suivants:

- une représentation graphique du déroulement de l'événement de tête, illustrant les vecteurs d'interaction par lesquels plusieurs événements simultanés peuvent se produire;
- une liste des coupes minimales (vecteurs individuels vers la défaillance) avec (lorsque les données sont disponibles) la probabilité de survenue de chacune d'elle;
- la probabilité de l'événement de tête.

B.14.6 Avantages et limites

Les avantages de l'analyse par arbre de panne sont les suivants:

- Elle 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 «du haut vers le bas», implicite dans la technique, met l'accent sur les effets de défaillance qui sont en rapport direct avec l'événement de tête.
- L'analyse par arbre de panne est particulièrement utile à l'analyse de systèmes disposant de nombreuses 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. Cette fonction permet d'inclure des relations logiques plus complexes (par exemple ET OU NON EXCLUSIF), mais rend également la vérification de l'arbre de panne plus difficile.
- L'analyse logique des arbres de panne et l'identification des coupes sont utiles pour identifier les vecteurs de défaillance simples d'un système très complexe, dans lequel

des combinaisons particulières d'événements donnant lieu à l'événement de tête peuvent être ignorées.

Les limites sont les suivantes:

- Les incertitudes liées aux probabilités des événements principaux sont prises en compte dans les calculs de la probabilité de l'événement de tête. Ceci peut donner lieu à des niveaux élevés d'incertitude lorsque les probabilités de défaillance de base ne sont pas connues avec exactitude. Cependant, il est possible d'obtenir un degré élevé de confiance pour un système bien compris.
- Dans certains cas, les événements de causalité ne sont pas liés, et il peut s'avérer difficile d'établir que tous les vecteurs importants menant vers l'événement de tête sont inclus. Par exemple, introduire comme événement de tête toutes les sources d'inflammation dans une analyse d'un incendie. Dans ce cas, l'analyse de probabilité est impossible.
- L'arbre de panne est un modèle statique ; les interdépendances temporelles ne sont pas traitées.
- Les arbres de panne ne peuvent traiter que les états binaires (défaillant/non défaillant).
- L'erreur humaine pouvant être intégrée dans un arbre de panne qualitatif, il n'est généralement pas aisé d'inclure les défaillances dont le degré ou la qualité présentent souvent les signes d'une erreur humaine.
- Un arbre de panne ne permet pas d'intégrer aisément les effets domino ou les défaillances conditionnelles.

B.14.7 Documents de référence

CEI 61025, *Analyse par arbre de panne (AAP)*

CEI 60300-3-9, *Gestion de la sûreté de fonctionnement — Partie 3: Guide d'application — Section 9: Analyse du risque des systèmes technologiques*

B.15 Analyse par arbre d'événements (AAE)

B.15.1 Présentation

L'analyse par arbre d'événements est une technique graphique permettant de représenter les séquences d'événements mutuellement exclusifs suivant un événement initiateur en fonction du fonctionnement/non fonctionnement des divers systèmes conçus pour limiter ses conséquences voir la Figure B.3). Elle peut être appliquée de manière qualitative et quantitative.

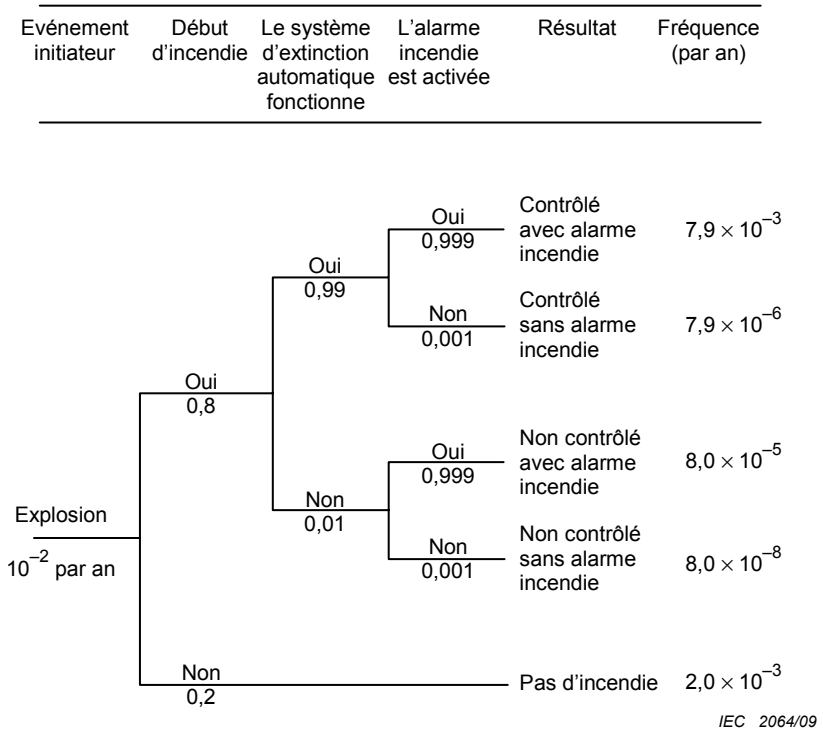

Figure B.3 – Exemple d'arbre d'événements

La Figure B.3 illustre des calculs simples d'un exemple d'arbre d'événements lorsque les nœuds sont totalement indépendants.

En se déployant comme un arbre, l'AAE permet de représenter les événements aggravants ou limiteurs résultant de l'événement initiateur, en tenant compte des systèmes, fonctions ou barrières supplémentaires.

B.15.2 Utilisation

L'AAE peut être utilisée pour modéliser, calculer et classer (du point de vue des risques) différents scénarii d'accidents à la suite d'un événement initiateur.

L'analyse par arbre d'événements peut être utilisée à toutes les étapes du cycle de vie d'un produit ou d'un processus. Elle peut être utilisée de manière qualitative pour faciliter la conception de scénarii potentiels et de séquences d'événements à la suite d'un événement initiateur, et déterminer dans quelle mesure les résultats sont affectés par différents traitements, barrières et contrôles destinés à limiter les résultats indésirables.

L'analyse quantitative se prête à la prise en compte de l'admissibilité des contrôles. Elle permet le plus souvent de modéliser les défaillances, lorsque plusieurs dispositifs de protection sont en place.

L'AAE peut être utilisée pour modéliser les événements initiateurs à l'origine de pertes ou de gains. Toutefois, les circonstances de recherche des vecteurs d'optimisation des gains sont plus souvent modélisées dans un arbre de décision.

B.15.3 Entrées

Les entrées sont les suivantes:

- une liste des événements initiateurs appropriés;

- des informations sur les traitements, les barrières et les contrôles, et leurs probabilités de défaillance (pour des analyses quantitatives);
- une compréhension des processus par lesquels une défaillance initiale s'aggrave.

B.15.4 Processus

Un arbre d'événements débute par la sélection d'un événement initiateur. Il peut s'agir d'un incident (une explosion due à la poussière, par exemple) ou d'un événement de causalité (une coupure d'alimentation, par exemple). Les fonctions ou systèmes en place pour limiter les résultats sont alors indiqués en séquence. Pour chaque fonction ou système, une droite est tracée pour représenter leur succès ou leur défaillance. Une probabilité particulière de défaillance peut être attribuée à chaque droite, cette probabilité conditionnelle étant estimée par l'avis d'un expert ou une analyse par arbre de panne, par exemple. De cette manière, différents vecteurs partant de l'événement initiateur sont modélisés.

Il est à noter que les probabilités de l'arbre d'événements sont conditionnelles, ce qui signifie par exemple que la probabilité de fonctionnement d'une installation fixe d'extinction automatique n'est pas la probabilité obtenue à partir des essais réalisés dans des conditions normales, mais la probabilité de fonctionnement dans des conditions d'incendie dû à l'explosion.

Chaque chemin traversant l'arbre représente la probabilité de survenue de tous les événements dudit chemin. Par conséquent, la fréquence du résultat est représentée par le produit des probabilités conditionnelles individuelles et de la fréquence de l'événement initiateur, étant donné que les différents événements sont indépendants.

B.15.5 Résultats

Les résultats de l'analyse par arbre d'événements sont les suivants:

- descriptions qualitatives des problèmes potentiels par combinaison des événements générant différents types de problèmes (étendue des résultats) issus d'événements initiateurs;
- estimations quantitatives des fréquences ou probabilités d'événement et importance relative des différentes séquences de défaillance et événement contributifs;
- listes des recommandations permettant de réduire les risques;
- évaluations quantitatives de l'efficacité des recommandations.

B.15.6 Avantages et limites

Les avantages de l'analyse par arbre d'événements sont les suivants:

- AAE permet un affichage graphique clair des scénarii potentiels analysés à la suite d'un événement initiateur et de l'impact du succès ou de l'échec des systèmes ou fonctions palliatifs;
- elle représente la durée, la dépendance et les effets domino qui gênent la modélisation des arbres de panne;
- elle représente de manière graphique les séquences d'événements qu'il n'est pas possible de représenter avec les arbres de panne.

Les limites sont les suivantes:

- pour utiliser l'analyse par arbre d'événements dans le cadre d'une évaluation cohérente, il est indispensable d'identifier tous les événements initiateurs potentiels. Ceci peut être réalisé en utilisant une autre méthode d'analyse (HAZOP, APD, par exemple), cependant, cette technique comporte toujours un risque d'omission de certains événements initiateurs importants.

- les arbres d'événements traitent uniquement des états de succès et de défaillance d'un système, et il est difficile d'y intégrer des événements de succès ou de récupération différés;
- tous les vecteurs sont conditionnels pour les événements se produisant sur des nœuds précédents le long du vecteur. La plupart des dépendances le long des vecteurs possibles sont donc résolues. Toutefois, certaines dépendances (les composants communs, les systèmes utilitaires et les opérateurs, par exemple) peuvent être ignorées, donnant lieu à des estimations optimistes du risque si elles ne sont pas correctement traitées.

B.16 Analyse causes-conséquences

B.16.1 Généralités

L'analyse causes-conséquences est une combinaison de l'analyse par arbre de panne et de l'analyse par arbre d'événements. Elle part d'un événement critique et analyse les conséquences en combinant des portes logiques OUI/NON qui représentent des conditions susceptibles de se produire ou des défaillances de systèmes conçus pour limiter les conséquences de l'événement initiateur. Les causes des conditions ou des défaillances sont analysées par des arbres de panne (voir Article B.15).

B.16.2 Utilisation

A l'origine, l'analyse causes-conséquences a été développée comme un outil de fiabilité des systèmes de sécurité critiques afin de mieux comprendre les défaillances des systèmes. Comme l'analyse par arbre de panne, elle permet de représenter la logique de défaillance donnant lieu à un événement critique, mais ajoute à la fonctionnalité d'un arbre de panne en permettant l'analyse des défaillances chronologiques. La méthode permet également d'incorporer des actions différées dans l'analyse des conséquences, cela n'étant pas possible dans les arbres d'événements.

La méthode permet d'analyser les différents chemins dont dispose un système à la suite d'un événement critique en fonction du comportement de sous-systèmes particuliers (les systèmes d'intervention d'urgence, par exemple). S'ils sont quantifiés, ils donnent une estimation de la probabilité des différentes conséquences possibles à la suite d'un événement critique.

Dans la mesure où chaque séquence dans un diagramme causes-conséquences est une combinaison de sous-arbres de panne, l'analyse causes-conséquences peut être utilisée comme un outil pour élaborer des arbres de panne de grande taille.

La génération et l'utilisation des diagrammes sont complexes. Ils ont tendance à être utilisés lorsque l'amplitude des conséquences potentielles de défaillance justifie un effort important.

B.16.3 Entrées

Une bonne compréhension du système, ainsi que de ses modes et scénarii de défaillance, est nécessaire.

B.16.4 Processus

La Figure B.4 illustre un diagramme conceptuel d'une analyse causes-conséquences typique.

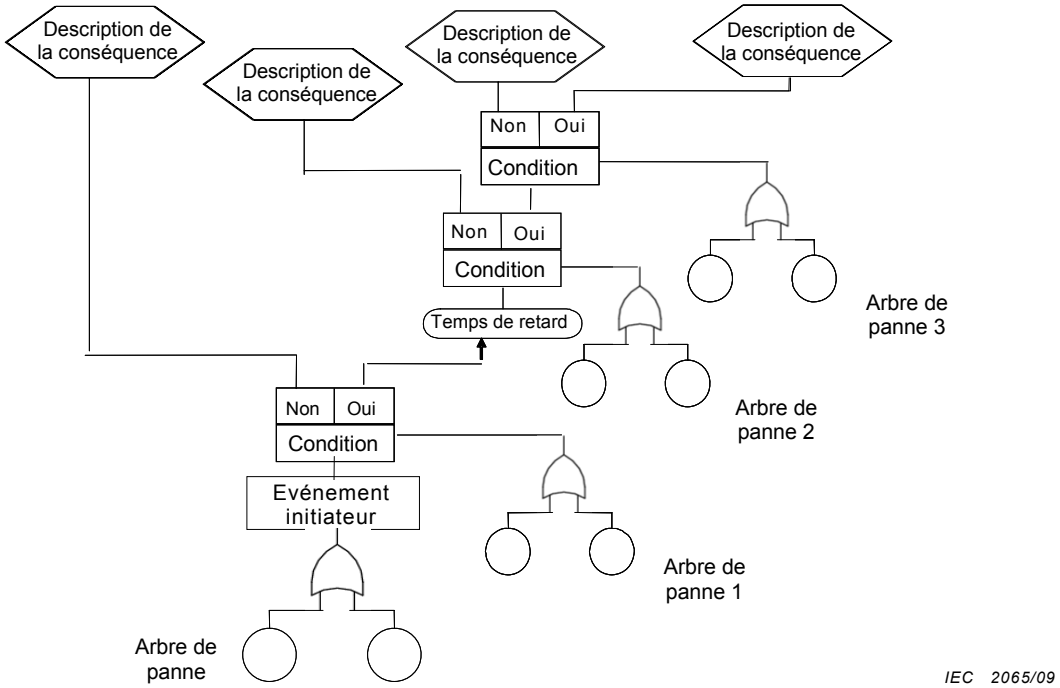

Figure B.4 – Exemple d'analyse des conséquences-cause

La procédure d'élaboration est la suivante:

a) Identification de l'événement critique (ou initiateur) (équivalent à l'événement de tête d'un arbre de panne et à l'événement initiateur d'un arbre d'événements).

b) Développement et validation de l'arbre de panne pour les causes de l'événement initiateur (voir Article B.14) Les mêmes symboles que ceux de l'analyse par arbre de panne conventionnelle sont utilisés.

c) Choix de l'ordre de prise en compte des conditions. Il convient qu'il s'agisse d'une séquence logique (la séquence chronologique dans laquelle elles se déroulent, par exemple).

d) Conception des vecteurs des conséquences en fonction des différentes conditions. Cela ressemble à un arbre d'événements, mais dont les vecteurs sont partagés en cases contenant la condition particulière qui s'applique.

e) La probabilité de chaque conséquence peut être calculée, à condition que les défaillances pour chaque case conditionnelle soient indépendantes. Pour ce faire, il s'agit en premier lieu d'attribuer des probabilités à chaque résultat de la case conditionnelle (en utilisant les arbres de panne correspondants, le cas échéant). La probabilité que l'une des séquences donne lieu à une conséquence particulière est obtenue en multipliant les probabilités de chaque séquence de conditions, dont l'issue est une conséquence particulière. Si plusieurs séquences se terminent par la même conséquence, les probabilités de chaque séquence sont ajoutées. S'il existe des dépendances entre les défaillances des conditions d'une séquence (une coupure d'alimentation pouvant provoquer la défaillance de plusieurs conditions, par exemple), il convient de traiter les dépendances avant de procéder au calcul.

