56/1268/CDV

COMMITTEE DRAFT FOR VOTE (CDV)
PROJET DE COMITÉ POUR VOTE (CDV)

	Project number Numéro de projet	IEC 31010 Ed. 1.0
	IEC/TC or SC: **TC 56** CEI/CE ou SC:	Secretariat / Secrétariat **UK**
☒ Submitted for parallel voting in CENELEC Soumis au vote parallèle au CENELEC	Date of circulation Date de diffusion **2008-05-23**	Closing date for voting (Voting mandatory for P-members) Date de clôture du vote (Vote obligatoire pour les membres (P)) **2008-10-24**

Also of interest to the following committees Intéresse également les comités suivants	Supersedes document Remplace le document 56/1201/CD and 56/1240A/CC

Functions concerned
Fonctions concernées

□ Safety Sécurité	□ EMC CEM	□ Environment Environnement	□ Quality assurance Assurance qualité

CE DOCUMENT EST TOUJOURS À L'ÉTUDE ET SUSCEPTIBLE DE MODIFICATION. IL NE PEUT SERVIR DE RÉFÉRENCE.

LES RÉCIPIENDAIRES DU PRÉSENT DOCUMENT SONT INVITÉS À PRÉSENTER, AVEC LEURS OBSERVATIONS, LA NOTIFICATION DES DROITS DE PROPRIÉTÉ DONT ILS AURAIENT ÉVENTUELLEMENT CONNAISSANCE ET À FOURNIR UNE DOCUMENTATION EXPLICATIVE.

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

RECIPIENTS OF THIS DOCUMENT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Titre :

Title : IEC 31010 Ed. 1.0: Risk Management - Risk Assessment Techniques

Note d'introduction

La version française sera diffusée ultérieurement.

Introductory note

French version will be circulated at a later date.

Please note: This project began as IEC 60300-3-9 Ed. 2.0. It was transformed to IEC 31010 Ed. 1.0 per SMB/3585A/RV dated 2008-01-09.

Also note: PT 3.16 will be meeting the week of October 13th, 2008 to resolve the comments submitted. National Committees are kindly asked to submit their comments prior to October 10th if possible. The official closing date for comments remains as 2008-10-24.

ATTENTION **VOTE PARALLÈLE** **CEI – CENELEC** L'attention des Comités nationaux de la CEI, membres du CENELEC, est attirée sur le fait que ce projet de comité pour vote (CDV) de Norme internationale est soumis au vote parallèle. Les membres du CENELEC sont invités à voter via le système de vote en ligne du CENELEC.	**ATTENTION** **IEC – CENELEC** **PARALLEL VOTING** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) for an International Standard is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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.

This international standard has been prepared by ISO TC56 and ISO TMB Risk Management working group

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

FDIS	Report on voting
XX/XX/FDIS	XX/XX/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.

Annexes A and B are for information only.

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 date1 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, or
- amended.

[1] The National Committees are requested to note that for this publication the maintenance result date is 2015.

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, 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 must 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 organization's context for identifying, analysing, evaluating, treating, and monitoring risk associated with any activity, product, function or process; and
- reporting 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 likelihood 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?
- How likely are these to occur?
- 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 utilisation 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 publication, the specific standards will generally be sufficient.

This standard complies with ISO/IEC policy and principles regarding risk management. Risk-related terms and definitions are traceable to ISO/IEC guidance and vocabulary standards.

1 Scope

This international standard provides guidance for the selection and application of systematic/methodical techniques for risk assessment.

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

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

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

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 31000, Risk Management – Guidelines on principles and implementation of risk management

ISO/IEC Guide 73, Risk Management - Vocabulary

3 Definitions

For the purposes of this International Standard, the terms and definitions of ISO/IEC Guide 73, Risk Management - Vocabulary, apply.

4 Risk assessment concepts for technological systems

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:

- providing objective information for decision makers;
- understanding of the risk and its potential impact upon objectives;
- identifying analysing and evaluating risks and determining the need for their treatment;
- quantification or ranking of risks;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identification of the important contributors to risks and weak links in systems and organisations;
- comparison of risks in alternative systems, technologies or approaches;

- identification and communication of risks and uncertainties;
- assisting with establishing priorities for health and safety;
- rationalising a basis for preventive maintenance and inspection;
- post-incident investigation and prevention;
- selecting different forms of risk treatment ;
- meeting regulatory requirements;
- providing information that will help evaluate the tolerability of the risk when compared with pre-defined criteria.

4.2 **Risk Assessment** (As part of the Risk Management Process and Framework)

4.2.1 General

A framework for managing risk aims to assist the organisation to manage risk effectively by developing policies and procedures which integrate the management of risk into organisational processes at varying levels and within specific contexts of the organisation.

As part of this framework the organisation should have a policy or strategy for ensuring that objectives are met and when risk assessment should be applied. This policy or strategy may specify:

- organisational objectives for risk assessment;
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated;
- methods and techniques to be used for risk assessment, and its' contribution to the Risk Management Process;
- accountability, responsibility and authority for performing risk assessment;
- resources available to carry out risk assessment;
- how performance will be reported and reviewed.

Risk assessment comprises the core elements of the Risk Management Process. This is defined in ISO 31000 and contains 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 must be fully integrated into the other components in the Risk Management Process.

4.2.2 Communication and Consultation

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

Involving stakeholders in the risk management process is necessary in order to:

- develop a communication plan;
- help define the context appropriately;
- ensure that the interests of stakeholders are understood and considered;

- ensure that different views are appropriately considered in evaluating risks;
- help ensure that risks are adequately identified; and
- secure 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.

4.2.3 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:

1) Establishing the external context involves familiarisation with the environment in which the organisation 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.
2) Establishing the internal context which may involve understanding :
   - capabilities of the organisation 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).
3) Establishing the risk management context includes:
   - defining accountabilities and responsibilities;
   - defining the depth and breadth 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 the way performance is evaluated in the management of risk;

- identifying and specifying the decisions that have to be made; and
- identifying scoping or framing studies needed, their extent, objectives, and the resources required for such studies.

4) The ‘Defining Risk criteria’ phase includes:

- the nature and types of consequences to be included and how they will be measured;
- the way in which likelihood is 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;
- organisational risk appetite;
- legal and other requirements for specific equipment or applications.

4.2.4 Risk Assessment

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

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

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

4.2.5 Risk Treatment

Having completed a Risk Assessment, Risk treatment involves selecting and agreeing one or more relevant options for changing the occurrence of, or mitigating the effect of risks, 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.

4.2.6 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 risk the assessment is based - in particular, 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 The risk assessment process

5.1 Overview

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.

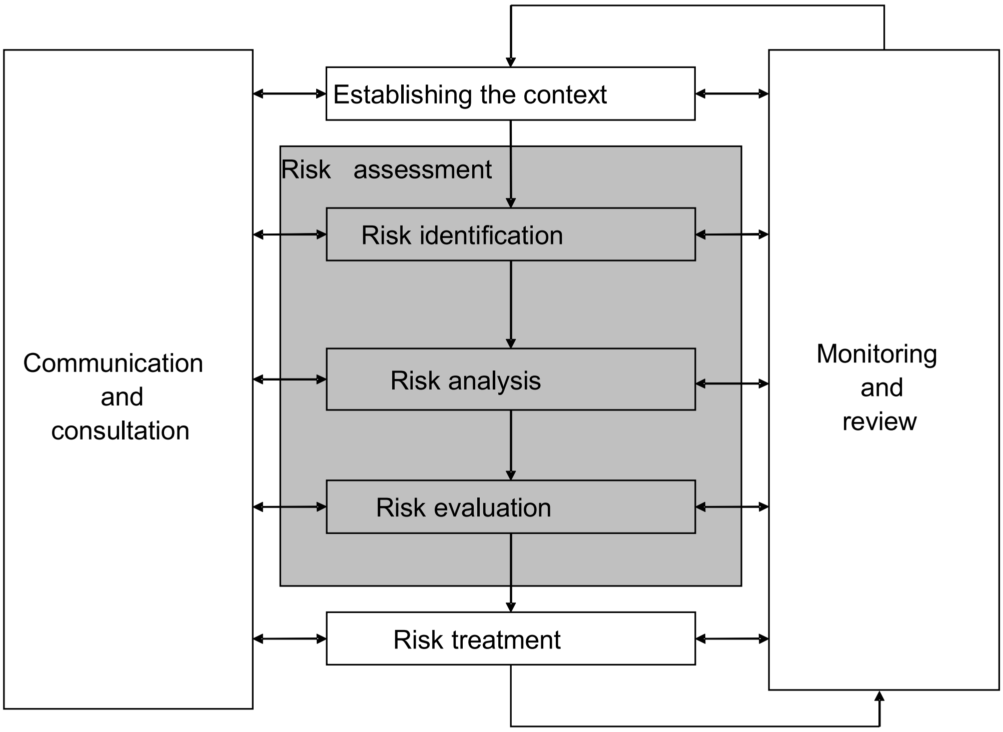


Figure 1 - The contribution of risk assessment to the risk management process

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

Risk assessment allows decision makers and responsible parties to have an improved understanding of risks that could affect objectives as well as of 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 should be used as input to the decision making processes of the organization.

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 may affect the achievement of the objectives of the system or organisation. 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 may have a material impact upon objectives, and the nature of that impact

Risk identification methods can include:

- evidence based methods, examples of which are checklists, 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 event tree logic diagrams.

Various 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 in the overall risk identification process due recognition is given to human and organizational factors. Hence events involving human and organizational deviations from expected should also be included in the risk identification process as well as "hardware” or “software” events.

5.3 Risk analysis

5.3.1 General

The objective of risk analysis is to understand the risk so that decisions about its tolerability or acceptability and the most appropriate form of treatment can be made.

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

The causes of the risk are analysed to determine their contribution to frequency or likelihood of occurrence, and consequences. This also provides a valuable insight into the most effective ways to further treat the risk if this is intended. The analysis may also include estimation of the likelihood of other risks contributing to the consequence(s) and may therefore involve analysis of the sequence of events by which the occurrence of the event can result in the consequence(s). Various methods for these analyses are described in Annex B.

