

Standards Australia/Standards New Zealand (1995). Risk analysis of technological systems - Application guide Australian/New Zealand Standard.

Commonwealth of Australia

Copyright Act 1968

Notice for paragraph 135ZXA (a) of the *Copyright Act 1968*

Warning

This material has been reproduced and communicated to you by or on behalf of Charles Sturt University under Part VB of the *Copyright Act 1968* (the *Act*).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.

Interim
Australian/New Zealand Standard®

**Risk analysis of technological
systems—Application guide**

PUBLISHED JOINTLY BY:

STANDARDS AUSTRALIA
1 The Crescent,
Homebush NSW 2140 Australia

STANDARDS NEW ZEALAND
Level 10, Standards House,
155 The Terrace,
Wellington 6001 New Zealand

ISBN 0 7262 9905 7

PREFACE

This Interim Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee QR/5 on Reliability and Maintainability.

This Interim Standard is equivalent to IEC/CDV 56 (Sec) 410, *Risk analysis of technological systems—Application guide*; it is identical with and has been reproduced, with permission, from the subsequent Committee Draft prepared in March 1995 by Working Group 12 of the International Electrotechnical Commission (IEC) Technical Committee on Dependability, IEC/TC 56.

The objectives of this Interim Standard are to provide guidelines for selecting and implementing risks analysis techniques, primarily for risk assessment of technological systems; to ensure quality and consistency in the planning and execution of risk analyses and in the presentation of results and conclusions; and to satisfy an urgent need for a generic Standard which provides a basic model for analysis.

Risk analysis is a major part of, and provides a basis for, risk management, which is an iterative process consisting of well-defined sequential steps, often carried out by a multidisciplinary team. Therefore, a common methodology and understanding of the risk analysis process can provide a gateway across a range of industries and applications, including design, dependability, quality and safety of technological systems.

Committee QR/5 endorses the view of IEC/TC 56 that adoption of the model and definitions which this Interim Standard provides will contribute to mutual compatibility and harmonization of Standards.

For the purpose of this Joint Interim Standard, the IEC text should be modified so that the words 'Australian Standard', 'New Zealand Standard' or 'Joint Australian/New Zealand Standard' replace the words 'International Standard' wherever they appear. Also, the draft uses the more general term 'Fault' as an alternative to 'Failure', e.g. in Table 1, Fault Modes and Effects Analysis (FMEA).

Standards Australia and Standards New Zealand invite comments on this Interim Standard from persons and organizations concerned with this subject. The date of expiry for comment is 5 September 1997, at which time this Interim Standard will be confirmed, withdrawn or revised in the light of public comment.

During the life of this document the Joint Standards Australia/Standards New Zealand Committee will monitor all comment or field data as it is received.

Attention is drawn to the fact that this document is an Interim Standard and should be regarded as a developmental Standard and liable to future alteration.

© Copyright – STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Users of Standards are reminded that copyright subsists in all Standards Australia and Standards New Zealand publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia or Standards New Zealand may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia or Standards New Zealand. Permission may be conditional on an appropriate royalty payment. Australian requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia. New Zealand requests should be directed to Standards New Zealand.

Up to 10 percent of the technical content pages of a Standard may be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia or Standards New Zealand.

Inclusion of copyright material in computer software programs is also permitted without royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia or Standards New Zealand at any time.

CONTENTS

	<i>Page</i>
Introduction	1
1. Scope	1
2. References	2
3. Definitions	3
4. Risk analysis concepts	4
4.1 Objective and basic concepts of risk analysis	4
4.2 Risk management and risk categorisation	5
4.3 Application of risk analysis during life cycle phases	5
5. Risk analysis process	6
5.1 Overview	6
5.2 Scope definition	7
5.3 Hazard identification and initial consequence evaluation	8
5.4 Risk estimation	8
5.5 Analysis verification	11
5.6 Documentation	11
5.7 Analysis update	12
6. Audit	12
7. Risk analysis methods	12
7.1 General	12
7.2 Selection of methods	12
7.3 Methods of analysis	13
ANNEXES	23
A. Methods for analysis (informative)	23
A.1 Hazard and Operability (HAZOP) Study	23
A.2 Fault Modes & Effects Analysis (FMEA)	26
A.3 Fault Tree Analysis (FTA)	27
A.4 Event Tree Analysis (ETA)	30
A.5 Preliminary Hazard Analysis (PHA)	32
A.6 Human Reliability Assessment (HRA)	33

INTERIM AUSTRALIAN/NEW ZEALAND STANDARD

Risk analysis of technological systems—Application guide

Introduction

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

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

Risk analysis attempts to answer three fundamental questions:

What can go wrong? (by hazard identification)

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

What are the consequences? (by consequence analysis)

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

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

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

1. Scope

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

The standard contains guidelines for risk analysis, in the following main parts: Risk analysis concepts; Risk analysis process; Risk analysis methods.

This International Standard is applicable as:

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

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

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

2. References

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of the IEC and ISO maintain registers of currently valid International Standards.

IEC 50 (191): 1990 - International Electrotechnical Vocabulary - Chapter 191: Dependability and quality of service.

ISO/IEC Guide 51: 1990 (E): Guidelines for the inclusion of safety aspects in standards.

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

IEC 1025: 1990 - Fault tree analysis (FTA)

IEC 1078: 1991 - Analysis techniques for dependability - Reliability block diagram method

IEC 300-3-1: 1991 - Dependability management, Part 3: Application guide, Section 1: Analysis techniques for dependability: Guide on methodology.

IEC 300-2: XX: [Lifecycle document].

IEC XXXX: Functional safety of electrical/electronic/programmable electronic systems: Generic Aspects. Part 1: General requirements (65A(Secretariat)123).

IEC XXXX: [Human Factors document].