B.16.5 Résultats

Le résultat de l'analyse causes-conséquences donne une représentation graphique du mode de défaillance d'un système, en illustrant les causes et les conséquences. Une estimation de la probabilité d'occurrence de chaque conséquence potentielle, en fonction de l'analyse des probabilités d'occurrence de conditions particulières à la suite d'un événement critique.

B.16.6 Avantages et limites

Une analyse causes-conséquences présente les mêmes avantages qu'une combinaison d'arbres d'événements et d'arbres de panne. En outre, elle pallie certaines limites de ces techniques en permettant d'analyser les événements se développant dans le temps. L'analyse causes-conséquences offre un point de vue cohérent du système.

Elle présente néanmoins l'inconvénient d'être plus complexe que les arbres de panne et les arbres d'événements, en terme de conception et dans la manière de traiter les dépendances lors de la quantification.

B.17 Analyse des causes et de leurs effets

B.17.1 Présentation

L'analyse des causes et de leurs effets est une méthode structurée permettant d'identifier les causes possibles d'un événement indésirable ou d'un problème. Elle organise les facteurs contributifs possibles en catégories générales, de sorte que toutes les hypothèses possibles puissent être considérées. Toutefois, les causes réelles ne sont pas automatiquement pointées étant donné qu'elles peuvent uniquement être déterminées par des preuves réelles et essais empiriques des hypothèses. Les informations sont organisées en diagramme d'Ishikawa ou parfois en arborescence (voir B.17.4).

B.17.2 Utilisation

L'analyse des causes et de leurs effets offre un affichage graphique structuré d'une liste des causes d'un effet particulier. L'effet peut être positif (un objectif) ou négatif (un problème), selon le contexte.

Elle permet de considérer tous les scénarii et causes possibles générés par une équipe d'experts et d'établir un consensus quant à la plupart des causes probables, qui peuvent alors être soumises à essai de manière empirique ou par évaluation des données disponibles. Au début d'une analyse, il peut s'avérer avantageux d'élargir la réflexion sur les causes possibles, puis d'établir les hypothèses potentielles à considérer de manière plus formelle.

Un diagramme des causes et de leurs effets peut être construit pour les raisons suivantes:

- identifier les causes profondes possibles, les raisons fondamentales, pour un effet, un problème ou une condition spécifique;
- trier et relier certaines des interactions parmi les facteurs ayant un effet sur un processus particulier;
- analyser les problèmes existants pour entreprendre des actions correctives.

Les avantages d'un diagramme des causes et de leurs effets comprennent:

- concentrer l'attention des experts sur un problème spécifique;
- faciliter la détermination des causes profondes d'un problème en utilisant une approche structurée;
- encourager la participation du groupe et utiliser les connaissances du groupe pour le produit ou le processus;

- utiliser un format ordonné et facile à lire pour les relations du diagramme cause-effet;
- indiquer les causes possibles de variation dans un processus;
- identifier les domaines dans lesquels il convient de collecter des données pour une étude supplémentaire.

L'analyse des causes et de leurs effets peut être utilisée comme une méthode d'analyse de causes profondes (voir Article B.12).

B.17.3 Entrées

L'entrée d'une analyse des causes et de leurs effets peut être une expertise et une expérience des participants ou un modèle préalablement développé déjà utilisé dans le passé.

B.17.4 Processus

Il convient que l'analyse des causes et de leurs effets soit réalisée par une équipe d'experts connaissant bien le problème à résoudre.

La procédure fondamentale d'une analyse des causes et de leurs effets consiste à:

- définir les effets à analyser et à les placer dans une case. L'effet peut être positif (un objectif) ou négatif (un problème), selon les circonstances;
- déterminer les principales catégories des causes représentées par les cases du diagramme d'Ishikawa. En principe, pour un problème lié à un système, les catégories peuvent être des personnes, des équipements, un environnement, des processus, etc. Toutefois, elles sont choisies en fonction du contexte particulier;
- renseigner les causes possibles pour chaque catégorie principale, avec des nœuds et sous-nœuds pour décrire les relations qu'elles entretiennent;
- se demander «pourquoi » ou «quelle en est la cause?» pour relier les éléments;
- examiner tous les nœuds pour vérifier la cohérence et l'exhaustivité et s'assurer que les causes s'appliquent au principal effet;
- identifier les causes les plus probables en fonction de l'avis de l'équipe et des preuves disponibles.

En général, les résultats s'affichent sous la forme d'un diagramme d'Ishikawa ou d'une arborescence. Le diagramme d'Ishikawa est structuré en plaçant des causes distinctes dans des catégories principales (représentées par les lignes partant de l'épine dorsale) avec des nœuds et sous-nœuds décrivant les causes se trouvant dans ces catégories.

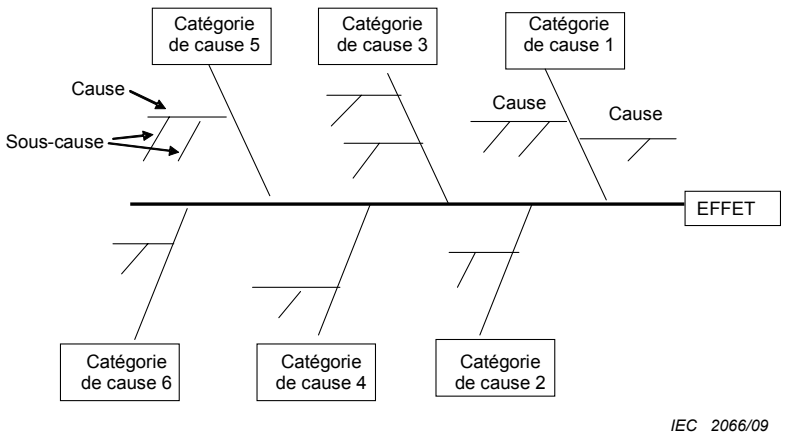

Figure B.5 – Diagramme d'Ishikawa

La représentation en arborescence ressemble à un arbre de panne, bien qu'elle se développe souvent de la gauche vers la droite, et non plus de haut en bas. Toutefois, il n'est pas possible d'évaluer de manière précise la probabilité d'occurrence de l'événement de tête étant donné que les causes sont des facteurs contributifs possibles plutôt que des défaillances dont la probabilité d'occurrence est connue.

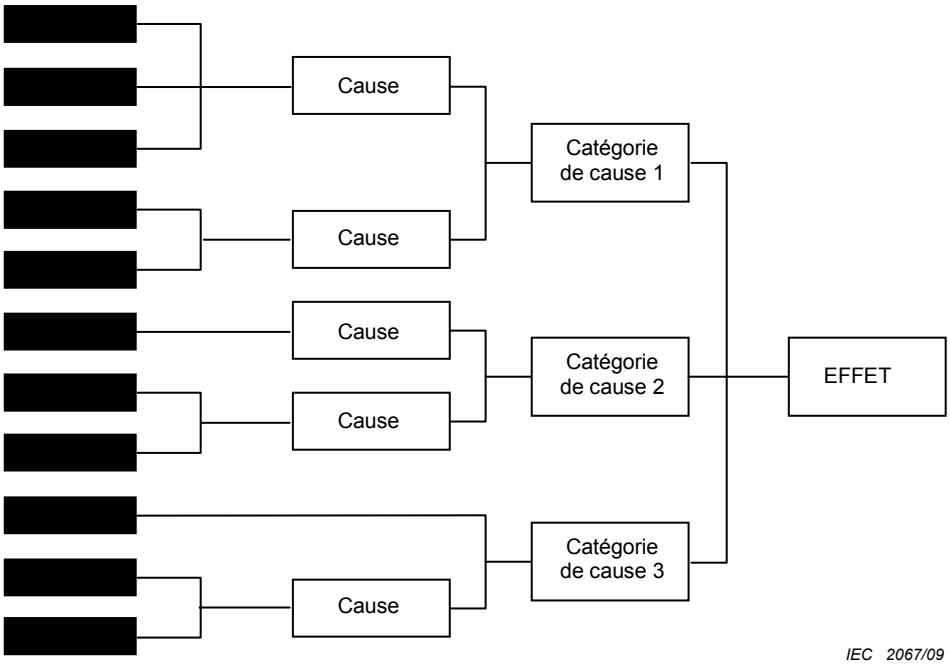

Figure B.6 – Exemple de formulation en arbre de l'analyse des causes et de leurs effets

Les diagrammes des causes et de leurs effets sont en général utilisés de manière qualitative. Il est possible d'évaluer la probabilité d'un problème à 1 et d'attribuer les probabilités aux causes génériques, puis aux sous-causes en fonction du degré de conviction sur leur pertinence. Toutefois, les facteurs contributifs interagissent souvent et participent aux effets de manière complexe, ce qui rend la quantification non valide.

B.17.5 Résultats

Le résultat d'une analyse des causes et de leurs effets est un diagramme d'Ishikawa ou une arborescence illustrant les causes possibles et probables. Il doit être vérifié et faire l'objet d'essais empiriques avant d'énoncer des recommandations.

B.17.6 Avantages et limites

Les avantages sont les suivants:

- implication d'experts concernés travaillant en équipe;
- analyse structurée;
- prise en compte des hypothèses probables;
- illustration graphique des résultats facile à lire;
- identifie les domaines dans lesquels des données supplémentaires sont nécessaires;
- permet d'identifier les facteurs contributifs à l'origine des effets indésirables et souhaités. Mettre l'accent de manière positive sur une question peut encourager une plus grande implication et participation.

Les limites sont les suivantes:

- l'expertise de l'équipe en la matière peut être insuffisante;
- il ne s'agit pas d'un processus complet en lui-même et doit faire partie intégrante d'une analyse de causes profondes pour produire des recommandations;
- il s'agit d'une technique d'affichage des causes du «brainstorming» plutôt que d'une technique d'analyse distincte;
- la classification des facteurs de causalité en catégories principales au début de l'analyse risque de ne pas permettre la prise en compte appropriée des interactions entre chacune d'elles (lorsqu'une erreur humaine est à l'origine de la défaillance d'un appareil ou que des problèmes humains sont le résultat d'une mauvaise conception, par exemple).

B.18 Méthode LOPA

B.18.1 Présentation

La méthode LOPA est une méthode semi-quantitative d'estimation des risques liés à un événement ou scénario indésirable. Elle analyse la suffisance des mesures de contrôle ou de limitation des risques prises.

Une paire cause-conséquence est sélectionnée, puis les niveaux de protection empêchant la cause de donner lieu à la conséquence indésirable sont identifiés. Un ordre de grandeur est calculé pour déterminer si la protection permet de réduire le risque à un niveau tolérable.

B.18.2 Utilisations

La méthode LOPA peut être utilisée de manière qualitative, simplement pour examiner les niveaux de protection entre un danger ou un événement de causalité et un résultat. Elle peut l'être de manière semi-quantitative pour être plus rigoureux dans les processus de dépistage (à la suite de la méthode HAZOP ou APD, par exemple).

La méthode LOPA pose les bases de la spécification des niveaux de protection indépendants (IPL)[8] et des niveaux d'intégrité de sécurité (niveaux SIL) applicables aux systèmes instrumentés, décrits dans la série CEI 61508 et dans la CEI 61511, pour déterminer les exigences en matière de niveau d'intégrité de sécurité (SIL) pour les systèmes instrumentés de sécurité. Elle peut être utilisée pour faciliter l'allocation efficace des ressources de réduction des risques en analysant la réduction des risques induite par chaque niveau de protection.

B.18.3 Entrées

Les entrées de la méthode LOPA sont les suivantes:

- informations fondamentales relatives aux risques, y compris les dangers, leurs causes et leurs conséquences (à la suite d'une analyse APD, par exemple);
- informations relatives aux contrôles en place ou proposés;
- fréquences d'événements de causalité, probabilités de défaillances d'un niveau de protection, mesures des conséquences et définition du risque tolérable;
- fréquences de causes initiatrices, probabilités de défaillances d'un niveau de protection, mesures des conséquences et définition du risque tolérable.

B.18.4 Processus

La méthode LOPA est réalisée par une équipe d'experts qui suivent la procédure suivante:

- les causes initiatrices d'un résultat indésirable sont identifiées et les fréquences et conséquences liées à des données sont recherchées;

---

8 IPL = *Independent Protection Layers*

- une seule paire cause-conséquence est sélectionnée;
- les niveaux de protection empêchant la cause de donner lieu à la conséquence indésirable sont identifiés, puis leur efficacité analysée;
- les IPL sont identifiés (tous les niveaux de protection ne sont pas des IPL);
- la probabilité de défaillance de chaque IPL est estimée;
- la fréquence de la cause initiatrice est combinée aux probabilités de défaillance de chaque IPL et d'éléments de modification conditionnels (un élément de modification conditionnel est, par exemple, si une personne est présente et qu'elle est incluse) pour déterminer la fréquence d'occurrence de la conséquence indésirable. Des ordres de grandeur sont utilisés pour connaître les fréquences et les probabilités;
- le niveau de risque calculé est comparé aux niveaux de tolérance du risque afin de déterminer si une protection supplémentaire est nécessaire.