Methods used in analysing risks may 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 organisation. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, likelihood and risk by words such as high medium and low and may combine consequence and likelihood and evaluate the resultant level of risk against qualitative criteria.

Semi quantitative methods use numerical rating scales for likelihood and consequence and combine them using a formula. Scales may be linear or logarithmic or have some other relationship and formulae used can also vary.

Quantitative analysis estimates realistic values for consequences and their likelihood and produces values 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 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 clear explanation of all the terms employed and the basis for all consequence and likelihood criteria should be recorded.

Even where full quantification has been carried out it needs to be recognized that the risk values calculated are estimates and care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and analytical methods employed.

5.3.2 Consequence analysis

Consequence analysis estimates the impacts upon objectives, assuming that particular events situations or circumstances have occurred. An event may have a range of impacts of different severity and affect a range of different objectives and different stakeholders.

Consequence analysis should:

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

5.3.3 Likelihood estimation

Likelihood, Probability or Frequency estimation is used to assign values to the likelihood of occurrence of each consequence associated with an event, situation or circumstance identified at the risk identification stage.

Three general approaches are commonly employed to estimate likelihood. They may be used individually or jointly:

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

2) Forecast likelihoods 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 likelihoods by analysis of the system, activity, equipment or organisation and its associated failure or success states. Numerical data for equipment, humans, organisations and systems from operational experience or published data sources, are then combined to produce an estimate of the likelihood 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. Simulation techniques may be required to generate likelihood of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.
3) Expert opinion can be used in a systematic and structured process to estimate likelihood. There are a number of formal methods for eliciting expert judgement which make the use of judgements visible and explicit and provide an aid to the asking of appropriate questions. Expert judgements should draw upon all relevant available information including historical, system-specific, organisational-specific, experimental, design, etc. The methods available include the Delphi approach, paired comparisons, category rating and absolute likelihood judgements.

All of these techniques may be used individually or jointly.

5.3.4 Screening Risks

The screening of identified and analysed risks, at least in a preliminary way may be done to identify the most significant risks. The purpose is to ensure that resources will be focussed on the most important risks. Screening should be based on criteria defined in the context.

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

Risks may be rated qualitatively on the basis of a combination of consequence and likelihood by positioning them within a consequence/likelihood matrix denoting different levels of risk.

The screening process determines one 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.

5.3.5 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 the size and significance of the level 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. These should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

5.3.6 Level of risk

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, a risk can be expressed as a likelihood distribution over a range of consequences.

5.4 Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, 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.

Factors affecting 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 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 don't. This gives attractively simple results but does not reflect the uncertainties involved both in estimating risks and in defining the boundary between those that require treatment and those that don't.

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; and
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 follows this approasch and is illustrated below in Figure 2.

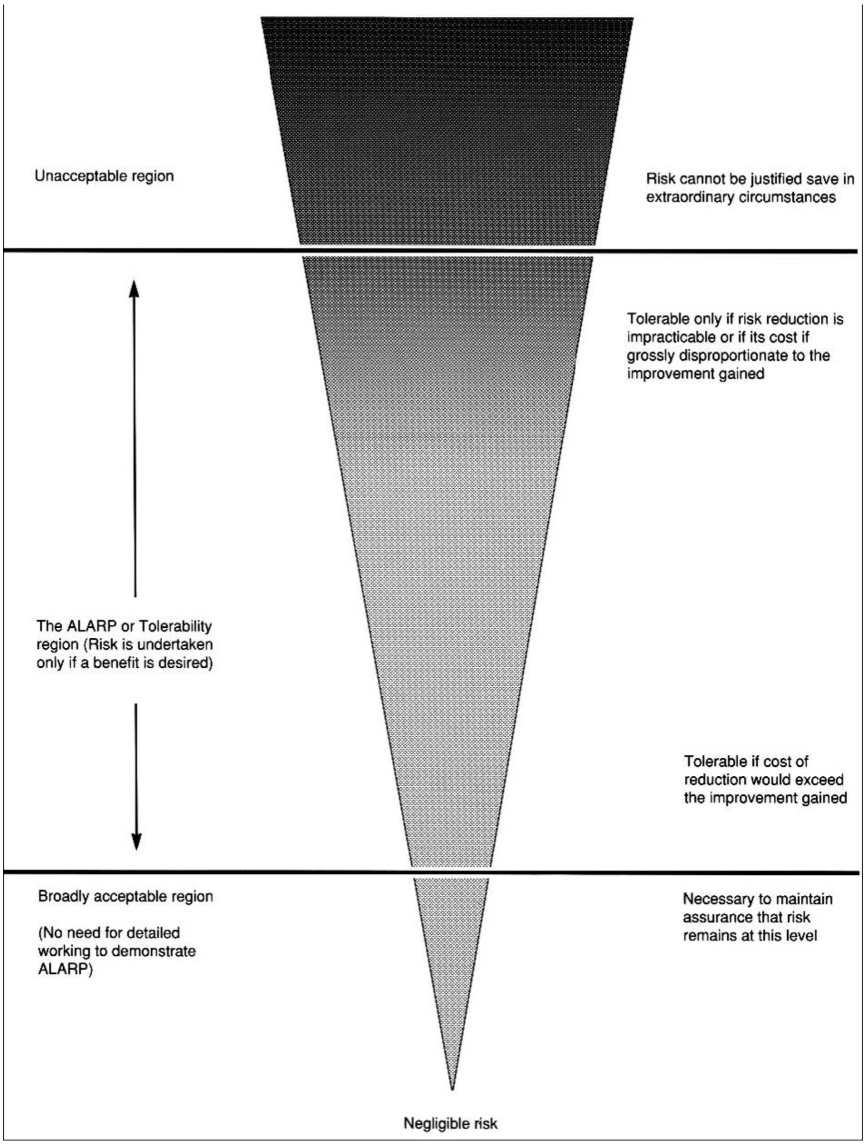

Unacceptable region
Risk cannot be justified save in extraordinary circumstances
Tolerable only if risk reduction is impracticable or if its cost if grossly disproportionate to the improvement gained
The ALARP or Tolerability region (Risk is undertaken only if a benefit is desired)
Tolerable if cost of reduction would exceed the improvement gained
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
Necessary to maintain assurance that risk remains at this level
Negligible risk

Figure 2 - The ALARP Concept[2]

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;
- a summary of the external and internal context of the organisation and how it relates to the situation, system or circumstances being assessed;
- risk criteria applied and their justification;
- limitations, assumptions and justification of hypotheses;
- description of relevant parts of the system;

[2] Taken from “The Tolerability of Risk from Nuclear Power Stations”, The Health and Safety Executive, 1988, Her Majesty’s Stationary Office, London, ISBN 0 11 883982 9

- assessment methodology;
- risk identification results;
- data, assumptions and their sources and validation;
- risk analysis results;
- sensitivity and uncertainty analysis;
- discussion of results;
- references.

If the risk assessment is required to support a continuing risk management process it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, organisation, 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 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 realisation 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.

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 contributes to design refinement process; contributes to cost-effectiveness studies and identifies 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 Methods

6.1 General

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

6.2 Selection of methods

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 methods and the factors present in a given risk situation, and provide illustrative examples of how organizations can select the appropriate risk assessment method(s) for a particular situation.

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

- it should be justifiable and appropriate to the situation or organisation 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 methods should be given, with regard to relevance and suitability. When integrating the results from different studies, the methods 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 method or methods 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 methods 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 required. A simple method, well done, can often 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 methods 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 methods 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 available resources and capabilities of the organization, the nature and degree of uncertainty and the complexity and potential consequences of the risk (see Table A2).

Resources and capabilities which may affect choice of risk assessment methods including the skills, experience, capacity and capability of the risk assessment team; the availability of management time and other resources within the organization; as well as the budget available if external resources are required.

The nature and degree of uncertainty require an understanding of the quality, quantity and integrity of information available about 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, systems methods used to collect data may change, the way organizations use systems methods may change or the organization may not have a system method in place 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 must always be communicated to decision makers.

Complexity is another important characteristic which should be taken into account in risk assessment. 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 synergies. 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 option for risk assessment.

6.3 Types of risk assessment methods

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

Each of the methods 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
Comparison of risk assessment methods
(Informative)

A.1 Types of methods

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

- risk identification;
- risk analysis - consequence analysis
- risk analysis - qualitative, semi-quantitative or quantitative likelihood analysis;
- 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 A1).

A.2 Factors influencing selection of risk assessment methods

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 nature of resources needed to carry out the risk assessment with regards to degree of involvement by management, amount and level of expertise required to perform the risk assessment or data and cost.

Examples of types of risk assessment methods available are listed in Table A2 where each method is rated as high medium or low in terms of these attributes.