3. Definitions

For the purposes of this International Standard, the terms and definitions of IEC Publication 50(191) apply. In addition, the following terms and definitions apply.

- 3.1 **harm:** A physical injury or damage to health, property or the environment.
- 3.2 **hazard:** A source of potential harm or a situation with a potential for harm.
- 3.3 **hazardous event:** An event which can cause harm.
- 3.4 **hazard identification:** The process of recognising that a hazard exists and defining its characteristics.
- 3.5 **risk:** The combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.

NOTE: The concept of risk always has two elements: the frequency or probability with which a hazardous event occurs and the consequences of the hazardous event.
- 3.6 **risk analysis** The systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment. (See Figure 1).

Risk analysis is also sometimes referred to as probabilistic safety analysis, probabilistic risk analysis, quantitative safety analysis and quantitative risk analysis.
- 3.7 **risk assessment:** The overall process of risk analysis and risk evaluation. (See Figure 1).
- 3.8 **risk control:** The process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using the results of risk assessment as one input.
- 3.9 **risk estimation:** The process used to produce a measure of the level of risks being analysed. Risk estimation consists of the following steps: frequency analysis, consequence analysis and their integration.
- 3.10 **risk evaluation:** The process in which judgements are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects.
- 3.11 **risk management:** The systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. (See Figure 1).
- 3.12 **system:** A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The elements of this composite entity are

used together in the intended operational or support environment to perform a given task or achieve a specific objective.

4. Risk analysis concepts

4.1 Objective and basic concepts of risk analysis

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

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

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

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

- (a) systematic identification of potential hazards;
- (b) systematic identification of potential failure modes;
- (c) quantitative risk statements or ranking;
- (d) evaluation of possible modifications to reduce risk or achieve better dependability levels;
- (e) identification of the important contributors to risk and weak links in a system;
- (f) better understanding of the system and its installation;
- (g) comparison of risks to those of alternative systems or technologies;
- (h) identification and communication of risks and uncertainties;
- (i) help in establishing priorities for improving health and safety;
- (j) a basis for preventive maintenance and inspection to be rationalised;
- (k) post-accident investigation and prevention;
- (l) selection between alternatives such as different risk-reduction measures and technologies.

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

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

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

4.2 Risk management and risk categorisation

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

Hazards may be grouped into four general categories, namely:

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

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

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

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

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

4.3 Application of risk analysis during life cycle phases

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

- (a) Concept and Definition/Design and Development Phase:

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

5. Risk analysis process

5.1 Overview

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

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

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

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

5.1.1 Risk analysis personnel

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

5.2 Scope definition

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

- (a) describe the reasons for and/or the problems that originated the risk analysis. This will involve:
 - (i) formulating the objectives of the risk analysis based on the main concerns identified;
 - (ii) defining the criteria for success/failure of the system. The main concern may be some undesirable outcome (e.g. system failure, release of poisonous material) or it may be a condition which is potentially harmful.
- (b) define the system being analysed. The definition should include:
 - (1) a general description of the system;
 - (2) a definition of boundaries and interfaces with related systems both physical and functional;
 - (3) a definition of the environment;
 - (4) a definition of energy, materials and information flows across boundaries;
 - (5) a definition of the operating conditions covered by the risk analysis and any relevant limitations.

- (c) identify sources giving details of all the technical, environmental, legal, organisational, and human circumstances that are relevant to the activity and the problem being analysed. In particular any circumstances related to safety should also be described;
- (d) state the assumptions and constraints governing the analysis;
- (e) identify the decisions that have to be made, the required output from the study and the decision-makers.

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

5.3 Hazard identification and initial consequence evaluation

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

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

- (a) take corrective actions at this point to eliminate or reduce the hazards;
- (b) end the analysis here because the hazards or their consequences are insignificant;
- (c) proceed with risk estimation.

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

5.4 Risk estimation

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

Methods used in estimating risks are often quantitative though the degree of detail required in preparing the estimates will depend upon the particular application (see Section 7.2). However, full quantitative analysis may not always be possible due to insufficient information about the system or activity being analysed, lack of failure data, influence of human factors, etc. In such circumstances a comparative quantitative or qualitative ranking of risks by specialists knowledgeable in their respective field may still be effective. In cases where the ranking is qualitative, there should be clear explanation of all the terms employed

and the basis for all frequency and consequence classifications should be recorded. Where full quantification has been carried out it needs to be recognised that the risk values calculated are estimates and care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and analytical methods employed.

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

5.4.1 Frequency analysis

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

- (a) to use relevant historical data;
- (b) to derive event frequencies using analytical or simulation techniques;
- (c) to use expert judgement.

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

5.4.2 Consequence analysis

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

Consequence analysis should:

- (a) be based on the undesirable events selected;
- (b) describe any consequences resulting from the undesirable events;
- (c) take into consideration existing measures to mitigate the consequences together with all relevant conditions that have an effect on the consequences;
- (d) give the criteria used for completing the identification of the consequences;
- (e) consider both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the study;
- (f) consider secondary consequences, such as those associated with adjacent equipment and systems.

5.4.3 Risk calculations

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

- (a) predicted frequency of mortality or morbidity to an individual (individual risk);
- (b) frequency versus consequence plots (known as F-N Curves where F stands for frequency and N the cumulative number of people suffering a specified level of harm or the cumulative cost of damage) for societal risk;
- (c) the statistically expected loss rate in terms of casualties, economic cost or environmental damage;
- (d) the distribution of the risk of a specific damage level, presented as a contour plot, displaying levels of equal damage.

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

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

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

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

5.4.4 Uncertainties

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

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

5.5 Analysis verification

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

Verification should include the following steps:

- (a) check that the scope is appropriate for the stated objectives;
- (b) review all critical assumptions and ensure that they are credible in the light of available information;
- (c) ensure that the analyst used appropriate methods, models and data;
- (d) check that the analysis is repeatable by personnel other than the original analyst(s);
- (e) check that the results of the analysis are insensitive to the way data or results are formatted.