Un IPL est un système ou une action capable d'empêcher un scénario d'évoluer vers sa conséquence indésirable, quel que soit l'événement de causalité ou le niveau de protection associé au scénario.

Les IPL incluent:

- les fonctions de conception;
- les dispositifs de protection physique;
- les systèmes de verrouillage et d'arrêt;
- les alarmes critiques et l'intervention manuelle;
- la protection physique après l'événement;
- les systèmes d'intervention d'urgence (les modes opératoires et les inspections ne sont pas des IPL).

B.18.5 Résultats

Des recommandations doivent être données pour des contrôles supplémentaires nécessaires et sur l'efficacité de ces contrôles dans la réduction du risque.

La méthode LOPA est l'une des techniques utilisées pour l'évaluation de SIL applicable aux systèmes relatifs à la sécurité/instrumentés.

B.18.6 Avantages et limites

Les avantages sont les suivants:

- elle demande moins de temps et de ressources qu'une analyse par arbre de panne ou une évaluation des risques intégralement quantitative, mais n'en reste pas moins plus rigoureuse que des opinions subjectives qualitatives;
- elle permet d'identifier et de mettre l'accent sur les ressources des niveaux de protection les plus critiques;
- elle permet d'identifier les opérations, les systèmes et les processus dont les dispositifs de protection sont insuffisants;
- elle met l'accent sur les conséquences les plus graves.

Les limites sont les suivantes:

- La méthode LOPA met l'accent sur une paire cause-conséquence et un scénario à la fois. Les interactions complexes entre les risques ou les contrôles ne sont pas couvertes;
- les risques quantifiés peuvent ne pas tenir compte des défaillances de mode commun;

- la méthode LOPA ne s'applique pas à des scénarii très complexes composés de plusieurs paires cause-conséquence ou d'un ensemble de conséquences ayant un impact sur les différents acteurs.

B.18.7 Documents de référence

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

CEI 61511, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

B.19 Analyse par arbre de décision

B.19.1 Présentation

Un arbre de décision représente des alternatives et des résultats de décision de manière séquentielle en tenant compte de résultats incertains. Un arbre de décision ressemble à un arbre d'événements en ce sens qu'il commence par un événement initiateur ou une décision initiale et modélise différents vecteurs et issues résultant des événements ayant pu se produire et des décisions qui peuvent être prises.

B.19.2 Utilisation

Un arbre de décision est utilisé dans la gestion des risques liés à un projet et dans d'autres circonstances afin de mieux orienter les choix d'action en cas d'incertitude. L'affichage graphique permet également de mieux transmettre les raisons justifiant des décisions.

B.19.3 Entrées

Un plan de projet comportant des points de décision. Des informations sur les résultats possibles des décisions et sur les éventuels événements susceptibles d'avoir un effet sur les décisions.

B.19.4 Processus

Un arbre de décision commence par une décision initiale (donner suite au projet A plutôt qu'au projet B, par exemple). A mesure du déroulement des deux projets hypothétiques, des événements se produisent et des décisions prévisibles doivent être prises. Ce processus est représenté dans une arborescence s'apparentant à un arbre d'événements. La probabilité des événements peut être estimée, ainsi que le coût ou l'utilité du résultat final du cheminement.

Logiquement, les informations relatives au meilleur cheminement de décision sont celles qui produisent la valeur probable la plus élevée, calculée comme le produit de toutes les probabilités conditionnelles tout au long du cheminement et de la valeur du résultat.

B.19.5 Résultats

Les résultats comprennent:

- une analyse logique du risque des différentes options qui peuvent être prises;
- un calcul de la valeur prévue pour chaque cheminement possible.

B.19.6 Avantages et limites

Les avantages sont les suivants:

- représentation graphique claire des détails d'un problème relatif à une décision;
- calcul du meilleur cheminement dans une situation.

Les limites sont les suivantes:

- les arbres de décisions de grande taille peuvent se révéler trop complexes et rendre de ce fait difficile la communication avec les autres;
- tendance à simplifier exagérément la situation pour pouvoir la représenter par un diagramme en arborescence.

B.20 Analyse de fiabilité humaine (AFH)

B.20.1 Présentation

L'analyse de fiabilité humaine (AFH) porte sur l'impact des personnes sur les performances du système. Elle peut être utilisée pour évaluer les influences de l'erreur humaine sur le système.

La plupart des processus se caractérisent par des potentiels d'erreur humaine, plus particulièrement lorsque le temps dont dispose l'opérateur pour prendre une décision est court. La probabilité d'évolution d'un problème vers un événement plus sérieux peut être réduite. Toutefois, l'action humaine est parfois le seul rempart contre l'évolution d'une défaillance initiale vers un accident.

L'importance de la méthode AFH a été illustrée par différents accidents au cours desquels des erreurs humaines critiques ont contribué au déclenchement d'une séquence d'événements catastrophique. Ces accidents sont des alertes, mettant en garde contre les évaluations des risques portant uniquement sur les éléments matériels et logiciels d'un système. Ils illustrent les dangers de l'ignorance des possibilités d'erreur humaine. De plus, la méthode AFH est utile pour mettre en évidence les erreurs pouvant entraver la productivité, et pour révéler les moyens dont disposent les opérateurs et le personnel de maintenance pour «réparer» ces erreurs et autres défaillances (matérielles et logicielles).

B.20.2 Utilisation

La méthode AFH peut être utilisée de manière qualitative ou quantitative. Du point de vue qualitatif, elle permet d'identifier le potentiel d'erreur humaine et ses causes, de façon à réduire la probabilité d'erreur. Du point de vue quantitatif, elle permet de fournir des données sur les défaillances humaines dans l'analyse par arbre de panne ou d'autres techniques.

B.20.3 Entrées

Les entrées de la méthode AFH sont les suivantes:

- informations permettant de définir les tâches qu'il convient que les personnes réalisent;
- expérience des types d'erreur se produisant dans la pratique et du potentiel d'erreur;
- compétence en matière d'erreur humaine et sa quantification.

B.20.4 Processus

Le processus AFH est le suivant:

- **Définition du problème**, quels types d'implication humaine doivent être recherchés/évalués ?
- **Analyse des tâches,** comment sera réalisée la tâche et quel type d'aide sera nécessaire pour être performant ?
- **Analyse de l'erreur humaine,** comment la tâche peut-elle échouer: quelles erreurs peuvent être commises et comment peuvent-elle être réparées ?
- **Représentation**, comment intégrer ces erreurs ou défaillances de performances de tâche à d'autres événements matériels, logiciels ou environnementaux afin de calculer les probabilités de défaillance de l'ensemble du système ?

- **Dépistage**, existe-t-il des erreurs ou des tâches ne nécessitant pas de quantification détaillée ?
- **Quantification**, quelle est la probabilité d'erreurs individuelles et de défaillances des tâches ?
- **Evaluation de l'impact**, quelles sont les erreurs ou les tâches les plus importantes (en d'autres termes, quelles sont celles contribuant de manière la plus importante à la fiabilité ou au risque) ?
- **Réduction de l'erreur**, comment obtenir une meilleure fiabilité humaine ?
- **Documentation**, quelles caractéristiques de la méthode AFH doivent être documentées ?

Dans la pratique, le processus AFH se déroule par étape bien que, parfois, des étapes (l'analyse des tâches et l'identification des erreurs, par exemple) s'effectuent en parallèle.

B.20.5 Résultats

Les résultats comprennent:

- une liste d'erreurs susceptibles de se produire et des méthodes permettant de les résoudre (par reprise de la conception du système, de préférence);
- modes d'erreur, causes et conséquences des types d'erreur;
- évaluation qualitative ou quantitative du risque posé par les erreurs.

B.20.6 Avantages et limites

Les avantages de l'analyse de fiabilité humaine sont les suivants:

- elle propose un mécanisme formel permettant d'inclure l'erreur humaine dans la prise en compte des risques liés aux systèmes dans lesquels l'intervention humaine joue un rôle prépondérant;
- la prise en compte formelle des modes d'erreurs humaines et de leurs mécanismes peut permettre de réduire la probabilité de défaillance due à l'erreur.

Les limites sont les suivantes:

- la complexité et la variabilité humaines rendent difficile la définition de modes et probabilités de défaillance simples;
- la plupart des activités humaines ne disposent pas de mode réussite/échec simple. L'analyse de fiabilité humaine traite difficilement des défaillances partielles ou des défaillances liées à la qualité ou aux mauvaises décisions.

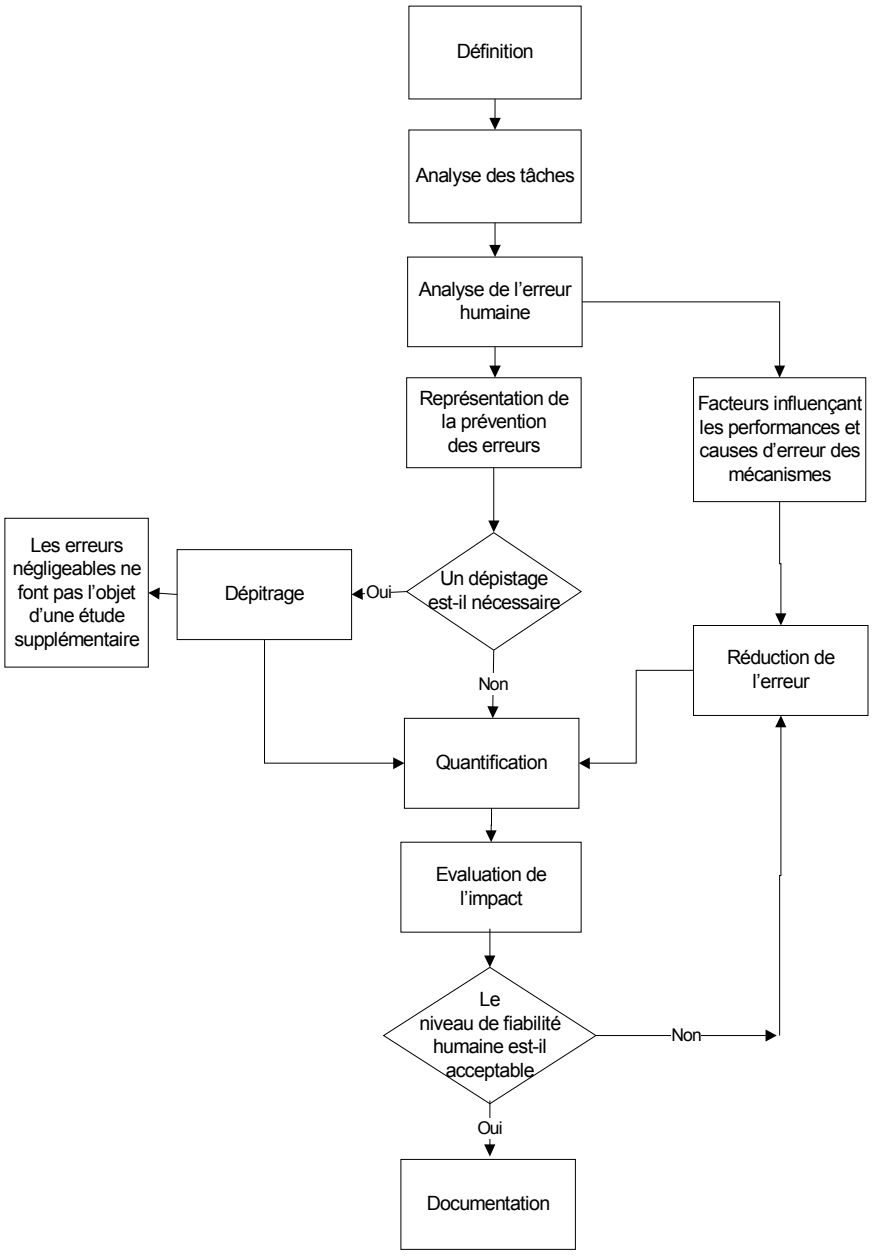

Figure B.7 – Exemple d'évaluation de fiabilité humaine

B.21 Analyse «nœud papillon»

B.21.1 Présentation

L'analyse «nœud papillon» est un moyen schématique simple permettant de décrire et d'analyser les chemins d'un risque en partant des causes jusqu'aux conséquences. Elle peut être considérée comme la combinaison d'un arbre de panne permettant d'analyser la cause d'un événement (représenté graphiquement par le «nœud papillon») et d'un arbre d'événements permettant d'analyser les conséquences. Toutefois, le «nœud papillon» met l'accent sur les barrières qui séparent les causes et le risque, puis le risque et les conséquences. Les diagrammes «nœud papillon» peuvent être conçus à partir d'arbres de panne et d'événement, mais ils sont le plus souvent élaborés directement à la suite d'une session de «brainstorming».

B.21.2 Utilisation

L'analyse «nœud papillon» est utilisée pour représenter un risque possédant un ensemble de causes et de conséquences possibles. L'analyse «nœud papillon» est utilisée lorsque la situation ne garantit pas la complexité d'une analyse par arbre de panne complète ou que l'accent est essentiellement placé sur l'absence absolue de barrière ou de contrôle pour chaque vecteur de défaillance. Elle est utile lorsque les vecteurs menant à la défaillance sont clairs et indépendants.

Un «nœud papillon» est souvent plus facile à comprendre qu'un arbre de panne ou d'événement. De ce fait, il peut s'agir d'un bon outil de communication lorsque l'analyse est faite par des techniques plus complexes.

B.21.3 Entrée

Une bonne compréhension des causes et conséquences d'un risque et des barrières et contrôles qui peuvent l'empêcher, le limiter ou le stimuler est nécessaire.