Table A1- Selection of tools for Risk Assessment

Tools & Techniques	RISK ASSESSMENT PROCESS				
		RISK ANALYSIS			RISK EVALUATION
	RISK IDENTIFICATION	CONSEQUENCE	LIKELIHOOD	LEVEL OF RISK	
Failure mode and effect analysis (IEC 60812)	SA	NA	NA	NA	NA
Failure mode, effect and criticality analysis (IEC 60812)	SA	SA	SA	SA	SA
Fault tree analysis (IEC 61025)	NA	A	A	A	A
Hazard and operability studies (HAZOP) (IEC 61882)	SA	SA	NA	NA	SA
Reliability centred maintenance (IEC 60300-3-11)	SA	SA	SA	SA	SA
Markov analysis (IEC 61665)	A	NA	SA	NA	NA
Human reliability analysis	SA	SA	SA	SA	A
Preliminary hazard analysis	SA	NA	NA	NA	NA
Event tree analysis	NA	SA	SA	A	NA
Brainstorming	SA	NA	NA	NA	NA
Structured or Semi-Structured Interviews	SA	NA	NA	NA	NA
Delphi Techniques	SA	NA	NA	NA	NA
Checklists	SA	NA	NA	NA	NA
Consequence/Likelihood Matrix	SA	SA	SA	SA	A
LOPA	SA	NA	NA	NA	NA
SWIFT	SA	SA	SA	SA	SA
Decision Tree	NA	SA	SA	A	A
Bow Tie Analysis	NA	A	SA	SA	A
Monte Carlo	NA	SA	SA	SA	SA
Root Cause Analysis	A	NA	SA	SA	NA
HACCP	SA	SA	NA	NA	SA
Environmental Risk Assessment	SA	SA	SA	SA	SA
Scenario Analysis	SA	SA	A	A	A
Budsiness Impact Analysis	A	SA	A	A	A
Cause & Consequence Analysis	A	SA	NA	A	A
Cause and effect analysis	SA	SA	NA	NA	NA
Sneak Circuit Analysis	A	NA	NA	NA	NA
Bayesian Analysis	NA	NA	SA	NA	SA

Table A2 – Attributes of a Selection of Risk Assessment tools

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output
		Resources and capability	Nature & Degree of uncertainty	Complexity	
Look-Up Methods					
Checklists	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	-
Preliminary Hazard Analysis	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.	low	high	medium	±

Creativity Methods					
Structured Interview & Brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them in a team. Brainstorming may be stimulated by prompts or by One-on-one and one-on-many interview techniques	low	low	low	-
Delphi Technique	A means of combining expert opinions that may support source and effects identification, likelihood and consequence estimation and risk evaluation. It is a collaborative technique for building consensus Involving independent analysis and voting by experts.	medium	medium	medium	-
Structured What-if (SWIFT)	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	
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	

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 should consider what controls were in place at the time the loss occurred and how controls might be improved.	medium	low	medium	-
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	+
Environmental 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 an description of the nature of risk and its level	high	high	Medium	+ +
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	+

Top Event Analysis					
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	high	++
Event Tree Analysis	Using inductive reasoning to translate likelihood of different initiating events into possible outcomes	med	med	med	++
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	++
Cause-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	med	+

Function Analysis					
FMEA and FMECA	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. In the case of Process FMEA, the Risk Priority number (a combination of severity of the failure, the failure cause occurrence and the detection effectiveness) is determined to prioritise the items for further action consideration. This analysis is usually semi-quantitative, but actual data for occurrence and detection can be used. FMECA extends a Design FMEA so that each fault mode identified is ranked according to the combined influence of its likelihood of occurrence and the severity of its consequences. This analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.	medium	medium	medium	+
Reliability-Centred Maintenance	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	medium	medium	medium	++

Sneak Analysis (Sneak Circuit Analysis)	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.	medium	medium	medium	++
HAZOP Hazard & Operability Studies	HAZOP is a general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system.	medium	high	high	+
HACCP Hazard Analysis and Critical Control Points	The Hazard Analysis and Critical Control Point is 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	+

Controls Assessment					
Layers of Protection Analysis (LOPA)	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated.	medium	medium	medium	+
Bow Tie Analysis	Bow tie analysis is 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 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	medium	high	medium	+

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	++
Monte-Carlo Analysis	Monte Carlo simulation is used to establish the aggregate variation in a system of the resulting from the variations in 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 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	++
Bayesian Analysis	Bayesian analysis is a statistical procedure which utilises prior distribution data to assess the likelihood 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	++

Annex B Methods of assessment
(Informative)

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 off 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 system, process or application being assessed.

B.1.4 The Process

Brainstorming may be formal or informal. Formal brainstorming is more structured with participants prepared in advanced 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 criticised 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 so identifies 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:

- The 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. (For example that all potential risks have been identified);
- There may be particular group dynamics so some people with valuable ideas stay quiet or others dominate discussion. This can be overcome by Computer brainstorming, using a chat forum. Computer brainstorming can be set up to be anonymous, avoiding political issues which may impede free flow of ideas.

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 therefore 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 interviewee. 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 interview may wish to go.

B.2.5 Output

The output is stakeholder views on the issues which are the subject of the interviews.

B.2.6 Strengths and Limitations

The strengths of structured interviews are:

- 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:

- 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

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 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 lifecycle wherever a consensus of views of experts is required.

B.3.3 Inputs

A set of options for which consensus is required.

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 steps are:

- 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 – avoids problems 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 lifecycle 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 checklist can be selected or developed.

B.4.4 Process

The steps are:

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 identfication risks;
- They address the ‘known knowns’, not the ‘known unknown’s or the ‘unknown unknowns’.
- The encourage ‘tick the box’ type behaviour;
- They tend to be observation based so miss problems 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 to prioritizing hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

B.5.3 Inputs

An understanding of the intended purpose of the system to be assessed;

Such details of the design of the system as are available.

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 likelihood may be carried out to identify risks for further assessment.

PHA should be updated during the phases of design, construction and testing 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

A list of hazards and risks;

Recommendations in the firm 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 will not be comprehensive or 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 organisational objectives. The study team is also expected to, where possible, provide a solution to eliminate the risk.

The HAZOP process is a qualitative technique based on use of guide-words which question how the design intention or operating conditions may 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.

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, including mechanical and electronic systems, procedures, software systems and even to organisational 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 (Control Hazards and Operability 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. 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 are current information about the system, process or procedure to be reviewed, 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 organisational 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 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 customised 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.

The normal steps in a HAZOP study include:

- Nomination of a person with the necessary responsibility and authority to conduct the HAZOP study and have any actions arising from it 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 operation 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/processes or elements to make the review tangible;
- Agreeing the design intent for each subsystem /process or 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.

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

Table B 1, Example of possible HAZOP guidewords

B.6.5 Outputs

Minutes of the HAZOP meeting(s) with items for each review point recorded. This 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 can not be corrected then the risk for the deviation needs to be assessed.

B.6.6 Strengths and Limitations

Strengths of a HAZOP include:

- 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.

Limitations include:

- It can be very time consuming and therefore expensive;
- It requires a high level of documentation or system/process and procedure specification;
- Because of the extent of documentation required it usually takes place so late in a design process (when detailed design data is available) that major modifications that are suggested can be expensive and untenable;
- There can be a overriding focus on finding solutions rather than on challenging “why are we doing this”;
- 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 requires 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 Comparisons

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 where as FMEA starts by identifying failure modes.

B.6.8 References

IEC 61882: “Hazard and operability studies (HAZOP studies) – Application guide”. International Electrotechnical Commission, Geneva.

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 minimised 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 organisations 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 generalised 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:

1) Identify hazards & preventive measures for them;
2) Determine the points in the process where the hazards can be controlled or eliminated (the critical control points or CCPs);
3) Establish critical limits needed to control the hazards. I.e. each CCP must operate within specific parameters to ensure the hazard is controlled;
4) Monitor the critical limits for each CCP at defined intervals;
5) Establish corrective actions if the process falls outside established limits;
6) Establish verification procedures;
7) Implement 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:

- the hazards which could be introduced, controlled or exacerbated at the step;
- whether the hazards present a significant risk (based on consideration of consequence and likelihood 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 that 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;
- It focuses on the practicalities of how and where in a process hazards can be prevented and risks controlled;
- It encourages risk control throughout the process rather than relying on final product inspection;

- It can 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 References

ISO 22000 Food Safety Management Systems.

B.8 Environmental risk assessment

B.8.1 Overview

Environmental risk assessment is here used 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 by laboratory based or epidemiological.

B.8.4 Process

Steps of the process are:

1) Problem formulation This includes setting the scope of the assessment by defining the range of target populations and hazard types of interest;
2) 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;
3) 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.

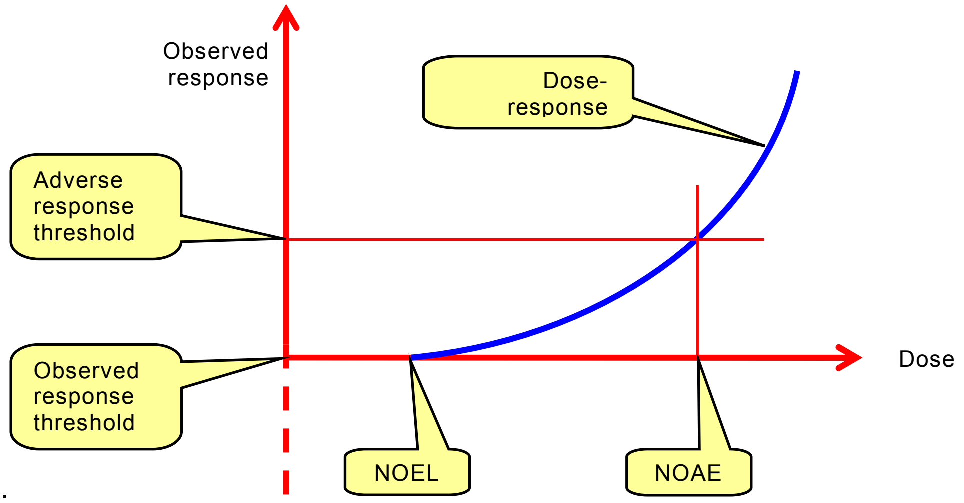


Figure B.1 — Dose-response curve

For chemical exposures test results, are used to derive dose-response curves, like the schematic one 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 likelihood that a particular level of harm from a particular exposure to the hazard is estimated.

4) Exposure analysis. This step examines how a hazard 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, the environmental fate of pesticide reaching the ground, whether it can accumulate in animals, 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.

5) Risk characterisation. In this step the information from the hazard analysis and the exposure analysis are brought together to estimate the likelihood 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 characterisation carried out on the higher risk scenarios.

B.8.5 Outputs

The output is normally a level of risks 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 cancer risk 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, qualitative output may be a level of risk (e.g. high, medium, low) or a description with data where practical 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 very useful tool generally for all areas of risk to identify how and where it may be possible to improve controls or introduce new ones.

It does however require 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 must 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 (SWIFT)

B.9.1 Overview

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team based study utilising 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, organisation 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, organisations 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. Typically a team or more than 4 and less than 20 is most efficient.