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

5.6 Documentation

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

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

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

5.7 Analysis update

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

6. Audits

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

7. Risk analysis methods

7.1 General

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

7.2 Selection of methods

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

- (a) it should be scientifically defensible and appropriate to the system under consideration;
- (b) it should provide results in a form which enhances understanding of the nature of the risk and how it can be controlled;
- (c) it should be capable of use by a variety of practitioners in a manner that is traceable, repeatable and verifiable.

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

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

- (a) the phase of the system's development. Early in system development less detailed methods may be used; they should be refined as more information becomes available;
- (b) the objectives of the study. The objectives of the analysis will have a direct bearing on the methods used. For example, if a comparative study between

different options is being undertaken, it may be acceptable to use fairly coarse consequence models for parts of the system not affected by the difference;

- (c) the type of system and hazard being analysed;
- (d) the potential level of severity. The decision on the depth to which analysis is carried out shall reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);
- (e) the manpower, degree of expertise and resources requirement. A simple method, well-done, will provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the analysis. Ordinarily the effort put into the analysis should be consistent with the potential level of risk being analysed;
- (f) the availability of information and data. Some methods require more information and data than others;
- (g) the need for modification/updating of the analysis. The analysis may need to be modified/updated in future and some methods are more amendable than others in this regard;
- (h) any regulatory and contractual requirements.

7.3 Methods of analysis

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

7.3.1 Hazard identification

Hazard identification involves a systematic review of the system under study to identify the type of inherent hazards that are present together with the ways in which they could be realised. Historical accident records and experience from previous risk analyses can provide a useful input to the hazard identification process. It needs to be recognised that there is an element of subjectivity in judgements about hazards, and that the hazards identified may not always be the only ones which could pose a threat to the system. It is important that the identified hazards are reviewed in the light of any relevant new data. Hazard identification methods fall broadly into three categories:

- (a) comparative methods, examples of which are checklists, hazard indices and reviews of historical data.
- (b) fundamental methods, that are structured to stimulate a group of people to apply foresight in conjunction with their knowledge to the task of identifying hazards by raising a series of "what if?" questions. Examples of this type of

methodology are Hazard and Operability (HAZOP) studies, and Fault Modes and Effects Analysis (FMEA).

- (c) Inductive reasoning techniques such as event tree logic diagrams.

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

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

7.3.2 Risk estimation

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

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

7.3.2.1 Frequency analysis

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

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

- (b) predict event frequencies using techniques such as fault tree analysis and event tree analysis. When historical data are unavailable or inadequate, it is necessary to derive event frequencies by analysis of the system and its associated fault modes. Numerical data on all relevant events, including equipment failure and human error from operational experience or published data sources, are then combined to produce an estimate of the frequency of the undesired events. When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the co-incidental failure of a number of different parts or components within the system. Simulation techniques may be required to generate frequencies of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties;
- (c) use expert judgement. There are a number of formal methods for eliciting expert judgement which make the use of judgements visible and explicit and provide an aid to the asking of appropriate questions. Expert judgements should draw upon all relevant available information including historical, system-specific, experimental, design, etc. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

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

7.3.2.2 Consequence analysis

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

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

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

Table 1

METHODS USED IN RISK ANALYSIS**A. Most Common Methods**

Method	Description and Usage	Reference
Event Tree Analysis	a hazard identification and frequency analysis technique which employs inductive reasoning to translate different initiating events into possible outcomes.	Annex A.4
Fault Mode & Effects Analysis & Fault Mode Effect & Criticality Analysis	a fundamental hazard identification and frequency analysis technique which analyses all the fault modes of a given equipment item for their effects both on other components and the system.	IEC 812 : 1985 - Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). Annex A.2
Fault Tree Analysis	a hazard identification and frequency analysis technique which starts with the undesired event and determines all the way in which it could occur. These are displayed graphically.	IEC 1025 : 1990 - Fault tree analysis (FTA) Annex A.3
Hazard & Operability Study	a fundamental hazard identification technique which systematically evaluates each part of the system to see how deviations from the design intent can occur and whether they can cause problems.	Annex A.1
Human Reliability Analysis	a frequency analysis technique which deals with the impact of people on system performance and evaluates the influence of human errors on reliability.	Annex A.6

Method	Description and Usage	Reference
Preliminary Hazard Analysis	a hazard identification and frequency analysis technique that can be used early in the design stage to identify hazards and assess their criticality.	Annex A.5
Reliability Block Diagram	a frequency analysis technique that creates a model of the system and its redundancies to evaluate the overall system reliability.	IEC 1078 : 1991 - Analysis techniques for dependability - Reliability block diagram method.