B.21.4 Processus

La procédure est la suivante:

a) Un risque particulier est identifié pour être analysé, puis représenté comme nœud de contrôle d'un «nœud papillon».

b) Les causes de l'événement sont répertoriées en fonction des sources de risque (ou des dangers dans un contexte de sécurité).

c) Le mécanisme par lequel la source de risque donne lieu à un événement critique est identifié.

d) Des droites relient chaque cause à l'événement, formant la partie gauche du «nœud papillon». Les facteurs susceptibles de donner lieu à intensification peuvent être identifiés et inclus dans le diagramme.

e) Les barrières prévues pour prévenir chaque cause donnant lieu aux conséquences indésirables peuvent être affichées sous la forme de barres verticales coupant la droite. En présence de facteurs susceptibles de provoquer une intensification, des barrières empêchant l'intensification peuvent également être représentées. La démarche peut être utilisée pour les conséquences positives, lorsque les barres reflètent les «contrôles» stimulant la génération de l'événement.

f) Sur le côté droit du «nœud papillon», différentes conséquences potentielles du risque sont identifiées et des droites tracées pour rayonner du risque vers chacune des conséquences potentielles.

g) Les barrières aux conséquences sont dessinées sous forme de barres coupant les lignes radiales. La démarche peut être utilisée pour les conséquences positives, lorsque les barres reflètent les «contrôles» prenant en charge la génération des conséquences.

h) Les fonctions de gestion qui prennent en charge les contrôles (formation et inspection par exemple) peuvent être représentées dans le diagramme «nœud papillon» et reliées au contrôle correspondant.

Certains niveaux de quantification d'un diagramme «nœud papillon» peuvent être possibles, lorsque les vecteurs sont indépendants, où la probabilité d'une conséquence ou d'un résultat particulier est connue et où l'efficacité d'un contrôle peut être chiffrée. Toutefois, dans de nombreux cas, les vecteurs et barrières ne sont pas indépendants, les contrôles pouvant être procéduraux et, par conséquent, l'efficacité assez floue. Souvent la quantification est meilleure à l'aide d'une analyse par arbre de panne et d'une analyse par arbre d'événements.

B.21.5 Résultat

Le résultat est un diagramme simple illustrant les principaux vecteurs de risque et les barrières mises en place pour prévenir ou limiter les conséquences indésirables, ou stimuler et favoriser les conséquences souhaitées.

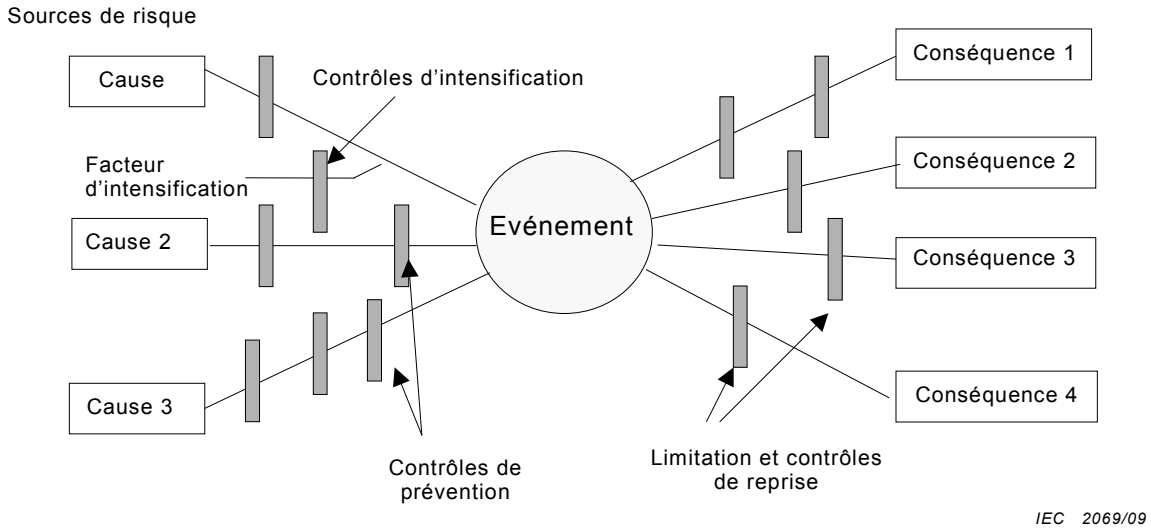

Figure B.8 – Exemple de diagramme «nœud papillon» des conséquences indésirables

B.21.6 Avantages et limites

L'analyse «nœud papillon» présente les avantages suivants:

- elle est simple à comprendre et donne une représentation graphique claire du problème;
- elle concentre l'attention sur les contrôles supposés mis en place pour la prévention et la limitation, et sur leur efficacité;
- elle peut être utilisée pour les conséquences souhaitées;
- son utilisation ne nécessite pas un niveau élevé d'expertise.

Les limites sont les suivantes:

- elle ne peut pas indiquer où plusieurs causes doivent se produire simultanément pour déclencher les conséquences (c'est-à-dire où se trouvent les portes ET dans un arbre de panne décrivant le côté gauche du nœud);
- elle peut simplifier de manière excessive des situations complexes, particulièrement en cas de quantification.

B.22 Maintenance basée sur la fiabilité

B.22.1 Présentation

La maintenance basée sur la fiabilité (MBF) est une méthode permettant d'identifier les règles qu'il convient de mettre en place pour gérer les défaillances et atteindre de manière efficace et efficiente le niveau de sécurité, de disponibilité et d'économie requis du fonctionnement pour tous les types d'équipement.

Aujourd'hui, la MBF est une méthodologie éprouvée, reconnue et utilisée dans de nombreux secteurs.

La MBF fournit un processus de décision permettant d'identifier les exigences de maintenance préventive applicables et efficaces liées aux équipements, en fonction des conséquences sécuritaires, fonctionnelles et économiques des défaillances identifiables, et du mécanisme de dégradation responsable de ces défaillances. Le résultat final du processus est un avis relatif à la nécessité de réaliser une tâche de maintenance ou autre action telle que des modifications fonctionnelles. Les détails relatifs à l'utilisation et à l'application de la MBF sont indiqués dans la CEI 60300-3-11.

B.22.2 Utilisation

Toutes les tâches reposent sur la sécurité des personnes et de l'environnement, et sur les problèmes fonctionnels et économiques. Toutefois, il convient de noter que les critères pris en compte dépendent de la nature du produit et de son application. Par exemple, un processus de production doit être viable du point de vue économique en pouvant être sensible aux questions strictes liées à l'environnement, alors qu'il convient qu'un matériel de défense soit opérationnel, tout en pouvant faire l'objet de critères moins rigoureux en matière de sécurité, d'économie et d'environnement. Il peut s'avérer plus profitable de cibler l'analyse sur les défaillances dont les effets sur la sécurité, l'environnement et l'économie seraient graves.

La MBF permet de garantir la maintenabilité et s'applique généralement lors des phases de conception et de développement, puis est mise en place lors du fonctionnement et de la maintenance.

B.22.3 Entrées

La réussite de l'application de la MBF nécessite une bonne compréhension des équipements et de la structure, de l'environnement d'exploitation et des systèmes, des sous-systèmes et éléments de l'équipement associés, ainsi que des défaillances possibles et leurs conséquences.

B.22.4 Processus

La procédure de base d'un programme MBF est la suivante:

- initiation et planification;
- analyse de défaillance fonctionnelle;
- sélection de tâche;
- mise en œuvre;
- amélioration continue.

La MBF repose sur les risques puisqu'elle suit la procédure de base en matière d'évaluation des risques. Le type d'évaluation des risques s'apparente à la méthode AMDEC (analyse des modes de défaillance, de leurs effets et de la criticité), mais nécessite une approche d'analyse particulière lorsqu'elle est utilisée dans ce contexte.

L'identification des risques met l'accent sur les situations dans lesquelles la fréquence et/ou les conséquences des défaillances potentielles peuvent être supprimées ou réduites en effectuant des tâches de maintenance. Il s'agit d'identifier les fonctions et normes de performances requises ainsi que les défaillances des équipements et des composants susceptibles de compromettre ces fonctions.

L'analyse des risques est composée d'une estimation de la fréquence de chaque défaillance ne faisant pas l'objet de procédure de maintenance. Les conséquences sont établies en définissant les effets de la défaillance. Une matrice de risque combinant la fréquence de la défaillance et les conséquences permet d'établir des catégories de niveau de risque.

Les risques sont alors évalués en sélectionnant la règle appropriée de gestion des défaillances pour chaque mode de défaillance.

L'ensemble du processus MBF est abondamment documenté pour référence et examen ultérieurs. La collecte de données liées à la défaillance et à la maintenance permet de contrôler les résultats et la mise en œuvre des améliorations.

B.22.5 Résultats

La MBF fournit une définition des tâches de maintenance (contrôle de fonctionnement, restauration planifiée, remplacement planifié, recherche de défaillance ou maintenance non préventive, par exemple). D'autres actions possibles pouvant découler de l'analyse sont la reprise de conception, la modification des procédures d'exploitation ou de maintenance ou une formation supplémentaire, par exemple. Les intervalles entre les tâches, ainsi que les ressources requises, sont alors identifiés.

B.22.6 Documents de référence

CEI 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11 : Guide d'application – Maintenance basée sur la fiabiltié*

B.23 Analyse transitoire (AT) et l'analyse de conditions insidieuses (ACI)

B.23.1 Présentation

L'analyse transitoire (AT) est une méthodologie permettant d'identifier les erreurs de conception. Une condition insidieuse est une condition matérielle, logicielle ou intégrée latente pouvant être à l'origine d'un événement indésirable ou pouvant gêner l'occurrence d'un événement souhaité; cette condition n'étant pas provoquée par la défaillance d'un composant. Ces conditions se caractérisent par leur nature aléatoire et leur aptitude à échapper à toute forme de détection lors d'essais normalisés les plus rigoureux du système. Les conditions insidieuses peuvent être à l'origine d'opération inappropriée, de la perte de disponibilité du système, de retards de programmation, voire de mort ou de blessure.

B.23.2 Utilisation

L'analyse de conditions insidieuses (ACI) a été développée à la fin des années 1960 pour permettre à la NASA de vérifier l'intégrité et la fonctionnalité de ses systèmes. L'analyse de conditions insidieuses était un outil utile pour rechercher les parcours de circuit électrique involontaires et a pris part à la conception de solutions visant à isoler chaque fonction. Toutefois, à mesure des avancées technologiques, les outils d'analyse de conditions insidieuses ont également dû évoluer. L'analyse transitoire comprend et dépasse le domaine d'application de l'analyse de conditions insidieuses. Elle peut détecter les problèmes matériels et logiciels grâce aux technologies. Les outils d'analyse transitoire peuvent intégrer plusieurs analyses (les arbres de panne, l'analyse des modes de défaillance et de leurs effets (AMDE), la fiabilité, par exemple) en une seule analyse, ce qui permet de gagner du temps et de réduire les frais liés au projet.

B.23.3 Entrées

L'analyse transitoire est un outil unique du processus de conception en ce qu'elle utilise différents outils (réseau arborescent, forêts et indices pour aider l'analyste à identifier les conditions insidieuses) pour rechercher un type de problème particulier. Les réseaux arborescents et forêts sont des regroupements topologiques du système réel. Chaque réseau représente une sous-fonction et illustre toutes les entrées susceptibles d'avoir un impact sur le résultat de la sous-fonction. Les forêts sont conçues en combinant les réseaux arborescents contribuant à la sortie d'un système particulier. Une forêt bien conçue présente la sortie d'un système en termes de toutes ses entrées connexes. Elles deviennent, avec d'autres, l'entrée de l'analyse.

B.23.4 Processus

La procédure fondamentale d'une analyse transitoire consiste à:

- préparer les données;
- construire le réseau arborescent;
- évaluer les chemins de réseau;
- produire des recommandations finales et un rapport.

B.23.5 Résultats

Une condition insidieuse est un chemin imprévu ou un flux logique au sein d'un système qui, dans certaines conditions, peut être à l'origine d'une fonction indésirable ou gêner une fonction souhaitée. Le chemin peut être composé de matériels, de logiciels ou d'actions de l'opérateur, ou d'une combinaison de ces éléments. Les conditions insidieuses ne sont pas le résultat d'une défaillance matérielle. Il s'agit de conditions latentes, conçues de manière involontaire dans le système, codées dans le programme logiciel ou déclenchées à la suite d'une erreur humaine. Les quatre catégories de conditions insidieuses sont les suivantes:

a) chemins insidieux : chemins imprévus le long desquels le courant, l'énergie ou la séquence logique s'écoule dans une direction inattendue;
b) temporisation insidieuse. événements se produisant dans une séquence inattendue ou incompatible;
c) indications insidieuses : affichages ambigus ou erronés des conditions de fonctionnement d'un système susceptibles d'impliquer une action indésirable du système ou d'un opérateur;
d) marquage insidieux : marquage incorrect ou imprécis des fonctions du système (entrées, contrôles, bus d'affichage du système, par exemple) susceptible de pousser l'opérateur à stimuler le système de manière incorrecte.

B.23.6 Avantages et limites

Les avantages sont les suivants:

- l'analyse transitoire est un bon moyen d'identification des erreurs de conception;
- elle fonctionne mieux lorsqu'elle est appliquée conjointement avec la méthode HAZOP;
- c'est un excellent moyen de traiter les systèmes comportant plusieurs états (atelier de composition et semi-continu, par exemple).

Les limites peuvent être les suivantes:

- le processus est quelque peu différent selon qu'il est appliqué aux circuits électriques, aux usines de processus, aux équipements mécaniques ou aux logiciels;
- la méthode dépend de la bonne conception des réseaux arborescents.

B.24 Analyse de Markov

B.24.1 Présentation

L'analyse de Markov est utilisée lorsque l'état futur d'un système dépend uniquement de son état présent. Elle est en général utilisée pour analyser les systèmes réparables comportant plusieurs états, une analyse par bloc de fiabilité étant inappropriée à l'analyse pertinente du système. La méthode peut être étendue à des systèmes plus complexes grâce à des chaînes de Markov d'ordre supérieur et est uniquement limitée par le modèle, les calculs mathématiques et les hypothèses.

Le processus d'analyse de Markov est une technique quantitative qui peut être discrète (utilisant des probabilités de passage d'un état à l'autre) ou continue (utilisant les vitesses de passage d'un état à l'autre).

Alors qu'une analyse de Markov peut être réalisée manuellement, la nature des techniques se prête à l'utilisation de programmes informatiques, dont la plupart est disponible dans le commerce.

B.24.2 Utilisation

La technique d'analyse de Markov peut être utilisée sur différentes structures de système, avec ou sans réparation, notamment:

- les composants indépendants en parallèle;
- les composants indépendants en série;
- les systèmes de partage de charge;
- les systèmes autonomes, y compris les cas dans lesquels une défaillance de communication peut se produire;
- les systèmes dégradés.

La technique d'analyse de Markov peut également permettre de calculer la disponibilité, notamment en tenant compte des composants de rechange destinés à la réparation.