B.9.4 Process

The general process followed is that:

1) 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;
2) At the workshop the external and internal context to the item, system, change or situation and the scope of the study are discussed and agreed;
3) The facilitator asks the participants raise and discuss:
    - Known risks and hazards;
    - Previous experience and incidents;
    - Known and existing controls and safeguards;
    - Regulatory requirements and constraints.
4) 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;
5) Risks are summarised and the team considers controls in place;
6) The description of the risk, its causes, consequences and expected controls are confirmed with the team and recorded;
7) The team considers whether the controls are adequate and effective and agree a statement of risk control effectiveness. If this is less that satisfactory, the team further risk treatment tasks and potential controls are defined;
8) During this discussion further 'what-if' questions are posed and the process is repeated for to identify further risks;
9) The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss;
10) 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

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 include:

- Is widely applicable to all forms of physical plant or system, situation or circumstance, organisation or activity;
- It requires 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 the likelihood of positive consequences;
- Involvement in the workshop by those who are accountable for existing controls and 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 prioritise 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 include:

- It requires an experienced and capable facilitator to be efficient;
- Careful preparation is required so that the workshop teams' 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.9.7 Comparisons and Links

Like most 'top-down' type risk identification type techniques, SWIFT allows the major risks to be quickly identified;

Often SWIFT can be used at an outline level to identify sub-systems and components that can be subjected to more detailed analysis using other methods such as HAZOP, FTA or FMECA.

Brainstorming and normal 'what-if' types of techniques are similar in approach. However, the use of a prompt system acts to ensure that the risk identification is comprehensive. Checklist based methods are also similar but the SWIFT prompt system is normally only seen and used by the facilitator and the discussion is not 'constrained' by the list.

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 is often used in conjunction with other approaches. In general terms it consists of defining a simplified 'model' of a real system and using the model to consider what might happen given various possible future developments.

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 likelihood of such changes but can consider consequences and help organisations 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 likelihood 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 organisation.

B.10.3 Inputs

The requirements for a scenario analysis are 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.

Informal scenario analysis has been used by risk analysts in a number of different ways, including to gain information about exposure; as a means of sensitivity analysis; and to set boundaries. These informal applications have provided information for scoping analyses.

One way of modelling a more formal scenario analysis process is to compare it to the steps of the risk management process as shown in the table below.

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 require 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 drive 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 now written for each scenario that tells how you might move from here and now to the subject scenario. The stories may include plausible details that add value to the scenarios.

The scenarios can now 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 likelihood 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 likelihood of each scenario occurring.

Risk management process	Scenario analysis process
Communicate and consult	Identify and communicate with stakeholders and t establish a team to be involved in the analysis
Describe the context (external, internal and risk management). Establish the terms of reference for the project. Identify criteria for analysis and evaluation.	Establish the key question under consideration. This may be a new product, service or activity that will require considerable investment. Describe the internal context that is driving the key question. Identify critical success factors
Identify risks	Identify changes that might occur including the factors or trends that might change stakeholder behaviour (regulatory, demographics, etc)
Analyse risks	Analyse and rank the factors in terms of importance and uncertainty. Map the factors against each other to help show, for example, four possible scenarios. Select the most likely scenarios (perhaps three) and elaborate on them with subtleties in a plausible story that shows how each scenario might come to pass.
Evaluate risks	Compare each scenario back with your key question. What vulnerabilities does each show up? Does the proposal look good under all or just one scenario?
Treat risk	Can the key question or proposal be adapted to make it more robust under each scenario? What leading indicators are available to show that change is indeed occurring? Such indicators may be crucial to responding earlier and so gaining advantage or opportunity.
Monitor and review	Monitor the chosen leading indicators. Keep the internal context and stakeholders under review in case unforeseen change occurs.

Table B.2The place of scenario analysis in the risk management process

B.10.5 Outputs

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

B.10.6 Comparisons and Links

Scenario analysis is a way of considering what might happen in the future by means of a story line. Once the scenario of the future is defined potential events could be displayed in a format similar to an event tree.

B.10.7 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 likely 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 (dependent on state of knowledge), 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 recognised as such.

B.11 Business Impact Analysis (BIA)

B.11.1 Overview

The business impact analysis, also known as business impact assessment, 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. Specifically, the BIA provides an agreed understanding of:

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

B.11.2 Use

The BIA is used to determine the criticality and recovery timeframes of processes and supporting resources (people, equipment, ICT) 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

- An understanding of 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 The 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, confirm the key processes and outputs of the organization to determine the criticality of the processes;
- Determine the consequences of a disruption on the identified critical processes in financial and/or operational terms, over defined periods;
- Identify the interdependencies with key internal and external stakeholders. This could include mapping the nature of the interdependencies through the supply chain;
- Determine the current available resources and the essential level of resources required to continue to operate at a minimum acceptable level following a disruption;
- Identify 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;
- Determine 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;
- Determine the recovery time objective(s) (RTO) for any specialized equipment or ICT infrastructure. The RTO represents the time within which the organization aims to recover the specialized equipment or ICT capability;
- Confirm 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:

- A priority list of critical processes and the associated interdependencies;
- Documented financial and operational impacts from a loss of the critical processes;
- Supporting resources required for the identified critical processes;
- Outage timeframes for the critical process and the associated ICT recovery timeframes.

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 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;
- Over realistic expectations of recovery requirements;
- Level of understanding of the organization's operations and activities.

B.12 Root cause analysis

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

Even though different methods can be used to perform the analysis, the basic steps in executing a 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;
- Perform a structured analysis to determine the root cause;
- Develop solutions and make recommendations;
- Implement the recommendations;
- Verify the success of the implemented recommendations.

Structured analysis methods may consist of one of the following:

- 5 Whys;
- 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 a RCA are:

- 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 a RCA may be:

- Required experts may not be available;
- Critical evidence may be destroyed in the failure or removed during cleanup;
- 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 Fault Modes and Effects Analysis (FMEA) and (FMECA)

B.13.1 Overview

Fault modes and effects analysis (FMEA) and Fault Modes and Effects and Criticality Analysis (FMECA) are techniques used to identify the ways in which components or systems can fail to perform to their design intent.

FMEA identifies:

- All potential failure modes of the various parts of a system;
- The effects these failures may have on the system;
- The causes 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 the combined influence of its likelihood of occurrence and the severity of its consequences. This analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

B.13.2 Use

FMEA /FMECA may be applied during the design, manufacture or operation of a system however changes are usually more easily implemented at the design stage.

FMEA/FMECA can be used to:

- Assist in selecting design alternatives with high dependability;
- Ensure that all failure modes and their effects on operational success have been considered;
- List potential failures and identify the severity of their effects;
- Provide a basis for planning testing and maintenance;
- Provide a basis for quantitative reliability and availability analyses.

It is most often applied to faults in components in physical systems but can also be used to identify human failure modes and effects.

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 requires information about the components of the system in sufficient detail for meaningful analysis of the ways in which each component can fail. This may include:

- Drawings of the system being analysed and its components;
- Drawings or information about the component of the system being analysed;
- Details of process and environmental parameters, which may affect operation;
- Operator interfaces;

- An understanding of the results of particular failures;
- Historical information on failures including failure rate data where available.

B.13.4 Process

The steps of FMEA are:

- Define scope and objectives of the study;
- Assemble the team;
- Understand the System to be subjected to FMECA;
- Break down of the system into its components or steps;
- 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 in the safe or unsafe direction?
  - How is the failure detected? What inherent provisions are provided 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 the combined influence of the severity of its consequences and its likelihood of occurrence;
- Define and Implement corrective actions to minimize the occurrence of the more significant failure modes;
- Compile a report that contains details of the system that was analysed , the way it was carried out, assumptions made in the analysis, sources of data and the results, including the completed worksheets and criticality matrices (if completed). Any recommendations for further analyses, design changes or features to be incorporated in test plans etc.;
- Reassess the system 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 and effects for each component (which may include the likelihood of failure). Information is also given on the causes of failure and the effect on the system as a whole.

The output from FMECA includes a qualitative risk assessment which indicates the criticality of the failure mode.

B.13.6 Strengths and limitations

The strengths of FMEA/FMECA are that they:

- Identify component fault 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 test programmes by highlighting key features to be tested;

- Assist in the definition of maintenance strategy.

The limitations are:

- 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 Comparisons

FMEA can be compared to HAZOP in being a technique for identifying risks based on a detailed consideration of separate components of a system. However FMEA considers the mechanisms whereby the component can fail whereas HAZOP considers how the intended result may not be achieved.

FMEA and FMECA can provide qualitative or quantitative information data for analysis techniques such as Fault Tree Analysis.

B.13.8 Reference

IEC 60812 “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.