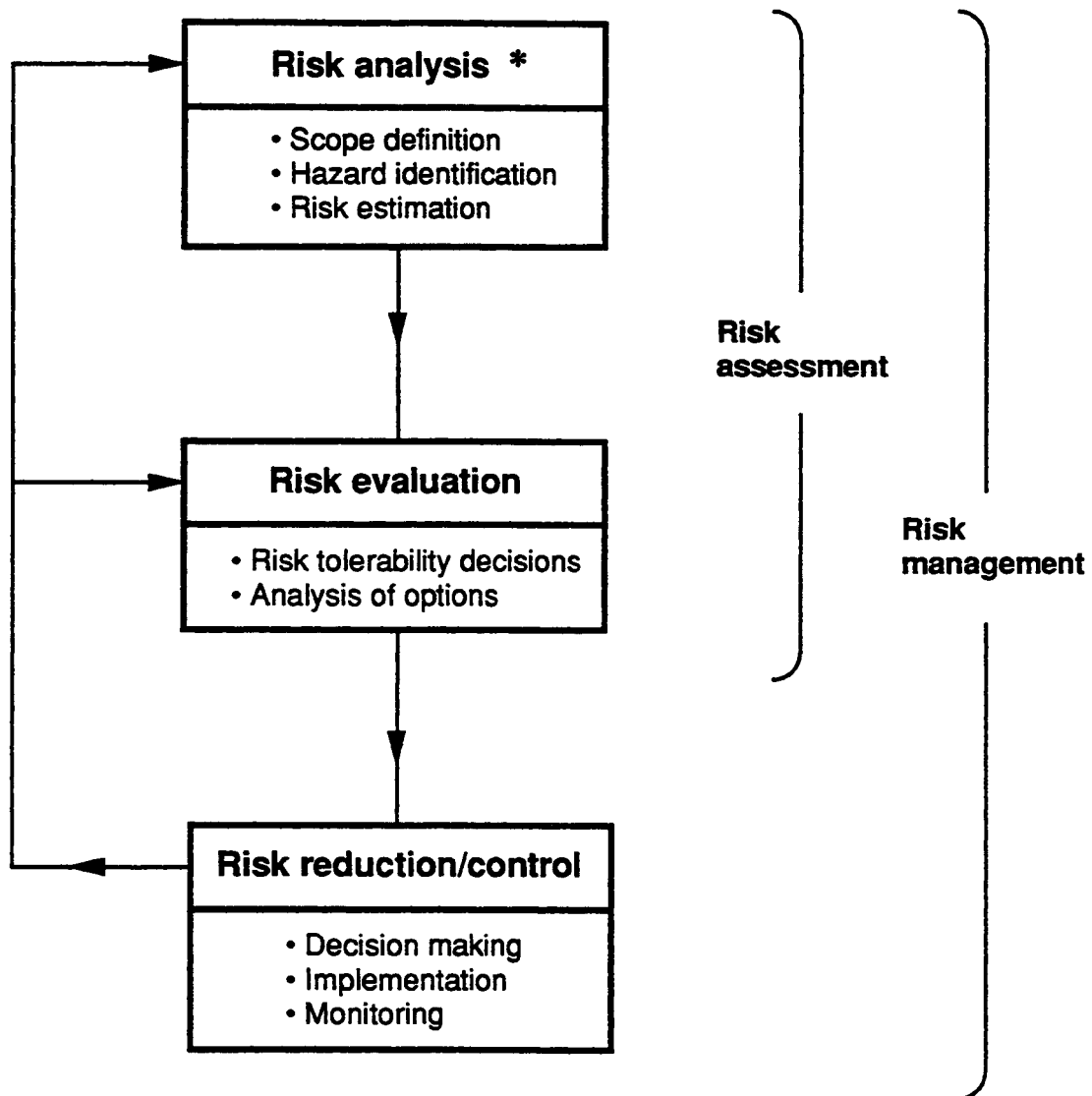
B. Additional Methods

Method	Description & Usage
Category Rating	a means of rating risks by the categories in which they fall in order to create prioritised groups of risks.
Checklists	a hazard identification technique which provides a listing of typical hazardous substances and/or potential accident sources which need to be considered. Can evaluate conformance with codes and standards
Common Mode Failure Analysis	a method for assessing whether the coincidental failure of a number of different parts or components within a system is possible and its likely overall effect.
Consequence Models	the estimation of the impact of an event on people, property or the environment. Both simplified analytical approaches and complex computer models are available.
Delphi Technique	a means of combining expert opinions that may support frequency analysis, consequence modelling and/or risk estimation

Method	Description & Usage
Hazard Indices	a hazard identification/evaluation technique which can be used to rank different system options and identify the less hazardous options.
Monte-Carlo Simulation and other simulation techniques	a frequency analysis technique which uses a model of the system to evaluate variations in input conditions and assumptions.
Paired Comparisons	a means of estimation and ranking a set of risks by looking at pairs of risks and evaluating just one pair at a time.
Review of Historical Data	a hazard identification technique that can be used to identify potential problem areas and also provide an input into frequency analysis-based on accident and reliability data et al.
Sneak Analysis	a method of identifying latent paths that could cause the occurrence of unforeseen events.

19
FIGURE 1

**A SIMPLIFIED RELATIONSHIP BETWEEN RISK ANALYSIS
AND OTHER RISK MANAGEMENT ACTIVITIES**



* the subject of this standard

FIGURE 2

THE RISK ANALYSIS PROCESS (SECTION 5)