B.24.3 Entrées

Les entrées essentielles à une analyse de Markov sont les suivantes:

- liste de différents états dans lesquels peut se trouver le système, le sous-système ou le composant (complètement opérationnel, partiellement opérationnel (c'est-à-dire à l'état dégradé), état défaillant, par exemple);
- une bonne compréhension des transitions possibles dont la modélisation est nécessaire. Par exemple, la dégradation d'un pneu de voiture doit tenir compte de l'état de la roue de secours, et donc de la fréquence d'inspection;
- la vitesse de passage d'un état à l'autre est en général représentée par une probabilité de changement d'état pour les événements discrets, ou par le taux de défaillance (λ) et/ou la fréquence de réparation (μ) pour les événements continus.

B.24.4 Processus

La technique d'analyse de Markov tourne autour du concept «d'état» (disponible et en panne, par exemple), le passage entre chacun d'eux dans le temps reposant sur une probabilité constante de modification. Une matrice de probabilité de transition stochastique permet de décrire la transition entre chacun de ces états afin de calculer les différents résultats.

Pour illustrer la technique d'analyse de Markov, soit un système complexe ne pouvant faire l'objet que de trois états: fonctionnement, dégradé et en panne, chacun d'eux étant respectivement défini comme les états S1, S2 et S3. Chaque jour, le système évolue dans l'un de ces trois états. Le Tableau B.3 illustre la probabilité de trouver demain le système à l'état S*i*, où *i* peut être 1, 2 ou 3.

Tableau B.2 — Matrice de Markov

		Etat aujourd'hui		
		S1	S2	S3
Etat demain	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

Ce tableau des probabilités est appelé matrice de Markov, ou matrice de transition. Noter que la somme de chaque colonne est 1, étant donné qu'il s'agit de la somme de tous les résultats possibles dans chaque cas. Le système peut également être représenté par un diagramme de Markov, dans lequel les cercles et les flèches représentent respectivement les états et la transition avec la probabilité qui l'accompagne.

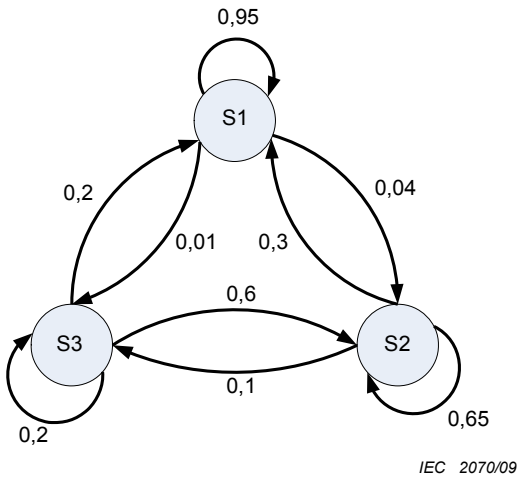

Figure B.9 – Exemple de diagramme de Markov du système

En règle générale, les flèches partant d'un état vers lui-même ne sont pas affichées, mais elles le sont dans ces exemples, par souci d'exhaustivité.

Soit P*i*, représentant la probabilité de trouver le système à l'état *i* pour *i* = 1, 2, 3, les équations simultanées à résoudre étant:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B.3)}$$

Ces trois équations ne sont pas indépendantes et ne résoudront pas les trois inconnues. Il convient d'utiliser l'équation suivante, et d'éliminer l'une des équations ci-dessous.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

La solution est 0,85, 0,13 et 0,02 pour les états respectifs 1, 2, 3. Le système fonctionne complètement pendant 85 % du temps, à l'état dégradé pendant 13 % du temps et est en panne pendant 2 % du temps.

Pour les événements continus, soit deux éléments fonctionnant en parallèle devant être opérationnels pour que le système fonctionne. Les éléments peuvent être opérationnels ou en panne, et la disponibilité du système dépend de l'état des éléments.

Les états peuvent être les suivants:

Etat 1 Les deux éléments fonctionnent correctement;

Etat 2 Un élément est tombé en panne et est en cours de réparation. L'autre élément fonctionne;

Etat 3 Les deux éléments sont tombés en panne et un 'élément est en cours de réparation.

Si le taux de défaillance continu de chaque élément est λ et que la fréquence de réparation est μ, le diagramme de transition d'état est donc:

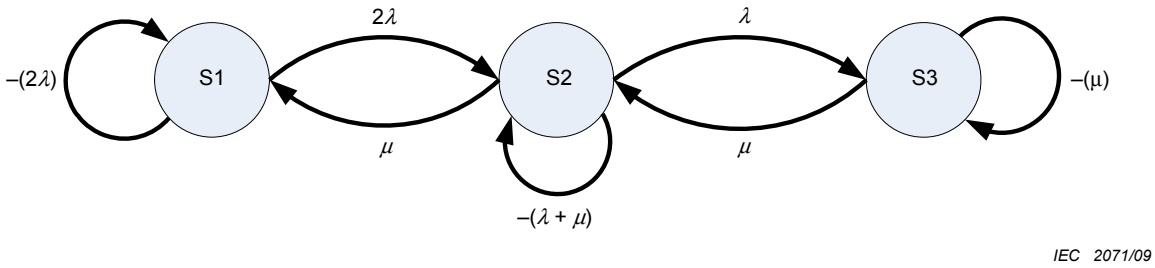

Figure B.10 – Exemple de diagramme de transition d'état

Noter que la transition de l'état 1 à l'état 2 est 2λ, étant donné que la défaillance de l'un ou l'autre des éléments fera passer le système à l'état 2.

Soit Pi(t), la probabilité d'être à l'état i à l'instant t, et

Soit Pi(t + δt), la probabilité d'être à l'état final à l'instant t + δt

La matrice de probabilité de transition devient:

Tableau B.3 – Matrice de Markov finale

		Etat initial		
		P1(t)	P2(t)	P3(t)
	P1(t + δt)	–2λ	μ	0
Etat final	P2(t + δt)	2λ	– (λ + μ)	μ
	P3(t + δt)	0	λ	– μ

Il convient de noter que les valeurs nulles sont probables, puisqu'il est impossible de passer de l'état 1 à l'état 3 ou inversement. De même, la somme des colonnes donne zéro lors de la spécification des taux.

Les équations simultanées deviennent:

$$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda\, P1(t) + -(\lambda + \mu)\, P2(t) + \mu\, P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda\, P2(t) + -\mu\, P3(t) \quad \text{(B.7)}$$

Pour plus de simplicité, la disponibilité requise est supposée être celle à l'état stable.

Si δt tend vers l'infini, dP_i/dt tend vers zéro, et les équations deviennent plus faciles à résoudre. Il convient également d'utiliser l'équation supplémentaire indiquée dans l'Équation (B.4) citée précédemment:

A présent, l'Équation $A(t) = P1(t) + P2(t)$ peut être exprimée sous la forme:

$A = P1 + P2$

De ce fait $A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Résultats

Le résultat d'une analyse de Markov est l'ensemble des différentes probabilités qu'un système se trouve dans différents états. Il s'agit donc d'une estimation des probabilités de défaillance et/ou disponibilité, l'un des composants essentiels d'un système.

B.24.6 Avantages et limites

L'analyse de Markov présente les avantages suivants:

- possibilité de calculer les probabilités pour des systèmes offrant des capacités de réparation et plusieurs états dégradés.

L'analyse de Markov présente les limites suivantes:

- hypothèse de probabilités constantes de modification de l'état: panne ou réparations;
- du point de vue statistique, tous les événements sont indépendants étant donné que les états à venir sont indépendants de tous les états passés, sauf pour l'état immédiatement antérieur;
- nécessite une bonne connaissance de toutes les probabilités de changement d'état;
- bonne connaissance des opérations matricielles;
- les résultats sont difficiles à communiquer au personnel non technique.

B.24.7 Comparaisons

L'analyse de Markov s'apparente à une analyse du réseau de Petri puisqu'elle permet de contrôler et d'observer les états du système. Elle présente tout de même quelques différences, étant donné que le réseau de Petri peut exister à plusieurs états en même temps.

B.24.8 Documents de référence

CEI 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

CEI 61165, *Application des techniques de Markov*

ISO/IEC 15909 (all parts)*, Software and systems engineering - High-level Petri nets*
(disponible uniquement en anglais)

B.25 Simulation de Monte-Carlo

B.25.1 Présentation

La plupart des systèmes sont trop complexes pour que l'on puisse modéliser les effets de l'incertitude, dont ils font l'objet, à l'aide de techniques analytiques. Cependant, ils peuvent

être évalués en considérant les entrées comme des variables aléatoires et en procédant à un certain nombre N de calculs (appelés simulations) dans lesquels les entrées sont échantillonnées pour obtenir N résultats possibles du résultat souhaité.

Cette méthode peut résoudre des situations complexes qu'il serait difficile de comprendre et de résoudre par une méthode analytique. Les systèmes peuvent être développés à l'aide d'une feuille de calcul et d'autres outils conventionnels, mais des outils plus sophistiqués sont disponibles pour répondre aux exigences plus complexes, la plupart d'entre eux étant aujourd'hui peu onéreux. Lorsque la technique a été développée, le nombre d'itérations requises pour les simulations de Monte-Carlo ralentissait le processus et prenait beaucoup de temps; pourtant, les avancées informatiques et les développements théoriques (l'échantillonnage par hypercube latin, par exemple) ont considérablement réduit la durée de traitement pour la plupart des applications.

B.25.2 Utilisation

La simulation de Monte-Carlo offre un moyen d'évaluer les effets de l'incertitude sur les systèmes dans un large éventail de situations. D'une manière générale, elle est utilisée pour évaluer l'étendue des résultats possibles et la fréquence relative des valeurs dans cette étendue pour les mesures quantitatives d'un système (le coût, la durée, le débit, la demande et autres mesures analogues, par exemple). La simulation de Monte-Carlo peut être utilisée à deux fins différentes:

- projection de l'incertitude sur des modèles d'analyse conventionnels;
- calculs probabilistes lorsque des techniques d'analyse ne s'appliquent pas.

B.25.3 Entrées

Une bonne compréhension du système et des informations sur les types d'entrée, les sources d'incertitude à représenter et le résultat requis sont nécessaires. Les données d'entrée liées à l'incertitude sont représentées comme des variables aléatoires dont les distributions sont plus ou moins réparties selon le niveau des incertitudes. Des distributions uniforme, triangulaire, normale et log-normale sont souvent utilisées à cette fin.

B.25.4 Processus

Le processus est le suivant:

a) Un modèle ou algorithme est défini pour représenter, le plus étroitement possible, le comportement du système étudié.

b) Le modèle est appliqué plusieurs fois en utilisant des nombres aléatoires pour générer des résultats du modèle (simulations du système). Lorsque l'application consiste à modéliser les effets de l'incertitude, le modèle se présente sous la forme d'une équation qui fournit la relation entre des paramètres d'entrée et un résultat en sortie. Les valeurs sélectionnées pour les entrées sont issues de distribution de probabilité appropriées qui représentent la nature de l'incertitude pour ces paramètres.

c) Dans tous les cas, un calculateur applique le modèle plusieurs fois (le plus souvent jusqu'à 10 000 fois) avec différentes entrées et génère plusieurs résultats en sortie. Ces résultats peuvent être traités au moyen de statistiques conventionnelles pour fournir des informations (valeurs moyennes, écarts types, intervalles de confiance, par exemple).

Un exemple de simulation est donné ci-dessous.

Considérer le cas de deux éléments fonctionnant en parallèle, un seul étant obligatoire pour que le système fonctionne. La fiabilité du premier élément s'élève à 0,9 et celle du deuxième élément à 0,8.

Il est possible de concevoir une feuille de calcul contenant les colonnes ci-dessous.

Tableau B.4 – Exemple de simulation de Monte-Carlo

	Elément 1		Elément 2		
Numéro de simulation	Numéro aléatoire	Fonctions?	Numéro aléatoire	Fonctions?	Système
1	0,577 243	OUI	0,059 355	OUI	1
2	0,746 909	OUI	0,311 324	OUI	1
3	0,541 728	OUI	0,919 765	NON	1
4	0,423 274	OUI	0,643 514	OUI	1
5	0,917 776	NON	0,539 349	OUI	1
6	0,994 043	NON	0,972 506	NON	0
7	0,082 574	OUI	0,950 241	NON	1
8	0,661 418	OUI	0,919 868	NON	1
9	0,213 376	OUI	0,367 555	OUI	1
10	0,565 657	OUI	0,119 215	OUI	1

Le générateur aléatoire crée un nombre compris entre 0 et 1 qui est comparé à la probabilité de chaque élément afin de déterminer si le système est opérationnel. Avec simplement 10 calculs, il convient de ne pas s'attendre à ce que le résultat de 0,9 soit précis. La démarche habituelle consiste à concevoir un calculateur afin de comparer le résultat total à mesure de l'avancée de la simulation, et d'obtenir le niveau de précision requis. Dans cet exemple, le résultat 0,979 9 a été obtenu après 20 000 itérations.

Le modèle ci-dessus peut être étendu de plusieurs façons. Par exemple:

- en étendant le modèle lui-même (en considérant, par exemple, que le deuxième élément devient opérationnel uniquement lorsque le premier tombe en panne);
- en transformant la probabilité fixe en probabilité variable (la distribution triangulaire en est un bon exemple) lorsqu'elle ne peut pas être définie de manière précise;
- en utilisant des taux de défaillance combinés au calculateur aléatoire pour déduire un temps de défaillance (distribution exponentielle, Weibull ou autre) et prévoir des temps de réparation.

Les applications incluent, entre autres, l'évaluation de l'incertitude des prévisions financières, des résultats en matière d'investissement, des prévisions liées au coût et à la planification du projet, des interruptions du processus métier et des exigences liées au recrutement.

Les techniques analytiques ne sont pas en mesure de fournir des résultats pertinents lorsqu'il existe une incertitude dans les données d'entrée, et de ce fait dans les résultats.

B.25.5 Résultats

Il peut s'agir d'une seule valeur, telle que déterminée dans l'exemple ci-dessus, d'un résultat exprimé sous la forme d'une distribution des probabilités ou des fréquences, ou de l'identification des principales fonctions du modèle dont l'impact sur le résultat est le plus important.