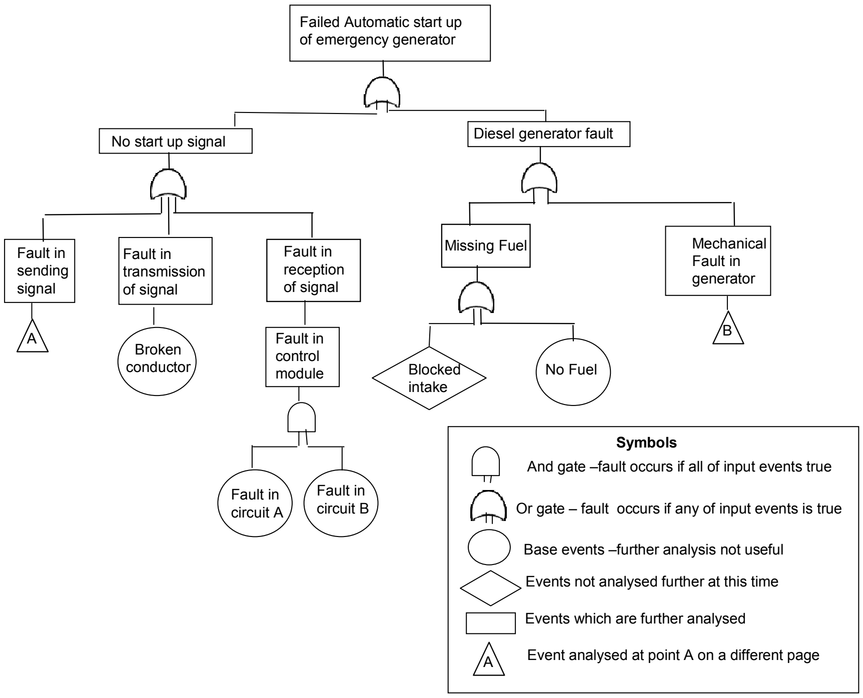

Failed Automatic start up of emergency generator
No start up signal
Diesel generator fault
Fault in sending signal
Fault in transmission of signal
Fault in reception of signal
Missing Fuel
Mechanical Fault in generator
A
Broken conductor
Fault in control module
Blocked intake
No Fuel
B
Fault in circuit A
Fault in circuit B
Symbols
And gate –fault occurs if all of input events true
Or gate – fault occurs if any of input events is true
Base events –further analysis not useful
Events not analysed further at this time
Events which are further analysed
A
Event analysed at point A on a different page

Figure B.3— Example of an FTA

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 likelihood 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. FTA is not based on detailed diagrams of the system like HAZOP and FMEA however a technical understanding of how the system can fail is needed.

For quantitative analysis failure rates for all basic events in the fault tree are required.

B.14.4 Process

The steps for developing a Fault Tree are:

- 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 fault modes leading to the top event are identified;

- Each of these causes/fault modes is analysed to identify how their failure could be caused;
- Following stepwise identification of undesirable system operation to successively lower system levels until further analysis becomes unproductive. In a hardware system this may be the component fault 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.

B.14.5 Outputs

The outputs from fault tree analysis are:

- 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 likelihood that each will occur;
- The likelihood of the top event (where this is required).

B.14.6 Strengths and Limitations

Strengths of FTA include:

- 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 (EG 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:-

- There is a high level of uncertainty in the calculated likelihood or frequency of the head event;
- In some situations causal events are not bounded and it can be difficult to ascertain whether all important pathways to the top event are included. (For example including

all ignition sources is an analysis of a fire as a top event. In this situation likelihood analysis is not possible);

- While human error can be included in a qualitative fault tree there is much disagreement on whether and how probabilities of error can be included in a quantified model. In general failures of degree or quality which often characterise human error cannot easily be included;
- A fault tree does not enable domino effects or conditional failures to be included easily.

B.14.7 Comparisons and Links

A fault tree diagram can be used qualitatively to display causes of a top event. In this case the “causes” may be possible contributory factors rather than faults with a known probability of occurrence. In this case the fault tree may become an alternative display technique for cause and effect analysis (B.17) or root cause analysis (B.10).

Tools such as Bow tie analysis (B.21) and cause consequence analysis (B.16) may incorporate fault trees as part of the causal analysis component.

B.14.8 References

IEC 61025. Fault Tree Analysis.

B.15 Event Tree Analysis (ETA)

B.15.1 Overview

ETA is an analysis technique, which is used to model a system qualitatively or quantitatively by identifying, possible pathways following an initiating even or failure and assessing the frequency of the various possible outcomes.

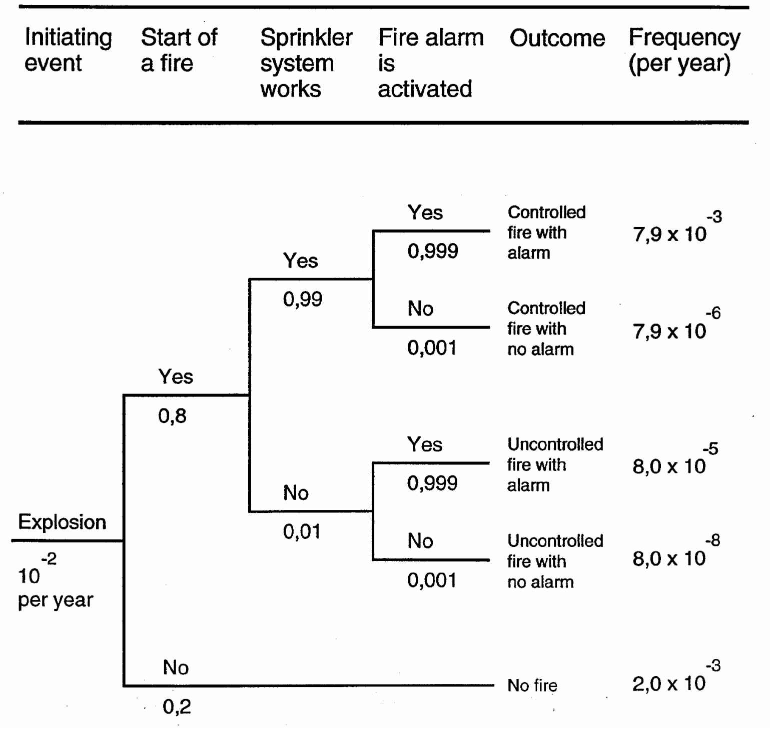


Figure B.4 — Event Tree

ETA is an inductive logic technique in which the basic question addressed is "what happens if...? “ 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 at any stage in the lifecycle 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.

B.15.3 Inputs

A list of appropriate initiating events;

Information;

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 likelihood of failure can be assigned to each line, with this conditional likelihood 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 likelihood of a sprinkler functioning is not the likelihood obtained from tests under normal conditions, but the likelihood of functioning under conditions of fire caused by an explosion.

Each path through the tree represents the likelihood 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 of ETA include:

- 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 Comparisons and Links

ETA is useful in identifying events which require further causal analysis using FTA (i.e. the top events of the fault trees). The likelihood of the corresponding top event can be substituted as the conditional likelihood of the failure line in the ETA.

In a “bow tie analysis” ETA represents the right hand side of the bow tie diagram, analyzing the consequences of the undesired event in the “middle of the bow tie”.

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

B.15.7 Strengths and limitations

Strengths of ETA include:

- 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.

Limitations include:

- In order to use ETA as part of a comprehensive assessment, all potential initiating events need to be identified. There is always a potential for missing some important initiating events. Furthermore, with event trees, only success and fault 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 leading to optimistic estimations of risk.

B.16 Cause Consequence Analysis

B.16.1 Overview

Cause Consequence Analysis is a combination of fault tree and event tree analysis which starts from a critical event and identifies all relevant causes and potential consequences.

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 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.

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

B.16.3 Inputs

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

B.16.4 Process

Figure B 2 shows a typical cause consequence analysis

Steps of construction are:

1) Identify the critical (or initiating) event (equivalent to the top event of a fault tree and the initiating event of an event tree);
2) Develop and validate the fault tree for causes of the initiating event as described in section B.14. (The same symbols are used as in conventional Fault tree analysis);
3) 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;
4) 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;

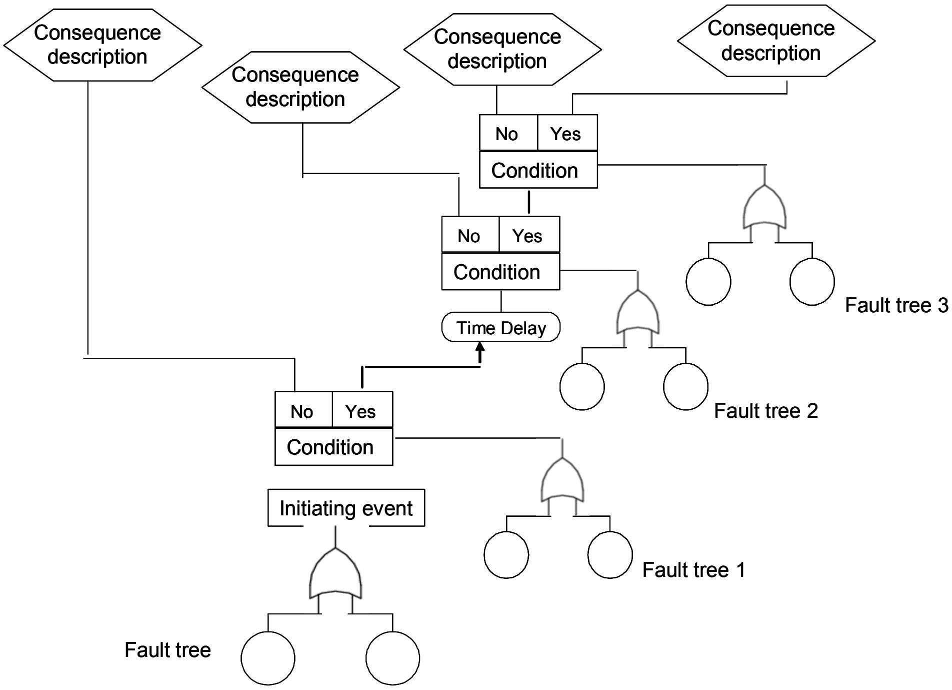


Figure B.5 — Cause/Consequence Analysis

5) Construct fault trees for the conditions as required;
6) 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 must be dealt with prior to calculation.

B.16.5 Outputs

A diagrammatic representation of how a system may fails 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

Strengths of Cause consequence analysis are the same strengths 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 trees and event trees both to construct and in the manner in which dependencies must be dealt with during quantification.

B.16.7 Comparisons and links

The method combines fault trees and event trees in a manner that overcomes the limitations of these techniques with respect to representing sequential events

B.17 Cause-and-effect analysis

B.17.1 Overview

Cause-and-effect analysis is a structured method to identifying 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 section B.14.7)

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.

Cause and effect analysis can be used as a method in performing root cause analysis (see paragraph B.17).

B.17.3 Inputs

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

The basic steps in performing a cause-and-effect analysis consist of:

- Establish the effect to be analyzed 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 may be 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.