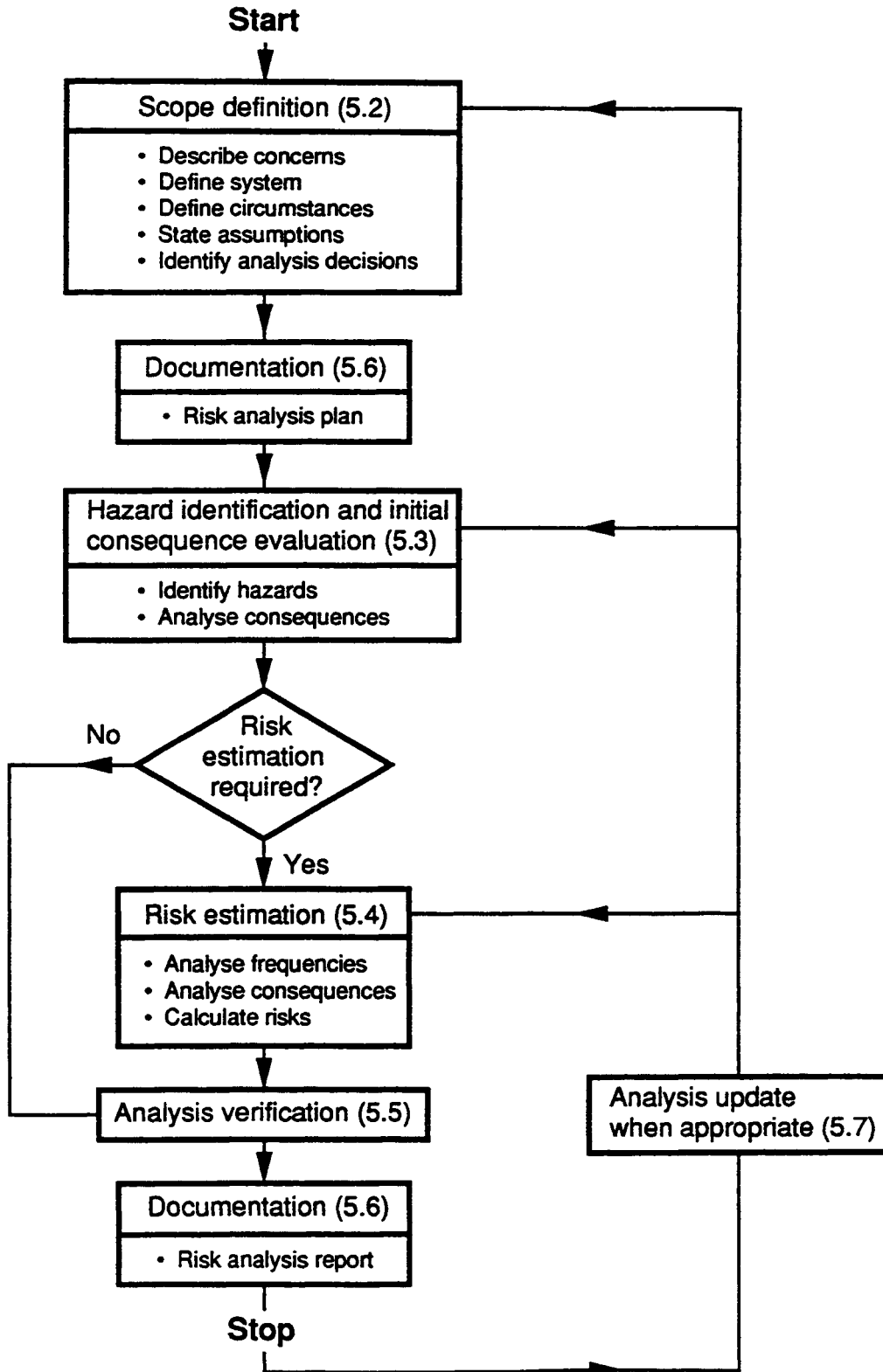


FIGURE 3

TYPICAL CONSIDERATIONS IN SELECTING TYPE OF ANALYSIS AND DEPTH OF STUDY

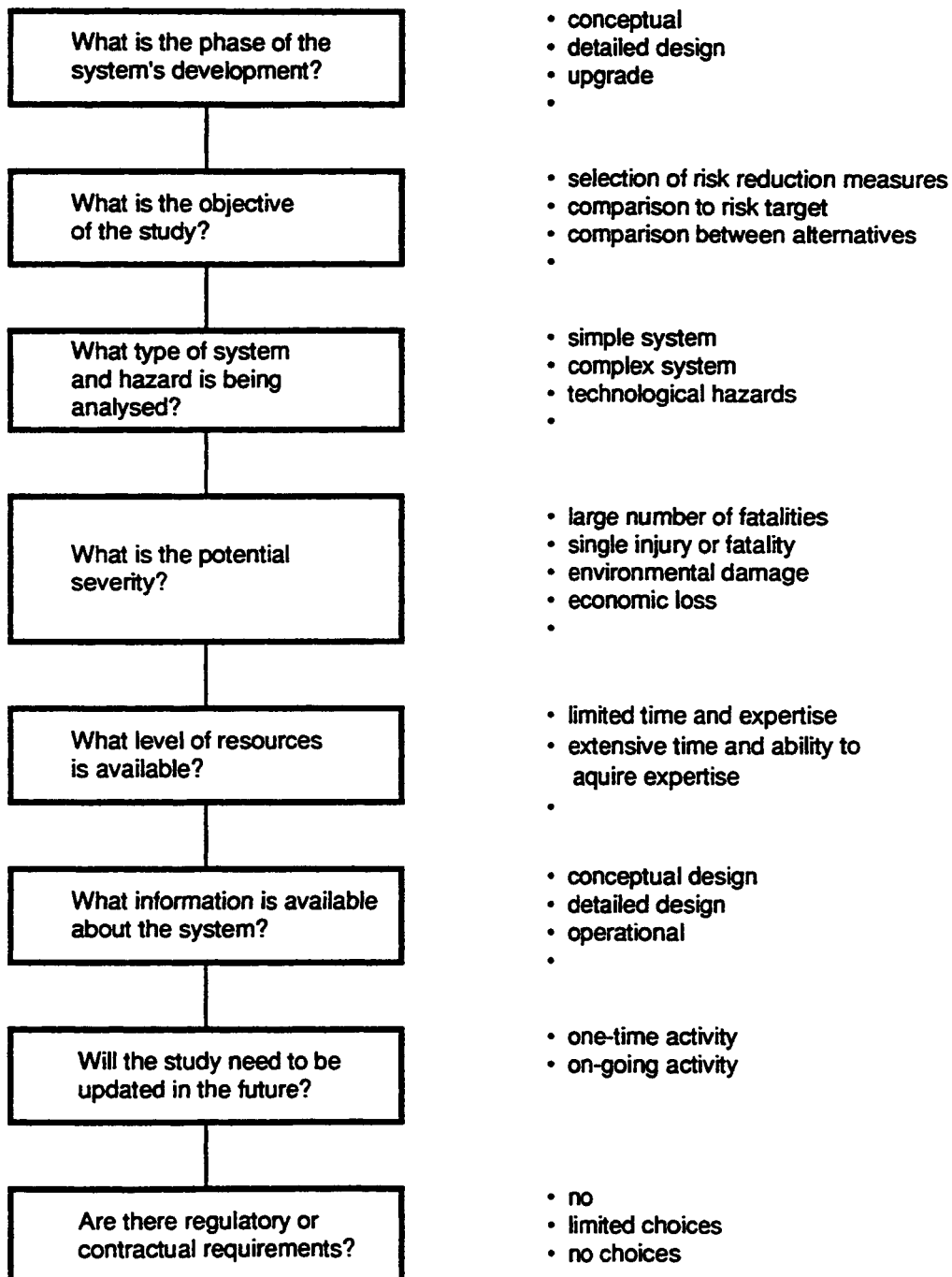


FIGURE 4

A RISK MATRIX

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

Where the risk classes are:

- H = HIGH RISK
 I = INTERMEDIATE RISK
 L = LOW RISK
 T = TRIVIAL RISK

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

- CATASTROPHIC** - Virtually complete loss of plant or system. Many fatalities.
MAJOR - Extensive damage to plant or system. Few fatalities.
SEVERE - Severe injury, severe occupational illness, significant damage to the plant or system.
MINOR - Minor injury, minor occupational illness or minor system damage.

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

ANNEX A (Informative)

Methods of Analysis

A.1 Hazard and Operability (HAZOP) Study

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

- (a) To produce a full description of the facility or process, including the intended design conditions;
- (b) To review systematically every part of the facility or process to discover how deviations from the intention of the design can occur; and
- (c) To decide whether these deviations can lead to hazards or operability problems.

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

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

A HAZOP II study involves the following steps:

1. Definition of the objectives and scope of the study, e.g hazards having only off-site impact or only on-site impact, areas of the plant to be considered, etc.
2. Assembly of a HAZOP study team. This team must consist of design and operation personnel with technical expertise to evaluate the effects of deviations from intended operation.
3. Collection of the required documentation, drawings and process description. This includes process flowsheets, piping and instrument drawings, equipment, piping and instrument specifications, process control logic diagrams, layout drawings, operating and maintenance procedures, emergency response procedures, etc.

4. Analysis of each major item of equipment, and all supporting equipment, piping and instrumentation, using documents collected in step 3. The process design intent is first defined, then, for each line and item of equipment, guide words (see Table A.1.1) are applied to process variables such as temperature, pressure, flow, level and chemical composition. (These guide words stimulate individual thought and induce group discussion).
5. Documentation of the consequences of any deviation from normal and highlights of those deviations which are considered hazardous and credible. In addition, an identification is made of means to detect and/or prevent the deviation. This documentation is usually done on HAZOP worksheets. A sample of such a worksheet for the guide word "Not, No" applied to "flow" is shown in Table A.1.2.

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

Table A.1.1

HAZOP II GUIDE WORDS	
Terms	Definitions
no or not	no part of the intended result is achieved (e.g. no flow)
more	quantitative increase (e.g. high pressure)
less	quantitative decrease (e.g. low pressure)
as well as	qualitative increase (e.g. additional material)
part of	qualitative decrease (e.g. only one or two components in a mixture)
reverse	opposite (e.g. backflow)
other than	no part of the intention is achieved, something completely different happens (e.g. flow of wrong material)

Table A.1.2

SAMPLE HAZOP II WORKSHEET FOR GUIDEWORD "NOT, NO"				
Guideword	Deviation	Possible Causes	Consequences	Action Required
Not, No	No flow	1. No feed material available	Reduced output polymer will be formed	a) Ensure good communication with operator b) Provide low level alarm on setting tank
		2. Pump fails (variety of reasons)	As for 1.	As for b)
		3. Line blockage or valve closed in error or control valve fails shut	As for A1. Pump will overheat	Install recirculation line on each pump

A.2. Fault Modes and Effects Analysis (FMEA)

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

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

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

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

FMEA (and FMECA) provide input to analyses such as fault tree analysis. As well as dealing with system components, they may be used to deal with human error. They can be used for both hazard identification and probability estimation (if only a limited level of redundancy is present in the system). Further details on both FMEA and FMECA are given in IEC 812: 1985.

A.3 Fault Tree Analysis (FTA)

FTA is a technique, which can be either qualitative or quantitative, by which conditions and factors that can contribute to a specified undesired event (called the top event) are deductively identified, organised in a logical manner and represented pictorially. The faults identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event. Starting with the top event, the possible causes or fault modes of the next lower functional system level are identified. Following stepwise identification of undesirable system operation to successively lower system levels will lead to the desired system level, which is usually the component fault mode. An example of a fault tree for an emergency generator is given in Figure A.3.1. A table of the most common fault tree symbols is given in Figure A.3.2.

FTA 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. This is a distinct advantage, although it may also lead to missing effects which are important elsewhere. 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 also makes the verification of the fault tree difficult.

FTA may be used for hazard identification, although it is primarily used in risk assessment as a tool to provide an estimate of failure probabilities or frequencies. Further details on FTA are given in IEC 1025: 1990.

Figure A.3.1

Fault tree example

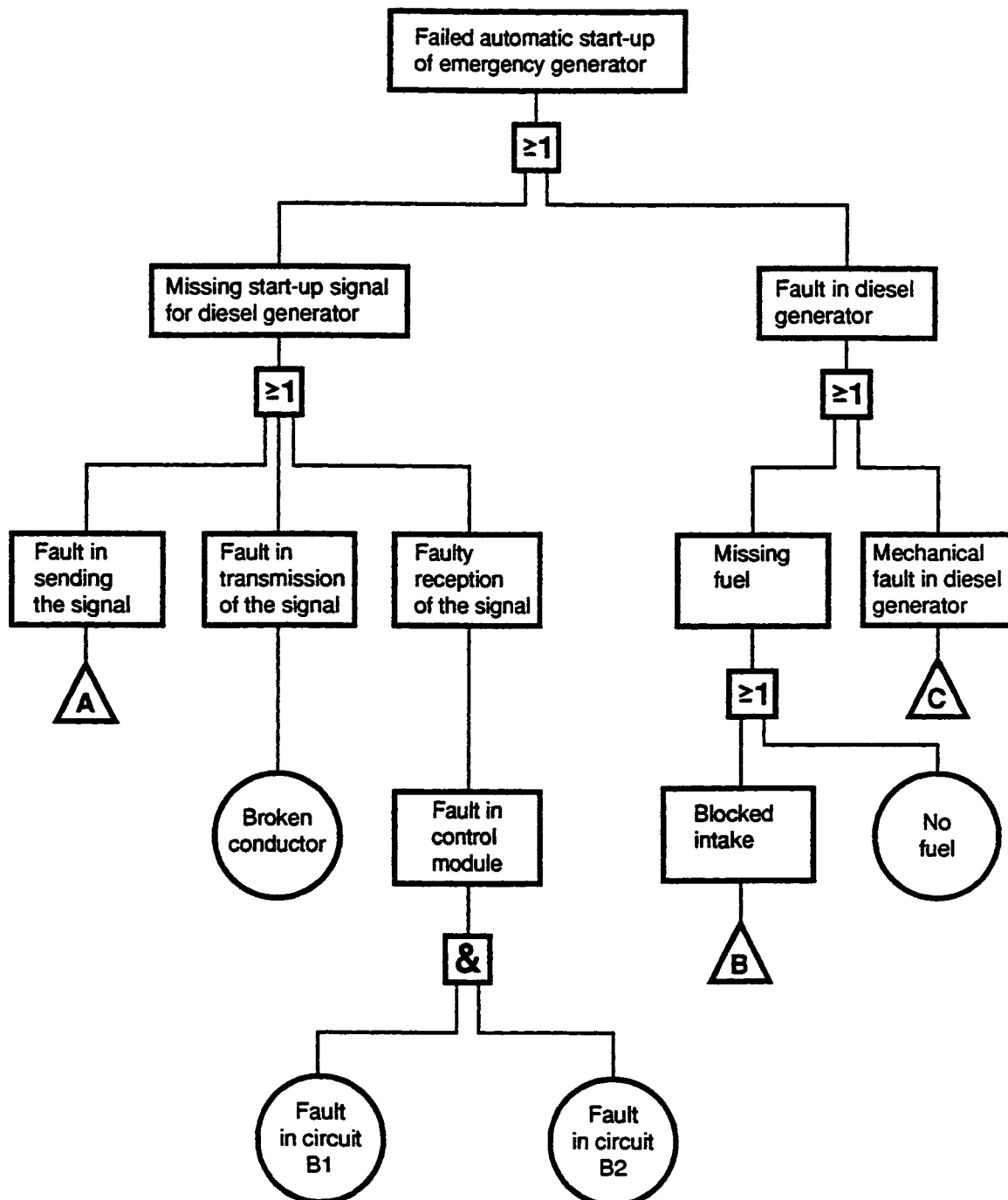

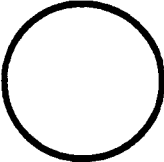





Figure A.3.2

Fault tree symbols *

Symbol	Function	Description
	Event description block	Name or description of the event, event code, and probability of occurrence (as required) shall be included within the symbol
	Basic event	Event which cannot be subdivided
	AND gate	Event occurs only if all input events occur simultaneously
	OR gate	Event occurs if any of the input events occur, either alone or in any combination
	Transfer-in	Event defined elsewhere in the fault tree

* Taken from IEC 1025: 1990 and used in Figure A.3.1. There are also alternative conventions for fault tree symbols in existence.

A.4 Event Tree Analysis (ETA)

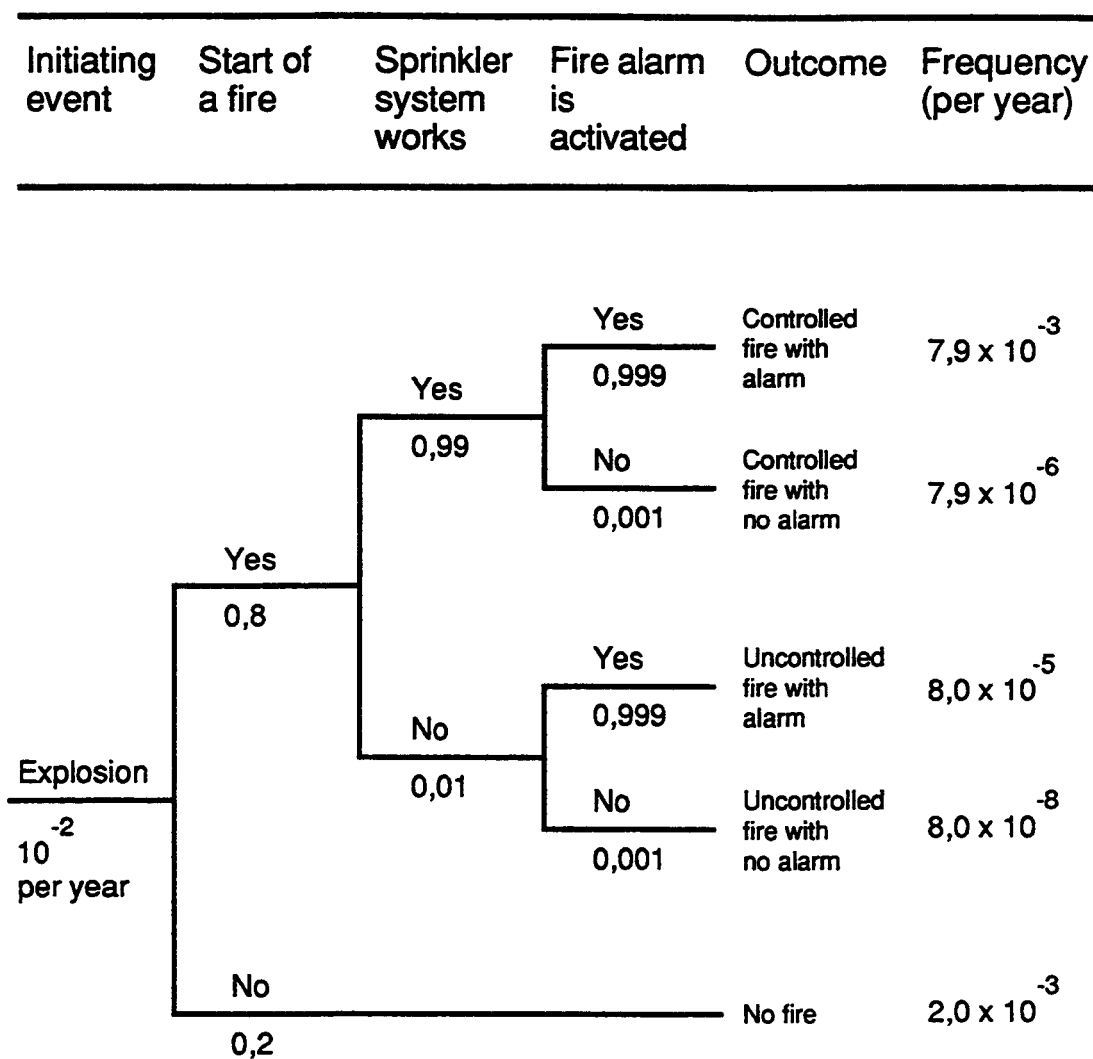
ETA is a technique, either qualitative or quantitative, which is used to identify the possible outcomes and if required, their probabilities, given the occurrence of an initiating event. ETA is widely used for facilities provided with engineered accident mitigating features, to identify the sequence of events which lead to the occurrence of specified consequences, following the occurrence of the initiating event. It is generally assumed that each event in the sequence is either a success or a failure. A simple event tree for a dust explosion is shown in Figure A.4.1, with probabilities included. Note that the probabilities on the event tree are conditional probabilities, e.g. the probability of the sprinkler functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under conditions of fire caused by explosion.

ETA is an inductive type of analysis in which the basic question addressed is "what happens if...?". It provides the relationship between the functioning or failure of various mitigating systems and ultimately the hazardous event following the occurrence of the single initiating event, in a clear way. ETA is very useful in identifying events which require further analysis using FTA (i.e. the top events of the fault trees). In order to be able to do a comprehensive risk assessment, all potential initiating events need to be identified. There is always a potential, however, for missing some important initiating events with this technique. 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.

ETA can be used both for hazard identification and for probability estimation of a sequence of events leading to hazardous situations.

Figure A.4.1

Example of an event tree for a dust explosion



A.5 Preliminary Hazard Analysis (PHA)

PHA is an inductive method of analysis whose objective is to identify the hazards, hazardous situations and events that can cause harm for a given activity, facility or system. 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. It can also be useful when analysing existing systems or prioritising hazards where circumstances prevent a more extensive technique from being used.

A PHA formulates a list of hazards and generic hazardous situations by considering characteristics such as:

- (a) materials used or produced and their reactivity
- (b) equipment employed
- (c) operating environment
- (d) layout
- (e) interfaces among system components etc.

The method is completed with the identification of the possibilities that the accident happens, the qualitative evaluation of the extent of possible injury or damage to health that could result and the identification of possible remedial measures. 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.

A.6 Human Reliability Assessment (HRA)

General

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

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 is often small. Sometimes however, human action will be the only defence to prevent an initial fault progressing towards an accident.

HRA identifies the various types of erroneous actions that can occur, including the following:

- (a) error of omission, a failure to carry out the required action;
- (b) error of commission, which may include the following:
 - (1) a failure to carry out the required action adequately;
 - (2) an action carried out with too much or too little force or without the required accuracy;
 - (3) an action carried out at the wrong time;
 - (4) an action (or actions) carried out in the wrong sequence;
- (c) extraneous action, an unrequired action carried out instead of or in addition to, the required action.

HRA also identifies error recovery opportunities, i.e. actions which can recover previous errors.

HRA is a hybrid discipline with researchers and practitioners generally coming from the domains of either reliability engineering or psychology and human factors.

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.

HRA may include the following steps:

1. Task analysis
2. Human error identification
3. Human reliability quantification.

Each step is further described below, and representative analysis methods are mentioned.

Task analysis and human error identification should usually start during the Concept and Definition Phase or early in the Design and Development Phase, and should be refined and updated during later stages of the system.

Task analysis (TA)

The objective of TA in the HRA process is to describe and characterise the task to be analysed in sufficient detail to perform human error identification and/or human reliability quantification. Task analysis may also be performed for other purposes, such as human machine interface evaluation or procedure design.

Human error identification (HEI)

This step identifies and describes possible erroneous actions in performing a task. Human error identification may include identification of possible consequences and causes of erroneous actions and suggestion of measures to reduce human error probability, improve opportunities for recovery, and/or reduce the consequences of erroneous actions. The results of HEI thus provide valuable input to risk management even if no quantification is performed.

Human reliability quantification (HRQ)

The objective of HRQ is to estimate the probability of correct task performance or the probability of erroneous actions. Some HRA techniques may also include steps to estimate the probability or frequency of specified undesired event sequences or undesired outcomes.

Further details on HRA are given in IEC XXXX: 19XX.