D'une manière générale, une simulation de Monte-Carlo est utilisée pour évaluer l'ensemble de la distribution des résultats ou les mesures-clés issues d'une distribution, comme:

- la probabilité d'un résultat défini;
- la valeur d'un résultat dans laquelle les personnes concernées par le problème ont un certain niveau de confiance ne sera pas dépassée, un coût inférieur à 10 % de chance de dépasser ou une durée à 80 % certaine d'être dépassée.

Une analyse des relations qu'entretiennent les entrées et les résultats peut éclairer la signification relative des facteurs en cours et identifier les cibles utiles pouvant influencer l'incertitude du résultat.

B.25.6 Avantages et limites

L'analyse de Monte-Carlo présente les avantages suivants:

- en principe, la méthode peut concilier toutes les distributions dans une variable d'entrée, y compris les distributions empiriques déduites des observations de systèmes connexes;
- les modèles sont relativement simples à développer et peuvent être étendus à mesure de l'évolution des besoins;
- toutes les influences ou relations se produisant dans la réalité peuvent être représentées, y compris les effets subtils tels que les dépendances conditionnelles;
- l'analyse de sensibilité peut être appliquée pour distinguer les influences importantes de celles qui le sont moins;
- les modèles sont aisément compréhensibles étant donné que la relation entre les entrées et les résultats est transparente;
- des modèles de comportement efficaces tels que les réseaux de Petri (future CEI 62551) sont disponibles et se révèlent très efficaces pour la simulation de Monte-Carlo;
- elle fournit une mesure de l'exactitude d'un résultat;
- le logiciel est disponible et relativement peu onéreux.

Les limites sont les suivantes:

- l'exactitude des solutions dépend du nombre de simulations qu'il est possible de réaliser (cette limite est réduite grâce à l'amélioration des vitesses de calcul informatique);
- elle repose sur l'aptitude à représenter les incertitudes liées aux paramètres par une distribution valide;
- des modèles volumineux et complexes peuvent faire concurrence au programme de modélisation et rendre le début du processus difficile pour les différents acteurs;
- la technique peut ne pas distinguer correctement les conséquences élevées des événements peu probables et, par conséquent, ne pas permettre de refléter dans l'analyse la sensibilisation au risque d'une organisation.

B.25.7 Documents de référence

CEI 61649, *Analyse de Weibull*

CEI 62551, *Techniques d'analyse pour la sûreté de fonctionnement – Modélisation par réseau de Petri*[9]

Guide ISO/CEI 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*
(disponible uniquement en anglais)

B.26 Statistique bayésienne et réseaux de Bayes

B.26.1 Présentation

La statistique bayésienne est attribuée au Révérend Thomas Bayes. Elle part du postulat que toute information déjà connue (l'a priori) peut être combinée à une mesure subséquente (l'a

9 Actuellement à l'étude.

posteriori) afin d'établir une probabilité globale. L'expression générale du théorème de Bayes peut être la suivante:

$$P(A \mid B) = \{P(A)P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

où

la probabilité de X est indiquée par P(X);

la probabilité de X à condition que Y se soit produit est indiquée par P(X|Y); et

E_i est le nième événement.

Sa forme la plus simple est réduite à P(A|B) = {P(A)P(B|A)} / P(B).

Les statistiques bayésiennes se distinguent des statistiques classiques en ce sens qu'elles ne supposent pas que tous les paramètres de distribution sont fixes, mais qu'il s'agit de variables aléatoires. Une probabilité bayésienne peut être mieux appréhendée si elle est considérée comme le degré de croyance d'une personne en un certain événement, par opposition à la théorie classique reposant sur la preuve physique. Etant donné que la démarche bayésienne repose sur l'interprétation subjective de la probabilité, elle offre une base directe de prise de décision et de développement de réseaux de Bayes (ou réseaux de croyance, réseaux bayésiens).

Les réseaux de Bayes utilisent un modèle graphique pour représenter un ensemble de variables et leurs relations probabilistes. Le réseau est composé de nœuds représentant une variable aléatoire et de flèches reliant un nœud parent à un nœud enfant (où un nœud parent est une variable qui a un effet direct sur une autre variable (enfant)).

B.26.2 Utilisation

Ces dernières années, l'utilisation de la théorie et des réseaux de Bayes s'est largement répandue en partie en raison de leur intérêt intuitif et de la disponibilité des outils de calcul logiciels. Les réseaux de Bayes ont été utilisés dans un large éventail de domaines: le diagnostic médical, la modélisation d'image, la génétique, la reconnaissance vocale, l'économie, l'exploration spatiale et dans les puissants moteurs de recherche sur le Web utilisés de nos jours. Ils sont valables dans tous les domaines impliquant la recherche de variables inconnues par l'utilisation de relations et de données structurelles. Les réseaux de Bayes permettent d'apprendre les relations de causalité pour appréhender un domaine problématique et prévoir les conséquences de l'intervention.

B.26.3 Entrées

Les entrées sont analogues à celles d'un modèle de Monte-Carlo. Dans le cas d'un réseau de Bayes, voici quelques exemples de procédure à suivre:

- définition des variables système;
- définition des liens de causalité entre des variables;
- spécification des probabilités conditionnelles ou a priori;
- ajout d'une preuve au réseau;
- mise à jour de croyances;
- extraction de croyances a posteriori.

B.26.4 Processus

La théorie de Bayes peut s'appliquer dans un large éventail de manières. Cet exemple concerne la création d'un tableau de Bayes dans lequel un contrôle médical permet de déterminer si le patient est malade. Avant le contrôle, la croyance est que 99 % de la

population ne porte pas cette maladie, contre 1 % qui la porte (c'est-à-dire l'information a priori). L'exactitude du contrôle a démontré que si la personne porte la maladie, le résultat du contrôle est positif dans 98 % des cas. De même, il existe une probabilité selon laquelle, si vous ne portez pas la maladie, le résultat du contrôle est positif dans 10 % des cas. Le tableau de Bayes contient les informations suivantes:

Tableau B.5 – Données du tableau de Bayes

	PRÉCÉDENT	PROBABILITÉ	PRODUIT	POSTERIEUR
Porte la maladie	0,01	0,98	0,009 8	0,090 1
Ne porte pas la maladie	0,99	0,10	0,099 0	0,909 9
SOMME	1		0,108 8	1

Grâce à la loi de Bayes, le produit est déterminé en combinant l'a priori et la probabilité. L'a posteriori est déterminé en divisant la valeur du produit par le total du produit. Le résultat montre qu'un contrôle positif indique que l'a priori est passé de 1 % à 9 %. Plus important, il existe une forte chance que, même si le contrôle est positif, la maladie soit peu probable. L'examen de l'équation $(0,01\times0,98)/((0,01\times0,98)+(0,99\times0,1))$ montre que la valeur 'pas de résultat positif de maladie' joue un rôle majeur dans les valeurs a posteriori.

Soit le réseau de Bayes suivant:

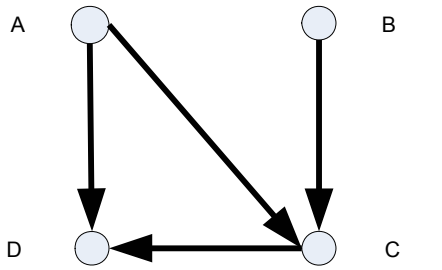

Figure B.11 – Exemple de réseau de Bayes

Avec les probabilités conditionnelles a priori définies dans les tableaux suivants et à l'aide de la notation que Y indique les éléments positifs et N les éléments négatifs, l'élément positif peut être «porte la maladie» (voir ci-dessus) ou Elevé, et N pourrait être Faible.

Tableau B.6 – Probabilités a priori pour les nœuds A et B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Tableau B.7 – Probabilités conditionnelles pour le nœud C, les nœuds A et B étant définis

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8
N	*N*	0,7	0,3

Tableau B.8 – Probabilités conditionnelles pour le nœud D, les nœuds A et C étant définis

A	*C*	P(*D* = *Y*)	P(*D* = *N*)
Y	*Y*	0,6	0,4
Y	*N*	1,0	0,0
N	*Y*	0,2	0,8
N	*N*	0,6	0,4

Pour déterminer la probabilité postérieure de P(*A*|*D*=*N*,*C*=*Y*), il est nécessaire de calculer en premier lieu P(*A*,B|*D*=*N,C*=*Y*).

Grâce à la loi de Bayes, la valeur P(*D*|*A,C*)P(*C*|*A,B*)P(*A)*P*(B*) est déterminée de la manière indiquée ci-dessous, la dernière colonne montrant les probabilités normalisées dont la somme est 1, à la suite de la déduction de l'exemple précédent (résultat arrondi).

Tableau B.9 – Probabilité postérieure pour les nœuds A et B, les nœuds D et C étant définis

A	*B*	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A,B*|*D*=*N,C*=*Y*)
Y	*Y*	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0,4
Y	*N*	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0,48
N	*Y*	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0,04
N	*N*	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0,08

Pour déduire P(*A*|*D*=*N,C*=*Y*), toutes les valeurs de *B* doivent être ajoutées:

Tableau B.10 – Probabilité postérieure pour le nœud A, les nœuds D et C étant définis

P(*A*=*Y*|*D*=*N,C*+*Y*)	P(*A*=*N*|*D*=*N,C*=*Y*)
0,88	0,12

Cela montre que l'a priori de P(*A*=*N*) est passé de 0,1 à un postérieur de 0,12, ce qui ne représente qu'une petite modification. D'un autre côté, P(*B*=*N*|*D*=*N,C*=*Y*) est passé de 0,4 à 0,56, ce qui représente une modification plus significative.

B.26.5 Résultats

La démarche bayésienne peut être appliquée dans la même mesure que les statistiques classiques, avec un large éventail de résultats (une analyse des données pour déduire les estimateurs de point et les intervalles de confiance, par exemple). Sa popularité récente est liée aux réseaux de Bayes pour déduire les distributions a posteriori. Le résultat graphique

offre un modèle aisé à comprendre, et les données peuvent être modifiées facilement pour tenir compte des corrélations et de la sensibilité des paramètres.

B.26.6 Avantages et limites

Avantages:

- il suffit de connaître les a priori;
- les exigences inférentielles sont faciles à comprendre;
- la loi de Bayes est la seule requise;
- elle offre un mécanisme permettant d'utiliser les croyances subjectives d'un problème.

Limites:

- difficulté à définir toutes les interactions dans les réseaux de Bayes pour des systèmes complexes;
- la démarche bayésienne nécessite de connaître une multitude de probabilités conditionnelles qui sont généralement fournies par un avis d'expert. Les outils logiciels ne peuvent offrir que des réponses fondées sur ces hypothèses.

B.27 Courbes F-N

B.27.1 Présentation

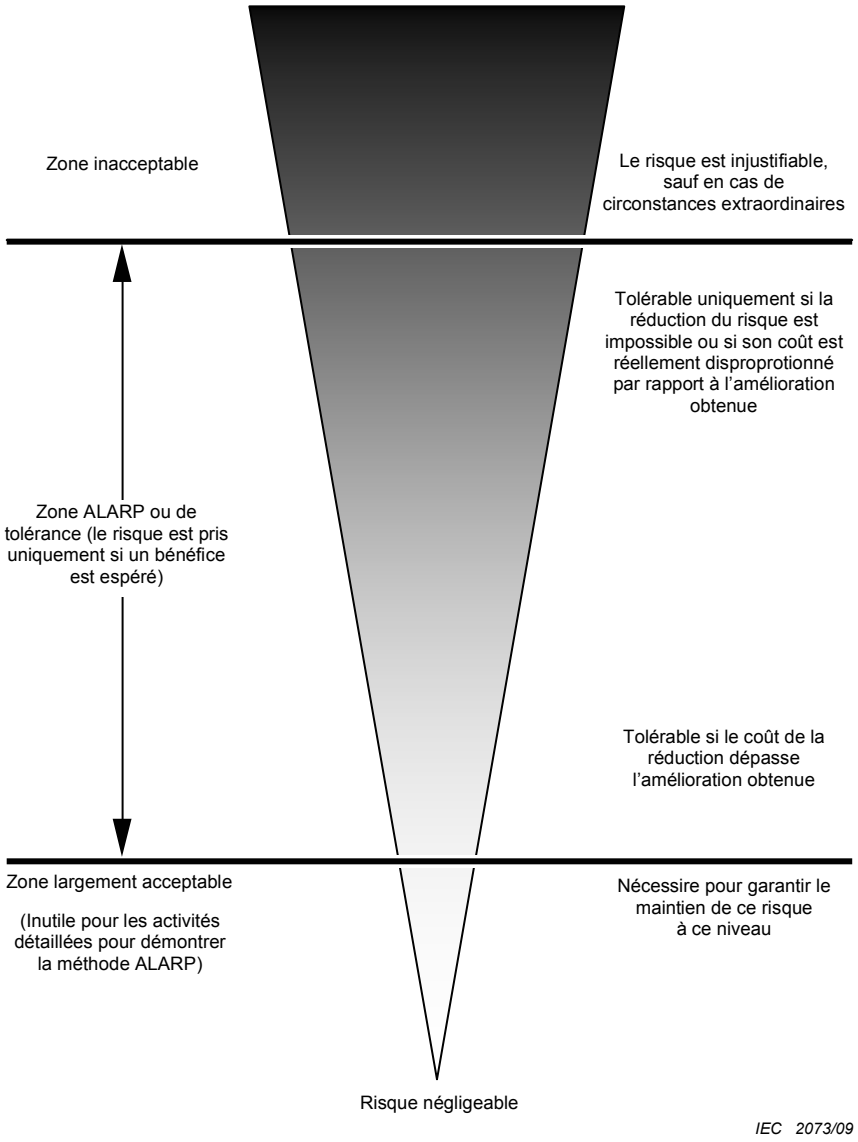

Figure B.12 – Concept ALARP

Les courbes F-N sont une représentation graphique de la probabilité de tous les événements à l'origine d'un niveau donné de nuisance dont fait l'objet une population donnée. La plupart du temps, elles sont liées à la fréquence d'un nombre donné de pertes se produisant.

Les courbes FN illustrent la fréquence cumulée (F) à laquelle au moins N membres de la population seront affectés. Des valeurs élevées de N susceptibles de se produire à une fréquence F élevée sont dignes d'intérêt car elles peuvent être inacceptables du point de vue social et politique.