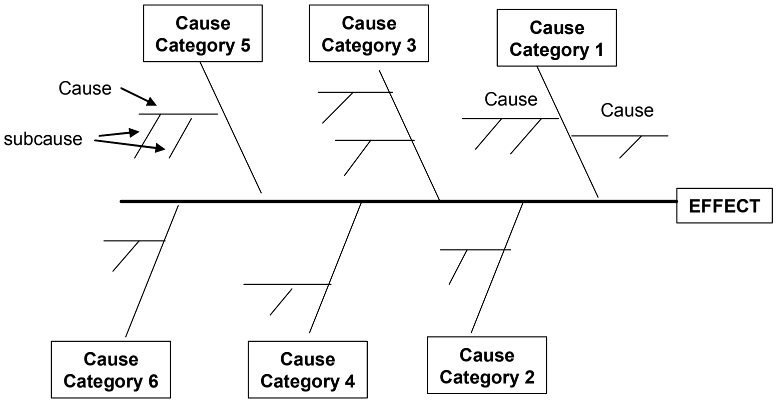


Figure B.6 — Ishikawa or Fishbone Diagram

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 faults with a known probability of occurrence

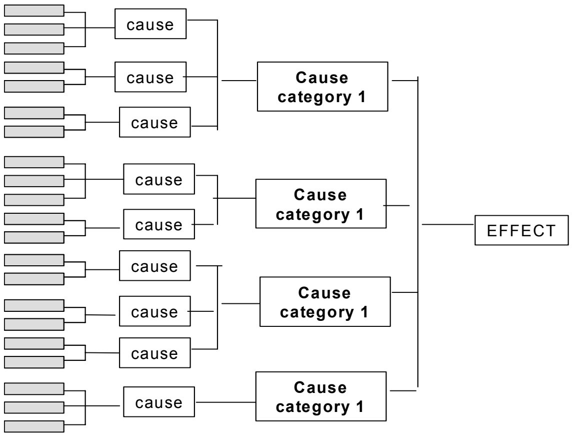


Figure B.7 —Tree Formulation of Cause and Effect Analysis

Cause and effect diagrams are usually used qualitatively. It is possible to assume the probability of the problem is 1 and assign probabilities to the 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 Outputs

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;
- Identifies areas 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 may be:

- 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 cause 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 cause 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 of 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 reduces risk to a tolerable level or is adequate.

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. It may be used semi quantitatively 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) as required by IEC61508 and IEC61511

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

Basic information on risks including hazards, causes and consequences such as provided by a PHA.

Information on controls in place or proposed.

Probabilities for initiating events, protection layer failures, measures of consequence and a definition of tolerable risk.

B.18.4 Process

LOPA is carried out using a team of experts:

- initiating causes for an undesired outcome are identified and data is sought on their probabilities and consequences;
- A single cause consequence pair is selected;
- The Scenario risk is estimated by combining the frequency of the initiating event and the severity of unmitigated consequences;
- Layers of protection which prevent the cause proceeding to the undesired consequence are identified and analysed for their effectiveness;
- Independent protect layers (IPL) are identified (not all layers of protection are IPLs);
- The initiating event frequency 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) Orders of magnitude are used for frequencies probabilities and consequences;
- The combined effect of protection layers 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 initiating 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 Outputs

Recommendations for where further controls are required and the effectiveness of these controls in reducing risk.

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;
- If LOPA is to be quantified the layers of protection must be independent from each other and from the initiating event (i.e. no 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.19 Decision Tree Analysis

B.19.1 Overview

A decision tree 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.

B.19.3 Inputs

A project plan with decision points.

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 likelihood 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

A logical analysis of the risk of different options that may be take to help make and justify decisions.

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 likelihood that problems will develop sufficiently to become serious can be small. Sometimes, however, human action will be the only defence to prevent an initial fault 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 likelihood of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

B.20.3 Inputs

Information to define tasks that people must 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 likelihoods 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 Outputs

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 likelihood 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.

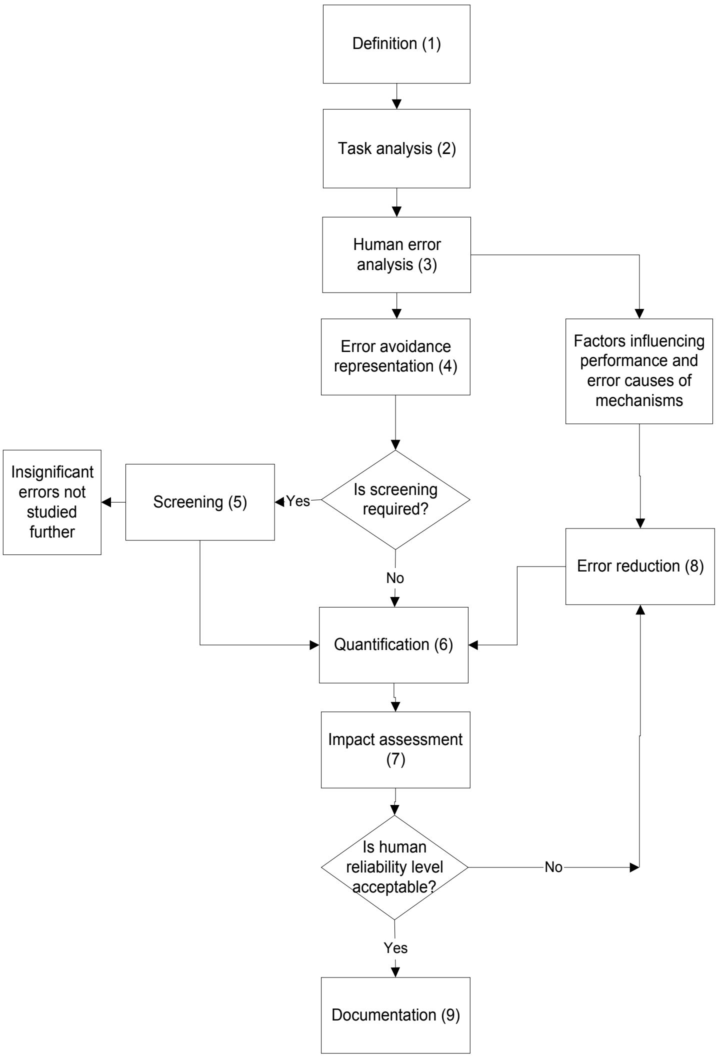


Figure B.8 — Human Reliability Assessment

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 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.

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

B.21.3 Input

An understanding of causes and consequences of a riskand the barriers and controls which may prevent or stimulate it.

B.21.4 Process

Risks are identified;

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

Causes which lead to consequences are listed

Lines are drawn between each cause and the consequence forming the left hand side of the bow tie. Factors which may lead to escalation may be identified and included in the diagram;

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 consequences

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 to each potential consequence;

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;

Some level of quantification of a bow tie diagram may be possible where pathways are independent. The likelihood 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 done using FTA and ETA.

B.21.5 Output

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

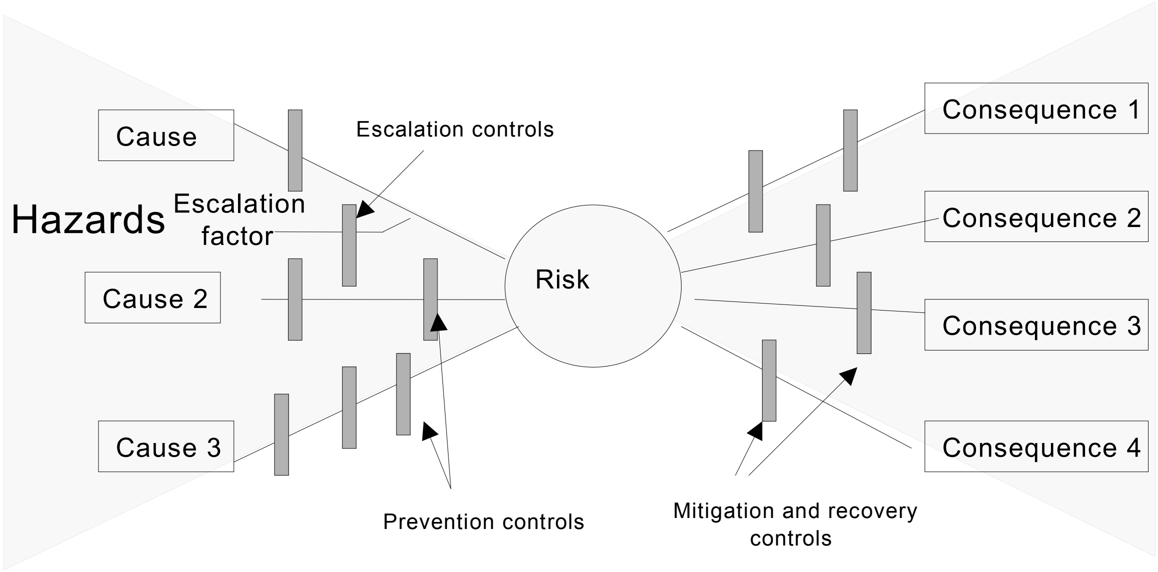


Figure B.9 — Bow-Tie diagram for unwanted consequences

B.21.6 Strengths and Limitations

Strength of Bow tie analysis:

- It is simple to understand and gives a clear pictorial representation of the problem;
- It focuses attention on barriers 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 require a high level of expertise to use.

Limitations include:

- It cannot depict where multiple causes must 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 was initially developed for the commercial aviation industry in the late 1960s, ultimately resulting in the publication of the document, Air Transport Association's ATA Operator/Manufacturer Scheduled Maintenance Development (MSG-3), upon which the modern usage of RCM is based. 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.

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 be required 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 maintainability and is generally applied during the design and development phase and then implemented during operation and maintenance.

B.22.3 Inputs

Successful application of RCM requires 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 similar to failure mode, effect and criticality analysis (FMECA) but some differences in methodology and intent.

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. Functional failures that may result are then identified for equipment and components associated with those functions.

Risk analysis consists of estimating the frequency of each failure without maintenance being done. This can be quantitative using a reliability technique such as Weibull analysis (see IEC 61649) or accessing failure databases compiled by industry. Semi-quantitative data may be developed based on actual experience or field data. Consequences are established by defining failure effects and criticality applicable to the situation.

A risk matrix that combines failure frequency and criticality allows categories of risk exposure 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 Outputs

Definition of maintenance tasks such as condition monitoring. scheduled restoration, scheduled replacement, failure-finding or no preventive maintenance. Other possible actions that can result from the analysis are results such as redesign, changes to operating or maintenance procedures or additional training. Task intervals and required resources are then identified.

B.22.6 References

Details regarding the use and application of RCM are provided in IEC 60300-3-11.

B.23 Sneak Analysis (Sneak Circuit Analysis)

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 1960's for NASA to verify the integrity and functionality of their designs. Sneak Circuit Analysis was a useful tool to discover 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 is the term used to describe an increased scope of Sneak Circuit Analysis. Sneak Analysis includes and far exceeds the coverage of Sneak Circuit Analysis. Sneak Analysis 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, etc. into a single analysis saving time and project expenses.

B.23.3 Inputs

Sneak Analysis is unique from the design process in that it uses different tools (network trees, forests, and clues) 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 Outputs

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. Four categories of sneak circuits are:

1. Sneak Paths - Unexpected paths along which current, energy, or logical sequence flows in an unintended direction;
2. Sneak Timing - Events occurring in an unexpected or conflicting sequence;
3. Sneak Indications - Ambiguous or false displays of system operating conditions that may cause the system or an operator to take an undesired action;
4. 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 be:

- 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 is unsuitable to adequately analyse the system. The method can be extended to more complex systems by employing higher order Markov chains and is only restricted by the model, mathematical computations, and the assumptions.

The Markov analysis process is a quantitative techniques 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; and
- 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 Inputs

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 which will be defined as states S1, S2, S3 respectively. Each day, the system exists in one of these three states. The following table shows the probability that tomorrow, the system is in state Si where i can be 1, 2 or 3.

Table B.3 — 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, the arrows represent the transition together with the accompanying probability.

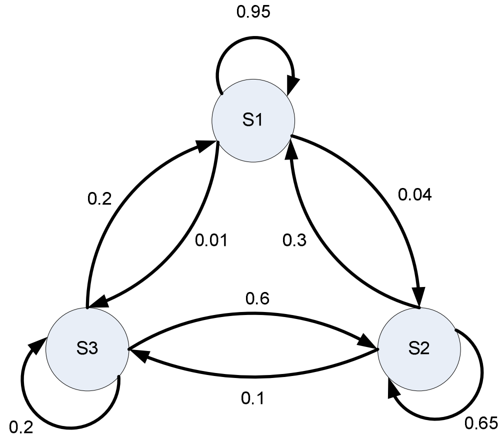


Figure B 10 — System Markov Diagram

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

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

P1 = 0.95P1 + 0.30P2 + 0.20 P3 …………………………….....(1)

P2 = 0.04P1 + 0.65P2 + 0.60P3…………………………………..(2)

P3 = 0.01P1 + 0.05P2 + 0.20P3……………………………………(3)

These 3 equations are not independent and will not solve the three unknowns. The following equation must be used and one of the above equations discarded.

1 = P1 + P2 + P3……………………………………(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.

For continuous events, 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 required.

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 are undergoing repair.

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

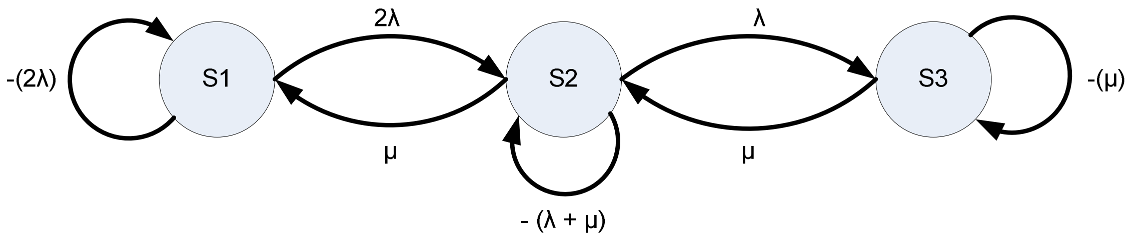


Figure B.11 — State Transition Diagram

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 Pi(t) be the probability of being in an initial state i at time t and

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

The transition probability matrix becomes:

Table B.4 — Final Markov Matrix

		Initial State		
		$P_1(t)$	$P_2(t)$	$P_3(t)$
	$P_1(t + \delta t)$	-2λ	μ	0
Final State	$P_2(t + \delta t)$	2λ	- (λ + μ)	μ
	$P_3(t + \delta t)$	0	λ	- μ

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:

$dP1/dt = -2\lambda\, P1(t) + \quad \mu\, P2(t)$

$dP2/dt = 2\lambda\, P1(t) \quad + \; -(\lambda + \mu)\, P2(t) \; + \; \mu\, P3(t)$

$dP3/dt = \quad \lambda\, P2(t) + \quad -\mu\, P3(t)$

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 4 (above) must also be used:

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

$$A = P1 + P2$$

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

B.24.5 Outputs

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 Risk Analysis.

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;
- Requires 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 References

IEC 61165 FDIS (2-2006) - Application of Markov techniques.

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 it can be evaluated by describing the input uncertainties and running a number of simulations in which the inputs are sampled to represent possible outcomes. 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 likelihood of values in that range for quantitative measures of a system such as cost, duration, throughput, demand and similar measures.

B.25.3 Inputs

A clear understanding of the model, the types of inputs, the sources of uncertainty that are to be represented and the required output. It is advisable build models from the top down and 'grow' complexity as opposed to commencing with a model of high complexity as this tends to focus attention on the most important areas and avoids effort being devoted to unimportant issues.

B.25.4 Process

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.5 — Simulation Data

	Item 1		Item 2		
Simulation Number	Random Number	Functions?	Random Number	Functions?	System
1	0,577243	YES	0,059355	YES	1
2	0,746909	YES	0,311324	YES	1
3	0,541728	YES	0,919765	NO	1
4	0,423274	YES	0,643514	YES	1
5	0,917776	NO	0,539349	YES	1
6	0,994043	NO	0,972506	NO	0
7	0,082574	YES	0,950241	NO	1
8	0,661418	YES	0,919868	NO	1
9	0,213376	YES	0,367555	YES	1
10	0,565657	YES	0,119215	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 0,9799 was achieved after 20 000 iterations which took less than a few seconds on a standard spreadsheet.

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 randomiser to derive a time of failure (exponential, weibull, or other suitable distribution) and building in repair times.

In general, Monte Carlo simulation may be applied to any system for which:

- A set of inputs interact to define an output;
- The relationship between the inputs and outputs can be expressed as logical and algebraic relationships;
- There is uncertainty in the inputs and so in the output.

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

B.25.5 Outputs

The output is dependent upon the result required. It 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 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 Monte Carlo analysis are:

- 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;
- Software is readily available and relatively inexpensive.

Limitations are:

- Solutions are not exact and depend upon the number of simulations;
- 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 adequate weight high consequence, low likelihood events and therefore not allow an organisation's risk appetite to be reflected in the analysis.

B.26 Bayesian Statistics and Bayes Nets.

B.26.1 Overview

Bayesian statistics is attributed to the Reverend Thomas Bayes who died in 1763. 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:

$$P(A|B) = \{P(A)P(B|A)\} / \sum_i P(B|Ei)P(Ei)$$

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 Ei is the ith event.

It is 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, Bayesian Networks). These nets use a graphical model to represent the probabilistic structure. The network is comprised of nodes that represent a random variable and arrows which link a parent node to a child node.

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 utilisation of structural relationships and data. Bayes Nets can be used to learn casual relationships to give an understanding about a problem domain and to predict the consequences of intervention.

B.26.3 Inputs

The inputs are similar to the inputs for a Monte Carlo Model. For a Bayes Net, examples of the steps to be taken are:

- 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 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 likelihood that if you do not have the disease, the test result is positive 10% of the time. The Bayes table has the following information:

Table B.6 — Bayes' Table Data

	PRIOR	LIKELIHOOD	PRODUCT	POSTERIOR
Have Disease	0,01	0,98	0,0098	0,09
No Disease	0,99	0,10	0,099	0,91
SUM	1		0,1088	1

Using Bayes rule the product is determined by combining the Prior and Likelihood. 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 form 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:

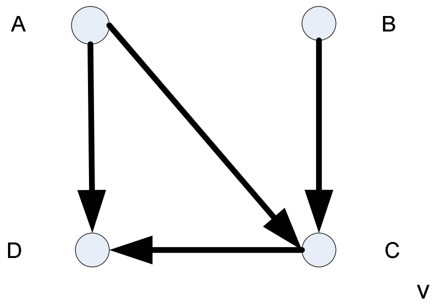


Figure B.12 — Sample Bayes' Net

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.7 — 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.8 — 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.9 — 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 normalised probabilities which sum to 1 as derived in the previous example (result rounded).

Table B.10 — 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 x 0,5 x 0,9 x 0,6 = 0,110	0,4
Y	N	0,4 x 0,9 x 0,9 x 0,4 = 0,130	0,48
N	Y	0,8 x 0,2 x 0,1 x 0,6 = 0,010	0,04
N	N	0,8 x 0,7 x 0,1 x 0,4 = 0,022	0,08

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

Table B.11 — 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; for example, 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 required 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:

Knowledge of priors is key. Software tools provide useful answers, but ‘rubbish in rubbish out’ is an important axiom to remember for Bayes Nets.

B.27 Risk Control Effectiveness

B.27.1 Overview

The risk identification and risk analysis steps in the risk management process should always consider the existing controls and their adequacy and effectiveness in order to estimate what is the level of residual risk. This requires Management to answer:

- What are the exiting 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 proper assurance processes, such as audit or control self assessment, have occurred and managers are informed of the outcome.

The property of risk control effectiveness (RCE) is used to give a relative assessment of actual level of control that is currently present and effective, compared with that which is reasonably achievable for a particular risk.

B.27.2 Process

Assessment of control effectiveness and adequacy by assurance providers is likely to be inhibited or compromised unless they can refer to adequate documentation that describes the control, its purpose and its design intent. Such validation also requires evidence of the operation of the control. Part of the control design process should include the creation of such documents and evidence and those accountable for controls are also accountable for preserving these records.

Expressing the level of effectiveness for a particular control or suite of related controls is technically very difficult and, in most cases, a high level of accuracy is not warranted. However, in all risk assessments it is valuable to express and record the measure of risk control effectiveness for the control suite as a whole so that judgements can be made on where effort is best expended in improving control through further or different risk treatment. The measure of Risk Control Effectiveness (RCE) can be used for this.

The table below shows a guide to estimating a qualitative rating for RCE.

Table B.12 — Sample qualitative RCE scale

RCE	Guide
Fully effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times.
Partially effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability.
Ineffective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. or Some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively.
Totally ineffective	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.
Not effective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

B.28 FN Curves

B.28.1 Overview

FN curves are a graphical representation for a specified hazard, of the likelihood of all 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.28.2 Use

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

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

B.28.3 Inputs

The required inputs are either (1), sets of the likelihood consequence pairs over a given period of time or (2), the output of data from a quantitative risk analysis giving estimated likelihoods for specified numbers of casualties or (3), data from both historical records and a quantitative risk analysis.

B.28.4 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 likelihood 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 may change over time.

B.28.5 Outputs

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.28.6 Comparisons and Links

The likelihood consequence pairs (fN pairs) may be derived from many forms of risk identification and analysis including quantitative risk analysis and quantitative modelling.

B.28.7 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 a form that allowed for comparisons between different types of risk.

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 pone 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.29 Risk Indices

B.29.1 Overview

A risk index 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 primarily used for risk analysis, though there is a component of risk evaluation.

B.29.2 Use

Indices are used for many different types of risk usually as a scoping device to determine which risks require further in depth and possibly quantitative assessment.

Indices are useful when they are well validated and the underlying models are understood. They can be used as a comparative tool, as long as the background conditions and assumptions are consistent.

B.29.3 Inputs

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 required to validate the index.

B.29.4 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 relativity. 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 must 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.29.5 Outputs

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.29.6 Comparisons and Links

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.29.7 Strengths and limitations

Strengths

- Indices can provide a good scoping tool for ranking different risks associated with a similar activity or similar location where there is a good understanding of the system. They allow multiple factors which affect the level of risk to be incorporated into a consideration of the level of risk

Limitations:

- If the process (model) and its output is 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.30 Consequence likelihood matrix

B.30.1 Overview

The consequence likelihood matrix is a means of combining qualitative or semi-quantitative ratings of consequence and likelihood 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.30.2 Use

A consequence likelihood 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 more detailed analysis or which risks need treatment first . It may be used as a screening tool to select which risks need not be considered further at this time. A form of consequence likelihood 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.30.3 Inputs

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

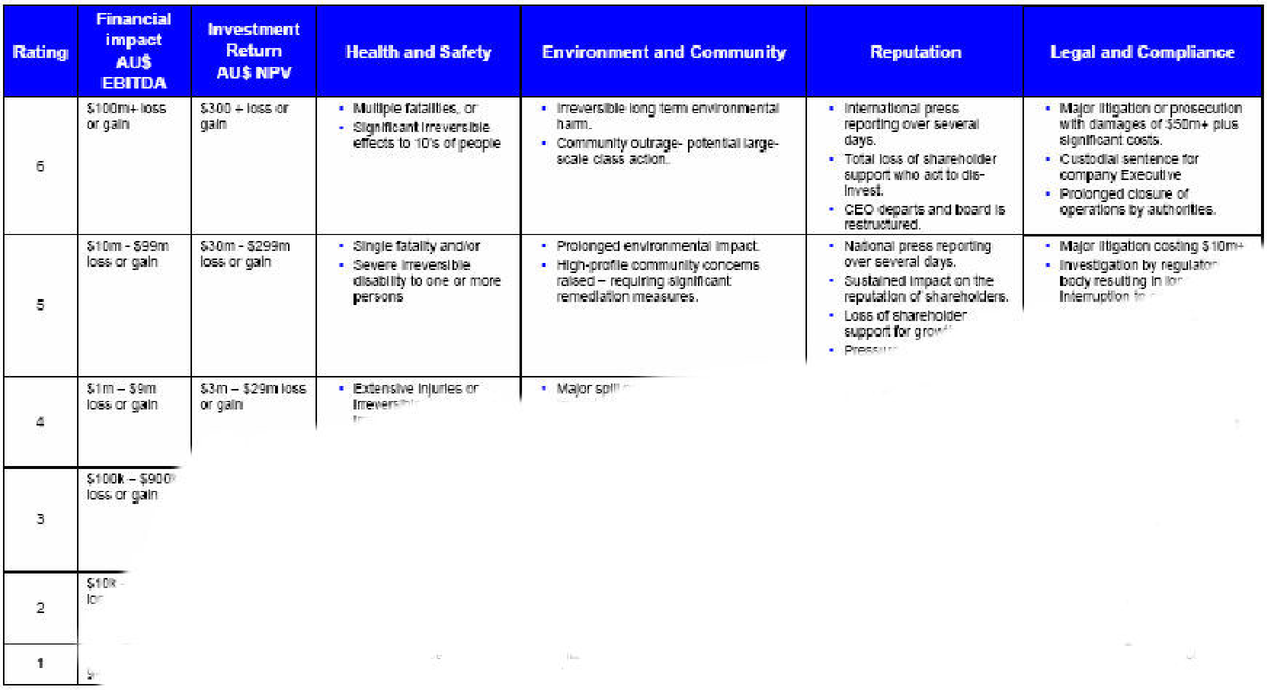
The consequence scale (or scales) should cover the range of different types of consequence to be considered (for example financial loss, safety, environment or other parameters depending on context) and should extend from the maximum credible consequence to the lowest consequence of concern. A part example is shown in Figure B6.

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

The likelihood scale may also have any number of points. Definitions for likelihood need to be selected to be as unambiguous as possible. If numerical guides are used to define different likelihoods then units should be given. The likelihood scale needs to span the range relevant to the study in hand, remembering that the lowest likelihood 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 B7.

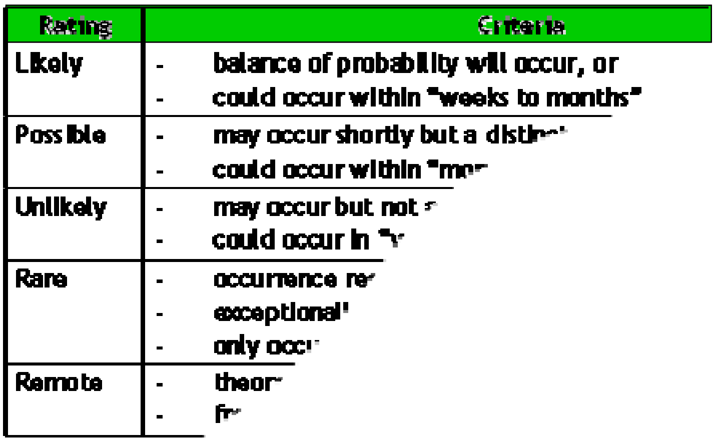
A matrix is drawn with consequence on one axis and likelihood on the other Figure B8 Shows part of an example matrix with a 6 point consequence and 5 point likelihood scales.

The risk levels assigned to the cells will depend on the definitions for the likelihood consequence scales. The matrix may be set up to give extra weight to consequences (as shown) or to likelihood, 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 grow ▪ Pressu	▪ Major litigation costing $10m+ ▪ Investigation by regulator body resulting in lo interruption fo
4	$1m – $9m loss or gain	$3m – $29m loss or gain	▪ Extensive injuries or irreversi	▪ Major spil		
3	$100k – $900 loss or gain					
2	$10k lo					
1						

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 occu
Remote	- theor - fr

Figure B 14 — Example of a Risk Ranking Matrix

Likelihood rating							
	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Consequence rating					

Figure B.15 — Part Example of a Likelihood Criteria matrix.

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

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

B.30.4 Process

To rank risks the user first finds the consequence descriptor that best fits the situation then defines the likelihood 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 likelihood. 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 as these pose the largest threat and are often of most concern to managers. In some cases it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important the likelihood relevant to the selected consequence is used and not the likelihood of the event as a whole.

B.30.5 Outputs

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

B.30.6 Strengths and limitations

Strengths include:

- Relatively easy to use;
- Provides a rapid ranking of risks into different significance levels.

Limitations:

- A matrix must 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 organisation;
- 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).

B.31 Cost benefit analysis

Cost benefit analysis is a fundamental method of risk evaluation where the costs of the risk treatment are compared with the benefits of the treatment. It is an implicit part of risk evaluation systems such as that for ALARP, as described above. It can also be used to differentiate between and decide on the best form of risk treatment. In this case the relative change in risk compared with the cost of achieving that change is compared for each option.

Cost benefit can be qualitative or quantitative or involve a combination of quantitative and qualitative elements,

In all cases both the direct and indirect benefits and costs should be identified and assessed in order to obtain a valid basis for decision making. Direct benefits are those which flow directly from the risk treatment while indirect or ancillary benefits are those which are coincidental but might still contribute significantly to the decision to treat a particular risk or not. 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 risk treatment and its implementation. Indirect costs are those additional, ancillary, and sunk costs associated with the risk treatment. Examples of indirect costs are loss of utility, distraction of management time or the diversion of capital away from other potential investments.

Benefits from not treating the risk i.e. the savings associated with taking the risk and which may be lost if the risk is treated should also be included

Cost benefit can involve the simple comparison of the costs and benefits associated with risk treatment (including risk toleration or risk retention). If there is uncertainty about the level of costs or benefits, either or both terms and be ‘weighted’. 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 obtain. This is the function of the net present value calculation.