B.27.2 Utilisation

Les courbes FN sont un moyen de représenter les résultats d'une analyse des risques. La plupart des événements présentent de fortes probabilités de conséquences limitées, et de faibles probabilités de conséquences élevées. Les courbes FN offrent une représentation du

niveau de risque sous la forme d'une droite décrivant cette étendue, et non plus un seul point représentant une paire probabilité-conséquence.

Les courbes FN peuvent être utilisées pour comparer les risques prévus en fonction des critères définis sous la forme d'une courbe FN ou les risques prévus aux données d'incidents historiques ou critères de décision (également exprimés par une courbe F/N).

Les courbes FN peuvent être utilisées pour la conception d'un système ou d'un processus, ou pour la gestion des systèmes existants.

B.27.3 Entrées

Les entrées requises sont:

- des ensembles de paires probabilité-conséquence sur une période donnée;
- des données provenant d'une analyse des risques quantitative donnant les probabilités estimées des nombres spécifiés de pertes;
- les données provenant d'enregistrements historiques et d'une analyse des risques quantitative.

B.27.4 Processus

Les données disponibles sont relevées sur un graphe, le nombre de pertes (à un niveau de nuisance donné, c'est-à-dire la mort) en abscisse et la probabilité de N pertes au moins en ordonnée. Compte tenu du large éventail de valeurs, ces deux axes reposent en principe sur des échelles logarithmiques.

Les courbes FN peuvent être construites de manière statistique à l'aide de nombres «réels» provenant de pertes passées, ou être calculées à partir d'estimations du modèle de simulation. Les données utilisées et les hypothèses mises en place peuvent indiquer que ces deux types de courbe FN donnent des informations différentes et qu'il convient de les utiliser séparément et à différentes fins. D'une manière générale, les courbes FN théoriques sont plus utiles pour la conception du système, les courbes FN statistiques étant plus adaptées à la gestion d'un système existant particulier.

Les deux approches de dérivation peuvent prendre beaucoup de temps et il n'est pas rare d'utiliser un mélange des deux. Des données empiriques forment alors des points fixes représentant des pertes précisément connues à la suite d'accidents/incidents connus dans une période donnée, l'analyse des risques quantitative produisant d'autres points par extrapolation ou interpolation.

La nécessité de prise en compte des accidents peu fréquents mais aux conséquences importantes peut exiger de rassembler suffisamment de données sur de longues périodes afin de procéder à une analyse correcte. Cela rend aussi les données disponibles suspectes si les événements initiateurs peuvent changer dans le temps.

B.27.5 Résultats

Une droite représentant les risques sur une plage de valeurs de conséquence qu'il est possible de comparer à des critères appropriés, permettant d'étudier la population et le niveau de nuisance donné.

B.27.6 Avantages et limites

Les courbes FN sont un moyen utile de présenter les informations relatives aux risques que les gestionnaires et concepteurs du système pourront exploiter pour prendre une décision concernant les risques et niveaux de sécurité. Elles permettent de présenter les informations relatives à la fréquence et aux conséquences sous une forme facilitant la comparaison entre les différents types de risque.

Les courbes FN permettent de comparer des risques découlant de situations analogues lorsque des données suffisantes sont disponibles. Il convient de ne pas les utiliser pour comparer des risques de types différents aux caractéristiques diverses dans des cas où la quantité et la qualité des données varient.

Outre le nombre de personnes impactées, les courbes FN présentent l'inconvénient de ne donner aucune information sur l'étendue des effets ou des résultats d'incidents, et il n'existe aucun moyen d'identifier les différentes manières dont le niveau de nuisance a pu se produire. Elles représentent un type de conséquence particulier, en général les nuisances dont font l'objet les personnes. Les courbes FN ne sont pas une méthode d'évaluation des risques, mais simplement un moyen d'en présenter les résultats.

Il s'agit d'une méthode bien établie de présentation des résultats de l'évaluation des risques qui doit être préparée par des analystes compétents et que les profanes ont souvent beaucoup de difficultés à interpréter et évaluer.

B.28 Indices de risque

B.28.1 Présentation

Un indice de risque est une mesure semi-quantitative des risques. Il s'agit d'une estimation déduite à l'aide d'une approche de correction utilisant des échelles ordinales. Les indices de risque permettent de classer une série de risques à l'aide de critères analogues afin de les comparer. Chaque composante du risque fait l'objet d'un pointage, les caractéristiques du polluant (sources), l'étendue des vecteurs d'exposition possibles et l'impact des récepteurs, par exemple.

En substance, les indices de risque représentent une approche qualitative du classement et de la comparaison des risques. Les nombres sont utilisés simplement pour tenir compte de la manipulation. Dans la plupart des cas, si le modèle ou le système sous-jacent n'est pas bien connu ou ne peut pas être représenté, il est préférable d'utiliser une démarche qualitative plus ouverte.

B.28.2 Utilisation

Les indices peuvent être utilisés pour le classement des différents risques associés à une activité lorsque le système est bien compris. Ils permettent d'intégrer plusieurs facteurs ayant un impact sur le niveau de risque dans un seul pointage numérique du niveau de risque.

Les indices sont utilisés pour différents types de risque, en général comme dispositif de pointage pour classer le risque en fonction du niveau de risque. Ceci peut être utilisé pour déterminer les risques devant faire l'objet d'une évaluation supplémentaire approfondie et, dans la mesure du possible, quantitative.

B.28.3 Entrées

Les entrées sont déduites de l'analyse du système ou d'une description précise du contexte. Cela nécessite une bonne compréhension de toutes les sources du risque, des vecteurs possibles et des éléments susceptibles d'être affectés. Il est possible d'utiliser des outils comme l'analyse par arbre de panne, l'analyse par arbre d'événements et l'analyse de décision générale pour appuyer le développement des indices de risque.

Etant donné que le choix des échelles ordinales est, dans une certaine mesure, arbitraire, des données suffisantes sont nécessaires à la validation de l'indice.

B.28.4 Processus

La première étape consiste à comprendre et décrire le système. Une fois défini le système, des pointages sont développés pour chaque composant de manière à pouvoir les combiner et

fournir un indice composite. Par exemple, dans un contexte lié à l'environnement, les sources, le vecteur et le/les récepteur(s) sont pointés, en notant que, dans certains cas, il existe plusieurs vecteurs et récepteurs pour chaque source. Les pointages individuels sont combinés selon un schéma tenant compte des réalités physiques du système. Il est important d'assurer la cohérence et la relativité interne des pointages de chaque partie du système (sources, vecteurs et récepteurs). Des pointages peuvent être prévus pour les composantes du risque (probabilité, exposition et conséquence, par exemple) ou les facteurs qui augmentent le risque.

Il est possible d'ajouter, de retirer, de multiplier et/ou de diviser des pointages en fonction de ce modèle à niveau élevé. Des effets cumulés peuvent être pris en compte en ajoutant des pointages (l'ajout de pointages pour différents vecteurs, par exemple). Il n'est absolument pas admis d'appliquer des formules mathématiques à des échelles ordinales. Par conséquent, une fois développé le système de pointage, il convient de valider le modèle en l'appliquant à un système connu. Le développement d'un indice est une démarche itérative, plusieurs systèmes différents de combinaisons des pointages pouvant être essayés avant que l'analyse ne maîtrise la validation.

L'incertitude peut être traitée par une analyse de sensibilité et différents pointages pour identifier les paramètres les plus sensibles.

B.28.5 Résultats

Le résultat est une série de nombres (indices composites) liée à une source particulière, et qu'il est possible de comparer aux indices développés pour d'autres sources à l'intérieur du même système ou de modéliser de la même façon.

B.28.6 Avantages et limites

Avantages:

- les indices peuvent être un bon outil de pointage pour le classement des différents risques ;
- ils permettent d'intégrer plusieurs facteurs ayant un impact sur le niveau de risque dans un seul pointage numérique du niveau de risque.

Limites:

- si le processus (modèle) et son résultat ne sont pas correctement validés, les résultats peuvent être dépourvus de sens. Le fait que le résultat soit une valeur numérique du risque peut prêter à interprétation et utilisation erronées, dans l'analyse coût/bénéfice subséquente, par exemple;
- dans la plupart des cas, lorsque les indices sont utilisés, aucun modèle fondamental ne permet de déterminer si les échelles individuelles des facteurs de risque sont linéaires, logarithmiques ou autre, ni de déterminer la manière dont il convient de combiner ces facteurs. Dans ces situations, le classement est naturellement peu fiable et la validation par rapport à des données réelles particulièrement importante.

B.29 Matrice conséquence/probabilité

B.29.1 Présentation

La matrice conséquence/probabilité est un moyen de combiner des classements qualitatifs ou semi-quantitatifs de conséquence et de probabilité pour générer un niveau de risque ou un classement des risques.

Le format de la matrice et les définitions la concernant dépendent du contexte dans lequel elle est utilisée, et il est important d'utiliser une conception appropriée aux circonstances.

B.29.2 Utilisation

Une matrice conséquence-probabilité permet de classer les risques, les sources de risque ou les traitements des risques en fonction de leur niveau de risque. Elle est habituellement utilisée comme un outil de dépistage lorsque de nombreux risques ont été identifiés (pour définir les risques qui doivent faire l'objet d'une analyse plus détaillée ou ceux qui doivent être traités en priorité, ou encore ceux qui doivent être référencés par rapport à un niveau de gestion plus élevé, par exemple). Elle peut également être utilisée pour sélectionner les risques qui doivent être ignorés à ce stade. Ce type de matrice de risque est également largement utilisé pour déterminer si un risque donné est largement acceptable ou inacceptable (voir 5.4) selon sa position dans la matrice.

La matrice conséquence-probabilité peut également être utilisée pour faciliter la communication d'une compréhension commune des niveaux qualitatifs des risques dans toute l'organisation. Il convient que la manière dont les niveaux de risque sont établis et les règles de décision leurs sont assignées soit conforme à la volonté de prise de risque de l'organisation.

Une forme de matrice conséquence/probabilité est utilisée pour l'analyse critique d'une analyse AMDEC ou pour définir les priorités à la suite d'une analyse HAZOP. Elle peut également être utilisée lorsque les données d'analyse détaillée ne sont pas suffisantes ou que la situation ne garantit pas la durée et l'effort à consentir pour procéder à une analyse plus quantitative.

B.29.3 Entrées

Les entrées du processus sont des échelles personnalisées pour la conséquence et la probabilité et une matrice combinant ces deux éléments.

Il convient que l'échelle (ou les échelles) de conséquence couvre la gamme des différents types de conséquence à prendre en compte (les pertes financières, la sécurité, l'environnement ou d'autres paramètres, selon le contexte, par exemple) et qu'elle s'étende de la conséquence la plus crédible à la conséquence la moins probable. Un exemple partiel est présenté dans la Figure B.6.

L'échelle peut comporter un certain nombre de points. Des échelles à 3, 4 ou 5 points sont les plus usuelles.

L'échelle de probabilité peut également comporter un certain nombre de points. Les définitions correspondant à la probabilité doivent être sélectionnées en fonction de leur caractère aussi univoque que possible. Si des guides numériques sont utilisés pour définir différentes probabilités, il convient de préciser les unités. L'échelle de probabilité doit s'étendre sur la plage correspondant à l'étude en cours, sans oublier que la probabilité la plus faible doit être acceptable pour la conséquence définie la plus élevée, sinon toutes les activités aux conséquences les plus élevées sont définies comme intolérables. Un exemple partiel est présenté dans la Figure B.7.

Une matrice est tracée, la conséquence et la probabilité étant placées sur leur axe respectif. La Figure B.8 illustre un exemple de matrice comportant des échelles de conséquence en 6 points et de probabilité en 5 points.

Les niveaux de risque attribués aux cellules dépendent des définitions des échelles probabilité/conséquence. La matrice peut être configurée pour donner une pondération supplémentaire aux conséquences (voir ci-contre) ou à la probabilité, ou être symétrique, selon l'application. Les niveaux de risque peuvent être liés aux règles de décision, comme le niveau de l'attention de gestion ou l'échelle de temps par laquelle une réponse est nécessaire.

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro • Pressu	• Major litigation costing $10m+ • Investigation by regulato body resulting in lo Interruption to
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or Irrevers	• Major spi		
3	$100k – $90 loss or gain					
2	$10 lo					
1						

IEC 2074/09

Figure B.13 – Exemple partiel d'un tableau de critères de conséquence

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distinct - could occur within "mor
Unlikely	- may occur but not e - could occur in "y
Rare	- occurrence re - exceptional - only occ
Remote	- theor - fr

IEC 2075/09

Figure B.14 – Exemple partiel de matrice de classement des risques

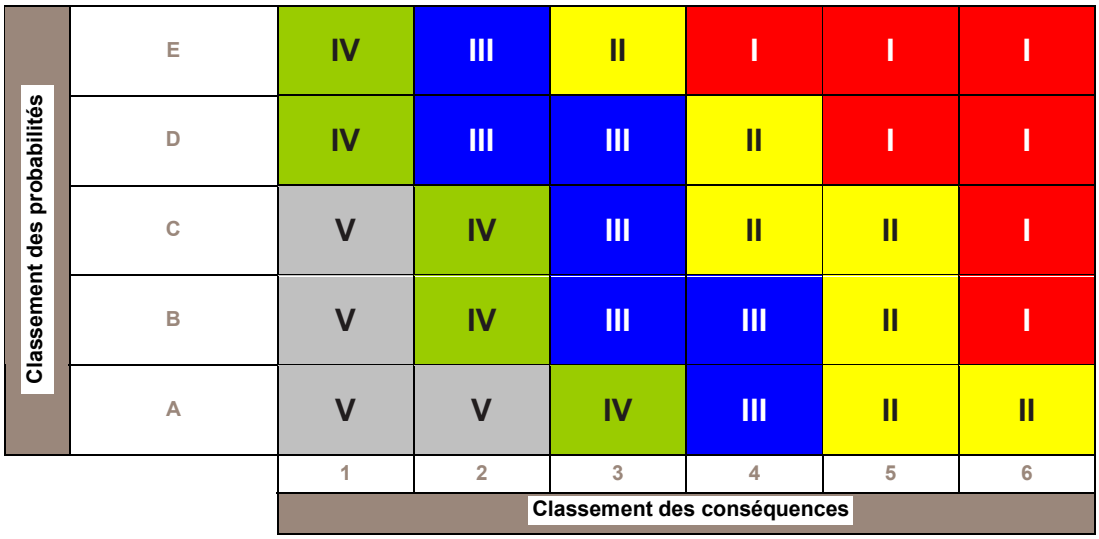

Figure B.15 – Exemple partiel de matrice de critères de probabilité

Les échelles de classement et une matrice peuvent être configurées avec des échelles quantitatives. Par exemple, dans un contexte de fiabilité, l'échelle de probabilité pourrait représenter des taux de défaillance indicatifs et l'échelle de conséquence, le coût de la défaillance, en dollars.

L'utilisation de l'outil implique d'avoir à disposition des personnes (l'idéal serait une équipe) aux compétences adaptées et des données de ce type pour faciliter le jugement des conséquences et probabilités.

B.29.4 Processus

Pour classer les risques, l'utilisateur recherche en premier lieu le descripteur de conséquence correspondant le mieux à la situation, puis définit la probabilité d'occurrence de ces conséquences. Le niveau de risque est alors annoncé en fonction de la matrice.

La plupart des risques peuvent comporter une étendue de résultats auxquels sont associées différentes probabilités. En règle générale, les incidents mineurs sont plus fréquents que les catastrophes. Par conséquent, il faut choisir entre classer le résultat le plus fréquent, le plus sérieux ou d'autres combinaisons de résultats. Dans la plupart des cas, il est pertinent de mettre l'accent sur les résultats crédibles les plus graves, puisqu'ils représentent la menace la plus importante et posent souvent beaucoup de problèmes aux gestionnaires. Dans certains cas, il peut être pertinent de classer les problèmes habituels et les catastrophes improbables comme des risques distincts. Il est important d'utiliser la probabilité correspondant à la conséquence sélectionnée et non pas la probabilité de l'événement dans son ensemble.

Le niveau de risque défini par la matrice peut être associé à une règle de décision relative par exemple à l'application ou non du traitement du risque.

B.29.5 Résultats

Le résultat est un classement de chaque risque ou une liste ordonnée des risques aux niveaux d'importance définis.

B.29.6 Avantages et limites

Les avantages sont les suivants:

- utilisation relativement aisée;
- permet de classer rapidement les risques en différents niveaux d'importance.

Limites:

- il convient de concevoir une matrice en fonction des circonstances. Il peut donc s'avérer difficile d'appliquer un système commun sur une étendue de circonstances liées à une organisation;
- il est difficile de définir les échelles sans équivoque;
- l'utilisation est très subjective et a tendance à varier de manière significative selon les personnes;
- il n'est pas possible d'agréger les risques (c'est-à-dire qu'il n'est pas possible de dire qu'un certain nombre de risques faibles ou qu'un risque faible identifié un certain nombre de fois équivaut à un risque moyen);
- il est difficile de combiner ou de comparer le niveau de risque de différentes catégories de conséquences.

Les résultats dépendent du niveau de détail de l'analyse, c'est-à-dire que plus l'analyse est détaillée plus le nombre de scénarii est élevé, chacun d'eux comportant une faible probabilité. Ceci risque de sous-estimer le niveau de risque réel. Dans le cadre de la description du risque, il convient que la manière dont les scénarii sont regroupés soit cohérente et définie au début de l'étude.

B.30 Analyse coût/bénéfice

B.30.1 Présentation

L'analyse coût/bénéfice peut être utilisée pour évaluer les risques lorsque les coûts prévus sont pondérés en fonction des avantages attendus afin de pouvoir choisir la meilleure option ou la plus rentable. Il s'agit d'une partie implicite de nombreux systèmes d'évaluation des risques. Elle peut être qualitative ou quantitative, ou impliquer une combinaison d'éléments quantitatifs et qualitatifs. L'analyse coût/bénéfice quantitative agrège la valeur pécuniaire de tous les coûts et bénéfices à tous les acteurs inclus dans le domaine d'application et elle ajuste les différentes durées pendant lesquelles les coûts et bénéfices sont actifs. La valeur actualisée nette (VAN) obtenue devient une entrée pour les décisions relatives au risque. Une VAN positive associée à une action indique généralement qu'il convient d'entreprendre l'action. Cependant, pour certains risques, notamment ceux pour la vie humaine ou pour l'environnement, le principe ALARP peut être appliqué. Les risques sont divisés en trois zones: un niveau au-dessus duquel les risques sont intolérables et qu'il convient de ne pas considérer, sauf dans des circonstances extraordinaires ; un niveau au-dessous duquel les risques sont négligeables et dont il suffit d'assurer par surveillance qu'ils restent faibles ; et un niveau moyen dans lequel les risques sont maintenus à un niveau qui soit aussi faible que possible de manière raisonnable (ALARP). Dans la zone limite à risque faible, une analyse coût-bénéfice rigoureuse peut s'appliquer mais lorsque les risques se rapprochent du niveau intolérable, le principe ALARP stipule d'appliquer un traitement, à moins que les coûts du traitement soient disproportionnés par rapport au bénéfice.

B.30.2 Utilisations

L'analyse coût/bénéfice peut être utilisée pour décider parmi les options impliquant un risque.

Par exemple

- comme entrée pour décider s'il convient de traiter ou non un risque,

- pour distinguer et choisir les meilleures formes de traitement des risques,
- pour décider parmi les différents déroulements de l'action.

B.30.3 Entrées

Les entrées comprennent des informations sur les coûts et bénéfices vis-à-vis des acteurs correspondants et sur les incertitudes liées à ces coûts et bénéfices. Il convient de tenir compte des coûts récupérables et irrécupérables et des bénéfices. Les coûts concernent les ressources dépensées et les résultats négatifs, les bénéfices concernent les résultats positifs, les résultats négatifs évités et les ressources économisées.

B.30.4 Processus

Les acteurs qui subissent les coûts ou bénéficient d'avantages sont identifiés. Tous les acteurs sont inclus dans une analyse coût-bénéfice complète.

Les bénéfices et les coûts directs et indirects imputables à tous les acteurs correspondants, issus des options considérées, sont identifiés. Les bénéfices directs sont ceux qui découlent directement de l'action entreprise, les bénéfices indirects ou annexes étant ceux purement fortuits mais participant encore de manière significative à la prise de décision. Les bénéfices indirects sont par exemple le gain de réputation, la satisfaction du personnel et la «tranquillité d'esprit». (Ils pèsent souvent lourd dans la prise de décision).

Les coûts directs sont les coûts directement associés à l'action. Les coûts indirects sont les coûts supplémentaires, annexes et non récupérables, tels que la perte d'utilité, le risque de gaspiller du temps de gestion ou le détournement du capital loin d'autres investissements potentiels. Lorsque l'analyse coût/bénéfice est appliquée à une décision de prendre, ou pas, un risque, il convient d'inclure les coûts et les bénéfices liés au traitement du risque et à la prise de risque.

S'agissant d'une analyse coût/bénéfice quantitative, après avoir identifié tous les coûts récupérables et irrécupérables et tous les bénéfices, une valeur pécuniaire est attribuée à tous les coûts et bénéfices (y compris les coûts irrécupérables). Un certain nombre de méthodes normalisées permettent de réaliser cette opération, notamment la démarche « volonté de payer » et l'utilisation de substituts. Si, comme cela est souvent le cas, le coût est subi sur une courte période (une année, par exemple) et que les bénéfices profitent pendant une longue période, il est en principe nécessaire d'actualiser les bénéfices pour les ramener en «monnaie courante» de manière à obtenir une comparaison valide. Tous les coûts et bénéfices sont exprimés en valeur actualisée. La valeur actualisée de tous les coûts et bénéfices vis-à-vis de tous les acteurs peut être combinée pour générer une valeur actualisée nette (VAN). Une VAN positive implique que l'action est bénéfique. Des rapports avantages-coûts sont également utilisés, voir B.30.5.

S'il subsiste une incertitude quant au niveau des coûts ou des bénéfices, les uns ou les autres, ou les deux, peuvent être pondérés en fonction de leurs probabilités.

L'analyse coût/bénéfice qualitative ne tente pas d'attribuer une valeur pécuniaire aux coûts irrécupérables, et plutôt que de fournir une seule valeur cumulant les coûts et les bénéfices, elle considère d'un point de vue qualitatif les relations et les compromis qui existent entre les différents coûts et bénéfices.

Une technique connexe est une analyse coût-efficacité. Elle suppose qu'un avantage ou un résultat donné est souhaité et qu'il existe plusieurs moyens alternatifs pour l'obtenir. L'analyse ne s'intéresse qu'aux coûts et à la manière la moins onéreuse d'obtenir l'avantage considéré.

B.30.5 Résultat

Le résultat d'une analyse coût-bénéfice est une information sur les coûts et bénéfices relatifs en fonction de différentes options ou actions. Il peut être exprimé de manière quantitative par une valeur actualisée nette (VAN), un taux de rentabilité interne (TRI) ou par le rapport de la valeur actualisée des bénéfices à la valeur actualisée des coûts. Du point de vue qualitatif, le résultat se traduit généralement par un tableau de comparaison des coûts et des bénéfices de différents types tenant particulièrement compte des compromis.

B.30.6 Avantages et limites

Les avantages de l'analyse coût/bénéfice sont les suivants:

- permet de comparer les coûts et les bénéfices selon une métrique simple (numéraire);
- garantit la transparence de la prise de décision;
- nécessite de recueillir des informations détaillées sur tous les aspects possibles de la décision. Ceci peut être utile pour déceler toute ignorance et communiquer la connaissance.

Les limites sont les suivantes:

- l'analyse coût/bénéfice quantitative peut produire des chiffres significativement différents en fonction des méthodes utilisées pour attribuer des valeurs économiques à des avantages non économiques;
- pour certaines applications, il est difficile de définir un taux d'actualisation valide pour les coûts et bénéfices futurs;
- les bénéfices dont profite une large population sont difficiles à estimer, notamment ceux liés aux biens publics qui ne font pas l'objet d'échange sur les marchés;
- l'actualisation signifie que les bénéfices obtenus sur le très long terme ont une influence négligeable sur la décision en fonction du taux d'actualisation choisi. La méthode ne s'applique plus lorsqu'il s'agit de tenir compte des risques ayant un effet sur les générations futures, à moins d'établir des taux d'actualisation très faibles, voire nuls.

B.31 Analyse de décision à critères multiples (ADCM)

B.31.1 Présentation

Il s'agit d'utiliser un ensemble de critères permettant d'évaluer de manière objective et transparente la valeur globale d'un ensemble d'options. En règle générale, le but global est d'établir un classement ordonné préférentiel des options disponibles. L'analyse implique l'élaboration d'une matrice d'options et de critères qui sont classés et agrégés pour fournir un pointage global pour chaque option.

B.31.2 Utilisation

L'ADCM peut être utilisée pour:

- comparer plusieurs options dans le cadre d'une première analyse pour déterminer les options privilégiées et potentielles et les options inappropriées;
- comparer les options lorsque les critères sont multiples, et parfois en contradiction;
- parvenir à un consensus sur une décision lorsque les objectifs ou les valeurs des différents acteurs sont en contradiction.

B.31.3 Entrées

Un ensemble d'options pour analyse. Des critères, fondés sur des objectifs, qu'il est possible d'appliquer de manière uniforme à toutes les options pour les différencier.

B.31.4 Processus

En règle générale, un groupe d'acteurs bien informés réalise le processus suivant:

a) définition du ou des objectifs;
b) détermination des attributs (critères ou mesures de performance) liés à chaque objectif;
c) hiérarchisation des attributs;
d) développement des options à évaluer en fonction des critères;
e) détermination de l'importance des critères et attribution des facteurs de pondération correspondants;
f) évaluation des alternatives par rapport aux critères. Ceci peut être représenté par une matrice de pointages.
g) combinaison de plusieurs pointages à attribut simple en un seul pointage à attributs multiples agrégés;
h) évaluation des résultats.

Différentes méthodes permettent d'obtenir la pondération applicable à chaque critère et les différentes manières d'agréger les pointages relatifs aux critères pour chaque option en un seul pointage à attributs multiples. Par exemple, les pointages peuvent être agrégés par une somme pondérée ou un produit pondéré, ou en utilisant une méthode de hiérarchie multicritère (Il s'agit d'une technique de stimulation en faveur des facteurs de pondération et des pointages, fondée sur des comparaisons par paire). Toutes ces méthodes supposent que la préférence accordée à un critère ne dépend pas des valeurs des autres critères. Lorsque cette hypothèse n'est pas valide, différents modèles sont utilisés.

Dans la mesure où les pointages sont subjectifs, l'analyse de sensibilité permet d'examiner la mesure dans laquelle les facteurs de pondération et les pointages ont un effet sur les préférences globales accordées aux différentes options.

B.31.5 Résultats

Le classement ordonné des options va des meilleures préférences aux moins bonnes. Si le processus génère une matrice dont les axes représentent les critères pondérés et les critères pointés pour chaque option, les options qui correspondent aux critères fortement pondérés peuvent également être éliminées.

B.31.6 Avantages et limites

Les avantages sont les suivants:

- fournit une structure simple pour prise de décision efficace et présentation des hypothèses et des conclusions;
- peut traiter des problèmes de décision complexes qui ne peuvent pas faire l'objet d'une analyse coût/bénéfice, plus gérable;
- permet de considérer de manière rationnelle les problèmes impliquant de faire des compromis;
- permet de parvenir à un accord lorsque les acteurs ont des objectifs divergents, et de ce fait, des critères différents.

Les limites sont les suivantes:

- peut être affectée par des erreurs et une mauvaise sélection des critères de décision;
- la plupart des problèmes traités par l'ADCM ne donne pas une solution définitive ou unique;

- les algorithmes d'agrégation qui calculent les facteurs de pondération des critères à partir des préférences déclarées ou qui agrègent différents points de vue peuvent masquer le véritable fondement de la décision.

Bibliographie

CEI 61511, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

CEI 61882, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

ISO 22000, *Systèmes de management de la sécurité des denrées alimentaires – Exigences pour tout organisme appartenant à la chaîne alimentaire*

ISO/CEI Guide 51, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

CEI 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11 : Guide d'application – Maintenance basée sur la fiabiltié*

CEI 61649, *Analyse de Weibull*

CEI 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

CEI 61165, *Application des techniques de Markov*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets* (disponible uniquement en anglais)

CEI 62551, *Techniques d'analyse pour la sûreté de fonctionnement – Modélisation par réseau de Petri*[10]

CEI 61882, *Études de danger et d'exploitabilité (études HAZOP) – Guide d'application*

_____

10 Actuellement à l'étude.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch