nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-21
ISBN 87-7893-071-5

Safety- and risk analysis activities in other areas than the nuclear industry

Igor Kozine, Nijs Jan Duijm
and Kurt Lauridsen

Risø National Laboratory, Roskilde
Denmark

December 2000

Abstract

The report gives an overview of the legislation within the European Union in the field of major industrial hazards and gives examples of decision criteria applied in a number of European countries when judging the acceptability of an activity. Furthermore, the report mentions a few methods used in the analysis of the safety of chemical installations.

Key words

Seveso directive, risk analysis, safety analysis, hazard identification techniques, decision criteria, chemical industry, off-shore industry

NKS-21
ISBN 87-7893-071-5

Klæbels Offset Tryk, 2001

The report can be obtained from
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde
Denmark

Phone +45 4677 4045
Fax +45 4677 4046
http://www.nks.org
e-mail: annette.lemmens@risoe.dk

SOS-1

Safety- and risk analysis activities in other areas than the nuclear industry

Igor Kozine, Nijs Jan Duijm, Kurt Lauridsen

Risø National Laboratory, Roskilde
December 2000

Contents

Preface

The present report has been written as part of the NKS/SOS-1 project with the purpose to inform the "Nordic nuclear community" about the status of safety- and risk assessment in other industrial areas than the nuclear one. The report informs about the methods used for analysis, the relevant legislation and acceptance criteria. It focuses on the situation in Europe, in particular within the European Union. The report is a compilation of information already existing, and extensive use has been made of text from some of the references.

1 Introduction

From early in the 20th century the process industry has clearly recognised the importance of the safety of their staff and of the public. In the early days careful investigation of accidents and the formulation of actions to prevent a recurrence achieved this. (Learning from experience). These lessons were incorporated into codes of practice. This approach still forms an important part of the industries' approach to safety improvement.

From the 1960's the increasing scale of operations and the introduction of new technology made it clear that a more analytical approach was required leading to the development of more searching methods such as HAZard and OPerability (HAZOP) which can be applied before a facility is put into operation. This technique is now an 'industry standard'. Leading companies use HAZOP as part of a series of Safety Reviews during the design process. Safety reviews are also carried-out at intervals on existing facilities handling hazardous materials. From the middle to late 70's the same detailed attention has been applied to protection of the environment.

In parallel with the identification of hazards came the requirement to predict their consequences. Early models used simple correlations; for example, an early correlation for predicting the effects of explosions related all explosions to an equivalent quantity TNT. Considerable work has been devoted to this aspect of risk assessment through theoretical work, large-scale experiments and the development of computer codes. Models are now available for the most important physical effects.

A number of major accidents in chemical factories, such as the Flixborough accident in 1974 and the Seveso accident in 1976 gave rise to new legislation in many countries and were part of the background for the European Community's formulation of the directive known as the Seveso directive.

2 Legislation within the European Union

Safety- and risk-related matters within the European Community (EC) are subject to consideration at three levels: (1) EC legislation, (2) European/international standardisation, and (3) socio-economic national entities.

EC directives define the "essential requirements", e.g. protection of health and safety, that must be fulfilled when goods are placed on the market or some industry is put into operation.

The European standards bodies (CEN, CENELEC and ETSI)[1] have the task of drawing up the corresponding technical specifications meeting the essential requirements of the directives, compliance with which will provide a presumption of conformity with the essential requirements. Such specifications are referred to as "harmonised standards". Compliance with harmonised standards remains voluntary, and manufacturers are free to choose any other technical solution that provides compliance with the essential requirements. This view is stated in the "New Approach" to technical harmonisation and standardisation (details can be found on the web page http://europe.eu.int/comm/enterprise/newapproach/standardization/index.html).

Standardisation as well as the regulation of technical risks is increasingly being undertaken at European or international level. The European legislator limits its role to the affirmation of overall objectives, and leaves it to the economic players to draw up the technical procedures and standards to specify in detail the ways and means of attaining them [1].

One of the pivot EC directives is Council Directive 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances (the Seveso Directive II) which is based on Article 174 (ex-Article 130s) of the EC Treaty. It is important to mention that,

[1] CEN – European Committee for Standardisation, CENELEC – European Committee for Electrotechnical Standardisation, and ETSI – European Telecommunications Standards Institute

according to Article 176 (ex-Article 130t) of the EC Treaty, Member States can maintain or adopt stricter measures than those contained in the Seveso II Directive.

The aim of the Seveso II Directive is two-fold. Firstly, the Directive aims at the prevention of major-accident hazards involving dangerous substances. Secondly, as accidents do continue to occur, the Directive aims at the limitation of the consequences of such accidents to man and the environment to ensure high levels of protection throughout the EC in a consistent and effective way. Industrial operators that use large amounts of dangerous substances must demonstrate that they have assessed the risks and are managing them. However, no corresponding procedures are contained in the Directive. As a result of difference of cultures in the Member States of the EU, a variety of such procedures is currently in use. These specific procedures and philosophies are developed by, what were called, socio-economic national entities.

Many countries have introduced requirements that new legislation and/or administrative regulations be subject to socio-economic analysis. In this respect there is a European and International mechanism of handling safety- and risk-related matters. So, the Organisation for Economic Co-operation and Development's (OECD) core objective on risk management is to support Member countries' efforts to develop national policies and actions, and, where appropriate, to develop and implement international risk management measures. In support of this objective, the OECD Risk Management Programme focuses on two areas: (1) developing methods and technical tools that can be used by OECD and Member countries to enhance their current risk management programmes; and (2) identifying specific chemical exposures of concern in Member countries and evaluating possible risk management opportunities [2].

Procedures exist for preparing risk assessments in most OECD countries as part of the OECD national risk assessment programme. In some cases, procedures are dictated by international requirements. For example, within the EU, Directive 93/67/EEC lays down common principles for assessing and evaluating risks to human health and the environment posed by new substances. Regulation (EC) No. 1488/94 lays down similar principles for the risks posed by existing substances. The recommended approach to risk assessment is set down in *Technical Guidance Document in Support of Commission Directive 93/67/EC on Risk Assessment of New Notified Substances* and *Directive and Commission Regulation (EC) No. 1488/94 on Risk Assessment of Existing Substance*s.

Under the EU procedures, risks are characterised by comparing effects with exposure and recommendations are made concerning the need for risk reduction or mitigation. The assessment process is designed to determine the risks associated with the 'reasonable worst-case scenario', the aim being to ensure that risks are not underestimated. The results are expressed as a risk/hazard quotient. In other countries, for example Canada and the US, the aim of the risk assessment phase is to prepare a fully quantified consequence analysis, presented as the probability of a particular effect given a specified level of exposure.

A number of Directives have been established to protect the health and safety of workers at work. The requirement in the European Framework Directive [3] that a risk assessment be undertaken is a considerable incentive in bringing about such a development. There is a set of individual directives (within the meaning of Article 16 of the European Framework Directive) (see particular national directives on http://europe.osha.eu.int/legislation/directives/a1.php3).

2.1 The Seveso directive

The scope of the Seveso II Directive is solely related to the *presence of dangerous substances in establishments*. It covers both, *industrial "activities"* as well as the *storage* of dangerous chemicals. The Directive can be viewed as inherently providing for three levels of proportionate controls in practice, where larger quantities mean more controls. A company who holds a quantity of dangerous substance less than the lower threshold levels given in the Directive is not covered by this legislation but will be proportionately controlled by general provisions on health, safety and the environment provided by other legislation which is not specific to major-accident hazards. Companies who hold a larger quantity of dangerous substance, above the lower threshold contained in the Directive, will be covered by the *lower tier* requirements. Companies who hold even larger quantities of dangerous substance (*upper* *tier establishments*), above the upper threshold contained in the Directive, will be covered by all the requirements contained within the Directive.

Important areas excluded from the scope of the Seveso II Directive include *nuclear safety*, *the transport of dangerous substances and intermediate temporary storage outside establishments* and *the transport of dangerous substances by pipelines*.

In order to assist Member States with the interpretation of certain provisions of the Seveso II Directive, the Commission in co-operation with the Member States has elaborated the following guidance documents that are available from the Institute for Systems Informatics and Safety, Major-Accident Hazards Bureau, Joint Research Centre, Italy:

- *Guidance on the preparation of a Safety Report* [4]
- *Guidelines on a Major Accident Prevention Policy and Safety Management System* [5]
- *Explanations and Guidelines on harmonised criteria for dispensations* [6]
- *Guidance on Land-use Planning* [7]
- *General Guidance for the content of information to the public* [8]
- *Guidance on Inspections* [9]

Operators of establishments, where substances in excess of the qualifying quantities given in column 3 of annex I of the Seveso II Directive are present, are in accordance with Art. 9 of the Directive required to produce a Safety Report within a fixed time frame, demonstrating that:

- A major accident prevention policy and a safety management system for implementing it are in effect.
- Major accident hazards have been identified and necessary measures have been taken to prevent such accidents and limit their consequences for man and the environment.
- Adequate safety and reliability have been incorporated into design, construction, operation and maintenance linked to major accident hazards.
- Internal emergency plans have been drawn up and information has been supplied enabling an external emergency plan to be drawn up.

Approaches to compliance

To fulfil this obligation the Operators shall adopt and implement procedures for systematic identification of major hazards arising from normal and abnormal operations and to assess their likelihood and severity. This is spelled out in details in the directive's Annex II on data and information to be considered in the Safety Report:

- Identification of installations and other activities of the establishment, which could present a major accident hazard.
- Description of areas where a major accident may occur.
- Identification and accidental risk analysis and prevention methods:

1. Detailed description of the possible major accident scenarios and their probability or the conditions, under which they occur, including a summary of the events, which may play a role in triggering each of these scenarios, the causes being internal or external to the installations.
2. Assessment of the extent and severity of the consequences of identified major accidents.
3. Description of technical parameters and equipment used for the safety of installations.

4. Measures of Protection and intervention to limit the consequences of a major accident

The approaches chosen by the Operators to demonstrate whether adequate measures have been taken may be based on the use of technical and managerial expertise supported by quantitative as well as qualitative methods. The methods used may vary considerably depending on the complexity of the substances, the processes, the installations and in particular, whether the necessary level of hazard control by and large have been laid down in Regulations, recognised Standards, Codes of Practices or other relevant documents.

To avoid misunderstandings during the preparation of the Safety Reports and promote the assessment by the Authorities as required by the directive, the methods used and the planned documentation of the results may be established in dialog with the Competent Authorities. However, in all cases the hazard identification and risk assessment should include [10]:

- Identification of the safety relevant sections/installations.
- Identification of hazard sources.
- Assessment of the consequences.
- Assessment of information on and lessons learnt from relevant major accidents.
- Assignment and assessment of the adequacy of the prevention, control and mitigation measures.

Other relevant directives

It is important to carry in mind that hazard identification and risk assessment are more or less universally required in other EU Directives such as the Machinery Directive, the Framework Directive on Labour protection and the Directive on equipment and protective systems intended for use in potentially explosive atmospheres.

The requirements on risk assessment included in these Directives may be limited to the safety or safe use of machines, explosion prevention and protection or the health and safety of workers, while Seveso II has a wider scope including the protection of the environment. However, the outcome of such assessments should be taken into account in relation to the risk assessment carried out by the Operator to demonstrate the adequacy of the measures taken to prevent major accidents - not least to avoid duplication of work.

At the end the final judgement by the Operators as well as the Authorities of the adequacy of the measures taken have to be based on technical and managerial expertise, supported when relevant by comparison with the outcome of quantitative or qualitative risk analysis, or use of recognised standards, Codes of Practices, lessons learnt from accidents etc. It is important to note that no acceptance criteria have been laid down in this field.

Operators of establishments, where substances in excess of the qualifying quantities given in column 2 but less than column 3 of annex I to the Seveso II Directive, are in accordance with Art. 7 of the Directive required to draw up a document setting its major accident prevention Policy and to ensure it is properly implemented.

This document shall be made available to the Authorities on request at any time in particular for the purpose of inspections and controls to be carried out by the Authorities.

EU legislation requires that the risks associated with chemicals and other dangerous products that are marketed be assessed and, where appropriate, reduced. The legislative framework is provided by the Directive on dangerous substances and preparations (67/548/EEC) and associated implementing Directives and Regulations (the key ones being Directive 93/67/EEC, Regulation (EEC) No. 793/93 and Regulation (EC) No. 1488/94). The dangerous substances Directive was originally conceived as a means of harmonising specifications which could otherwise create obstacles to free movement of goods. However, subsequent amendments have been aimed at ensuring chemical safety and environmental protection. The other Directive of direct relevance to risk management is 76/769/EEC on the marketing and use of dangerous substances and preparations. Under this Directive, bans and other controls can be placed on dangerous substances. Few Member States have legislation in place at the national level to regulate chemical substances.

In a Working Paper on Risk Management (European Commission, 1997), Directorate General III of the European Commission defined risk management within the framework of Directive 76/769/EEC as 'the process of weighing policy alternatives and selecting the most appropriate regulatory action, integrating the results of the risk assessment with additional data on social, economic and political concerns to reach a decision.' This implies the following approach to risk management:

- identification of chemicals for consideration;
- risk assessment;
- risk evaluation; and
- risk mitigation or reduction.

Under Article 10 of Council Regulation (EEC) No. 793/93, where marketing and use restrictions are recommended, 'an analysis of the advantages and drawbacks of the substance and of the availability of replacement substances' is required. More generally, the Commission has 'engaged itself to carry out a comprehensive risk assessment and an adequate analysis of the costs and benefits prior to adoption or proposal of measures affecting the chemical industry.' The form of such analyses is left open, as is the detail regarding what should be considered.

The document *Technical Guidance on Development of Risk Reduction Strategies* under EEC 793/93 [11] provides general guidance as to what should be considered in such assessments. It puts forward a five-step approach to risk management, which includes the consideration of socio-economic issues.

The document also highlights the differences in attitude, which exist across the various Member States concerning the use of socio-economic analysis. For example, some favour a precautionary approach and call for action, including when evidence for the existence of risks is highly disputed, while others place more stress on adopting an approach which insists that actions which could entail large costs should not be taken without a clear benefit [11]. As a result, there are differing views within the EU on the level of assessment which should be undertaken as part of the risk management process and the assessment of 'advantages and drawbacks', and the treatment of uncertainty within such assessments. For example, some Member States prefer a simple 'check box' technique, while others prefer as fully quantitative Socio-Economic Analysis (SEA) as possible.

3 National concepts to safety and risk analysis of process industry

The extent to which the Quantified Risk Assessment (QRA) of different industries has gained acceptance in addressing major accident hazards varies from country to country and indeed company to company. Within Europe some regulators were very enthusiastic requiring QRA studies in law (e.g. the UK and the Netherlands). The other countries (e.g. France) preferred to adopt more of a consequence based approach, whilst others (e.g. Germany) focused on adherence to codes, standards and good practice [12].

For substances identified as potentially damaging, a range of regulatory controls exists at both national and international levels. The approaches adopted in setting such controls vary across countries and regulatory agencies. In some countries, regulation is based on a precautionary stance, which requires that risks be minimised where the causes and mechanisms are unknown, or human health or the environment health is under threat. In the extreme, such an approach implies that many hazardous chemicals and activities are considered unacceptable because of the uncertain nature of associated risks. This type of approach to the management of chemical risks may neglect the benefits, which the chemicals could confer on society. Less extreme interpretations of the precautionary principle stress the cost of taking precautionary measures, while others come closer to a 'safe minimum standards' approach [2].

Other approaches to risk reduction are technology-led: for example, where they are based on the concepts of making emissions 'as low as reasonably practicable' or the use of 'best available techniques not entailing excessive costs'. Both these concepts recognise, at least implicitly, that a balance should be struck between the costs involved in reducing risks and the benefits stemming from risk reductions. However, they provide no guidance on the level of environmental protection that is socially desirable, the level of risk to human health that is socially acceptable, or what constitutes excessive cost in terms of both public and private expenditure. Thus, risk versus benefit trade-offs are neither made explicit nor expressed in a way that allows direct comparison. As a result, decisions may be taken which imply widely varying valuations for the environment and for reductions in morbidity and mortality rates [2].

At a national level, in the Netherlands, probabilistic risk analysis is a requirement of the safety report. The Netherlands has a clearly defined policy on the maximum levels of risk that are acceptable when considering land-use decisions. In the UK, the probabilistic approach to risk analysis is favoured, but up to now, quantitative risk criteria have been published only as far as the control of land-use in the vicinity of industrial facilities is concerned, whereas criteria for siting of new activities are being developed. In Germany, deterministic approaches are extensively used in the chemical process industry to demonstrate the quality of measures taken to avoid risk inside and outside the installation. The hazard potential is primarily determined by the impact range of material and energy emissions on the basis of exceptional incidents and nomogram techniques. The probability of occurrence can most often be derived from the triggering sensitivity of the hazardous substances. An assessment is only possible on the basis of general statements of probability and this approach has become an established and useful technique in practice, in particular in the classification of process control engineering systems as operating, monitoring, safety or damage minimising systems, maintenance and instrumentation [13].

3.1 French practices

The text in this section is based on the document [14].

Major accidents generally involve a series of phenomena, which so far have often been poorly understood.

The importance of the stakes at play in the field of major technological risk prevention therefore implies that every caution be taken in their evaluation: the risk of underestimating the effects of major accident, even if its probability is extremely low, cannot be accepted.

While evaluation methods have been significantly enhanced over the last few years, there still remains a certain margin of uncertainty, which, although increasingly low, nonetheless incites to be prudent with regard to any probabilistic quantitative approach.

Many manufacturers themselves agree that the bases for any such approach have yet to be proven (indeed very few of them have used risk probability evaluation when performing their hazard surveys).

Analysis of past industrial accidents leads to the same conclusion: the BLEVE*, for example, a phenomenon considered as being one of the worst accident scenarios, and one with a very low probability, has already occurred 135 times in 30 years.

While a probability approach is a useful tool enhancing understanding by manufacturers of the risk their facilities entail, and can help them determine what technical measures of prevention are required, *the data are not considered useful for public information display purposes of high-risk areas around the site.*

* BLEVE: Boiling Liquid Expanding Vapour Explosion

A deterministic, conservative approach is therefore seen as necessary (based on overestimated hypotheses and scenarios).

The only approach which is deemed acceptable and technically well-founded for public risk information purposes is to take into consideration *all possible accident scenarios, including those with the worst effects, to determine their maximum effects* (eventually reduced by taking into account the technical measures of protection implemented by the manufacturer, recognised as being reliable and verified by inspecting the classified facilities; for example, automatic insulation valves etc.) *and then presenting the scenarios to the general public and their elected representatives*.

In order to ensure homogeneity and equal treatment in the initial display of risks based on the deterministic approach, the Secretary of State for the Prime Minister for the Environment and the Prevention of Natural and Major Technological Risks has drawn up a list of accidents and reference criteria which are presented below.

In particular they are the fruit of feedback from experience, resulting from the examination of danger studies carried out by manufacturers subject to the prescriptions contained in the Seveso II Directive and statistical analysis of past industrial accidents.

The main reference scenarios, which serve as a basis for determining the area for concerted policy around a high-risk facility, are the following:

- Risks linked to liquefied combustible gas facilities (fixed, semi-mobile or mobile):
  Scenario A
  - BLEVE type explosion

  Scenario B
  - UVCE* type explosion

- Risks linked to containers with liquefied or non-toxic gases, which risk breaking during handling, or after internal explosions or external shocks:
  Scenario C
  - Total instantaneous loss of confinement

- Risks linked to toxic gas facilities (when the capacity is dimensioned to resist external shocks or internal product reactions):
  Scenario D
  - Instantaneous breakage of the largest pipeline leading to the highest mass flow

* UVCE – Unconfined Vapour Cloud Explosion

- Risks linked to high-capacity storage of inflammable liquids:
  Scenario E
  - Fire in the largest tank
  - Explosion of the gas phase of fixed-deck tanks
  - Fireball and projection of ignited product by boil-over

- Risk linked to the use and storage of explosives or explosive products:
  Scenario F
  - Explosion of the largest mass of products present or which can be produced by reaction.

Each of these scenarios comprises reference criteria:

- Hypotheses concerning the conditions in which the accident occurs: leak characteristics, aerology etc.
- Gravity thresholds to characterise the effects of the accident (toxicity, thermal radiation, excess pressure).

For each case, the criteria together enable evaluation of the extent of the risk zones corresponding to the first deaths and the first irreversible effects on people (and, for accidents with slow kinetics, the possibility of evacuating facilities or housing).

The area for concerted policy, in which control of urban development is necessary, is then determined by overall area of the zones defined above.

Each scenario is illustrated by several major accidents that have occurred over the last few years in industrialised countries.

In addition, for each scenario a simple reference method enabling the extent of the zone of risk to be evaluated and an example of its use are supplied.

The administrative departments thus have available a simple, reliable technical instrument enabling them to proceed with the public display of risk information on the basis of the results of the danger studies and the use of the reference methods proposed in the brochure [14].

3.2 German practices

The text in this section is based on the materials [15]-[17].

The German standard DIN 31 000, Part 2, defines safety as "a state of affairs in which the risk is not greater than the greatest acceptable risk due to the technical process or condition under consideration".

The standard states that this risk is generally not quantifiable, since only in rare cases can it be expressed as the product of a frequency and a measure of severity.

The standard treats danger as the diametrical opposite of safety, where the risk of a process is greater than the acceptable limiting risk (Figure 1).

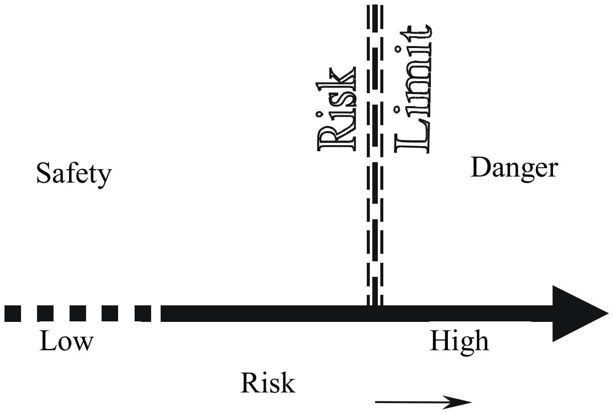


Figure 1 Risk chart

A useful notion in plant and process safety industry is the hazard potential, a measure of the greatest harm that can occur in the worst possible event in a plant or plant subdivision. It is reasonable to use this concept in assessing safety measures in a plant: the greater the hazard potential, the more and better safety measures are needed to lower the probability of occurrence of the undesired event to the point that the level of risk is at or below the acceptable risk level.

Safety measures may include intrinsic measures and conditions, which ensure a priori that a hazard potential can become real only in the event of a relatively improbable combination of multiple independent failures.

Safety or protective measures can be built up on the basis of this intrinsic safety in order to lower the risk to the acceptable level.

An anticipated value for the risk posed by chemical plants to employees or uninvolved third parties can be derived in a relatively simple way by statistical analysis of historical data.

Consider the risk of death incurred by a chemical worker due to a typical chemical accident (poisoning, chemical burn, explosion). In Germany this risk can be determined by analysis of the annual reports of the mutual accident insurance association of chemical industry. When the number of persons per year suffering death from poisoning, chemical burn, fire, or explosion is divided by the total number of persons employed in the chemical industry, the annual individual lethal risk averaged over the period 1983-1992 is ca. 7×10^{-6} a^{-1}, i.e., statistically 7 persons in 10^6 die every year owing to an on-the-job chemical accident. This risk is a factor of 20 less than the risk of dying in a traffic accident in Germany (currently ca. 1.5×10^{-4} a^{-1}) and is comparable to the risk of drowning (ca. 8×10^{-6} a^{-1}).

Those living nearby and others outside the chemical plant are even safer from chemical effects, because the effects of the infrequent incidents in chemical plants fall off quite rapidly with distance. It can be assumed that this risk is, at most, of the same order as the risks due to natural catastrophes. In Germany, the past 50 years have seen no identifiable serious personal injuries or deaths outside a chemical plant site resulting from accidents inside. This shows that the German chemical industry, like those in many other industrialised countries, operates very safely.

However, it is true that a low risk may well conceal high hazard potential, when the probability of occurrence is low. It is therefore advantageous to consider the size of hazard potential in chemical plants.

Reformulating the term “risk” [17]

When considering a hypothetical case, i.e. one for which a statically insufficient number of typical incidents have been reported within the chemical industry, the severity is replaced by the *activated hazard potential*

$$R=F\times S=F\times Gf,$$

where R is risk, F is frequency, S is severity, and Gf is activated hazard potential. In the following, a new definition for the probability of occurrence is introduced. F is determined by *triggering sensitivity parameters h* and the related *preventive measures* ψ

$$F=h\times\psi.$$

The triggering sensitivities h are primarily those material properties which must necessarily be present in order that a hazardous incident can be triggered. Or, expressed differently, these sensitivities would alone determine the probability of occurrence if no preventive measures ($\psi=1$) were present.

The *activated hazard potential* is defined analogously as the product of the *hazard potential G* and the related *limiting measures* Φ. Alternatively, Φ can be treated as that part of the hazard potential G which is active in a particular scenario:

$$Gf=G\times\Phi=e\times M\times\Phi$$

The hazard potential itself comprises the specific, *hazardous material properties e* and the *material inventory M*. The quantities ψ and Φ correspond to weighting parameters and contain all information about the prevention or limitation of plant malfunctions and accidents.

The new definition of risk is thus given by the following expressions:

$$R=(h\times\psi)\times(e\times M\times\Phi)$$

or

$$R=R_0\times\psi\times\Phi$$

where $R_0=h\times e\times M$.

According to this new definition, risk can be interpreted as a combination of the basic risk R_0 and the weighting factors ψ and Φ, the technical and organisational means of prevention and limitation. This approach thus allows the materials-related risk factor to be decoupled from the operative elements.

Four important theoretical limiting cases can now be derived directly from this definition:

Inherent safety:	$(h, e, M) \Rightarrow 0$
Integrated safety:	$\psi \Rightarrow 0$
Additive safety:	$\Phi \Rightarrow 0$
Worst-case scenario:	$(\psi, \Phi) = 1$

The utility of this new risk definition is demonstrated by the fact that these four limiting cases can be simply represented as shown. The practical applicability of this approach is illustrated in the following. The worst-case scenario represents a theoretical limit, which in practical alarm and hazard control planning does not lead to the generation of useful information. Therefore the so-called ‘exceptional incident’ scenarios are used in Germany which conform to physical and chemical laws and to the individual characteristics of the chemical plant concerned. Experience shows that a complete failure of all preventive and limiting measures is not realistic. Generally ψ and $\Phi << 1$, as only a small fraction of the hazard potential has an impact during any one incident.

In addition, risk assessments are also performed under the simplification in setting the probability of occurrence equal to one ($F=1$). In this case, risk assessment is then controlled solely by the hazard impact range or, if further reduction $\Phi=1$ is made, solely by the hazard potential.

In order to assess the hazard impact range, an impact assessment study must be performed.

3.3 Dutch practices

The text in this section is mainly based on the paper [18].

The use of risk assessment techniques is fairly widespread in policy and regulations in the Netherlands for such fields as design criteria for the dike system along the rivers, the introduction and use of chemicals and the transport of hazardous materials. Several attempts have been made to harmonise the techniques and criteria over the different fields. This has proven unsuccessful to date. Especially the field of toxic chemical agents stands out both in methodology and in assessment procedures. In the field of major hazards the methodology and procedures are closely related to those used in engineering and in nuclear industry.

Although some risk management concepts were introduced in public policies associated with nuclear power generation, most of the development resulted from some major disasters in the chemical industry in the mid seventies. The regulation in the Netherlands was shaped by the regulation on LPG [19] and follows a risk-based approach. The introduction of this approach in environmental policy to a certain extent was a breach with the general opinion until then that no kind of pollution or risk was acceptable.

The principle considerations in the risk-based approach are

- Risk is not zero and cannot be made zero
- Risk policy should be transparent, predictable and controllable
- Risk policy should focus on the largest risk
- Risk policy should be equitable

Risk regulation on the basis of the first principle creates the necessity to know the magnitude of risks and to limit the acceptability of these risks by setting finite, non-zero standards.

In the risk management process quantification plays a central role. It has been therefore necessary to standardise to a certain extent the metrics by which risk is expressed and the methodology, which is to be used to quantify risks and to manage them.

In the context of the external safety policy in the Netherlands three measures of risk are used: the individual risk (IR), the societal risk (SR) and the expected value of the number of people killed per year, also called the potential loss of life (PLL).

The individual risk is defined as the probability that a person who permanently is present at a certain location in the vicinity of a hazardous activity will be killed as a consequence of an accident with that activity. Usually IR is expressed for a period of a year. It can be pictured on a map by connecting point of equal IR around a facility, the risk contours.

Societal risk is defined as the probability that in an accident more than a certain number of people are killed. Societal risk usually is represented as a graph in which the probability or frequency F is given as a function of N, the number killed. This graph is called FN curve.

For the policy regarding the risk for the environment similar measures have been developed. In the document “Premises for Risk Management”, which is part of the Dutch National Environmental Policy Plan, these issues are discussed extensively [20].

A considerable number of systems have been developed to automate the necessary calculations. Many of these developments have led to commercially available systems. The SAFETI package, which originally was developed under contracts from the Directorate General for Environment and the Rijnmond Authority is an example. At the time being it is the most comprehensive and most expensive package available.

From a description of the process and associated flow diagrams and other technical material it is established which vessels and pipes are present in the installation. For each part it is determined how it can fail, how much of the contents is released and how this release takes place. Because the number of ways, by which a release can occur are endless, a choice is made of what events or scenarios can be taken to be representative for the whole gamut of releases possible in the installation.

Subsequently the dispersion into the surroundings of the released chemical is determined. For a flammable material the explosive force and the heat radiation levels are calculated. For a toxic – the toxic load in the surroundings. The results are combined with data on population density, weather and wind and failure frequencies pertinent for the installation to calculate the individual risk and the societal risk.

A series handbooks, the so-called coloured books [21]-[25], has been issued by the Committee for the Prevention of Disasters, which together form the guideline for quantified risk analysis in the Netherlands. The handbooks cover the methodology for the quantification of risks for hazardous installations and for the transport of dangerous materials.

In other areas similar standardisation has taken place. For the calculation of airport risk the method described in [26],[27] serves as the "de facto" standard in the Netherlands, although other methods are used elsewhere [28],[29]. Similar standard methods exist in the construction of bridges and other civil engineering objects. These methods are also probabilistic in nature [30].

In the Netherlands risk assessments are carried out as part of safety reporting studies under the Seveso II directive, as part of permit applications, as part of environmental impact assessment and as part of policy development. The methodology is well established and documentation on preferred practices is extensive.

3.4 UK practices

This text is in part based on [31].

The Seveso II Directive is implemented in the UK through the Control of Major Accident Hazard Regulations 1999 (COMAH). The COMAH Regulations substitute its predecessor (CIMAH) and it

- Simplifies the application criteria;
- Removes some exemptions, such as chemical hazards at nuclear installations and explosives;
- Place greater emphasis on the need for effective safety management systems, and
- Put specific duties on the competent authorities

The UK Health & Safety Executive (HSE) plays a central role in the COMAH Regulations. Previously (under CIMAH), HSE was the sole "Competent Authority", nowadays HSE shares responsibility with the national environment agencies.

The general principle in managing risks is that risks should be reduced to a level as low as reasonably practicable (ALARP). The ideal should always be, wherever possible, to avoid hazards altogether. In demonstrating ALARP, it is not a requirement of the regulations that Quantitative Risk Analysis (QRA) should always be undertaken. There is, however, a strong tradition in the UK to use QRA. In the case of land-use planning around hazardous sites, decision-making is always based on formal quantified risk criteria, requiring a QRA to be made for the hazardous site in question.

With respect to land-use planning, HSE's original approach was to advise on the basis of the concept of "protection" of those exposed to a hazard. This approach involved the identification of the worst events and then the determination of a separation distance based on a defined level of injury or impact. This approach was subject to criticism on a number of reasons, including:

1. the possibility that the protection provided is beyond that which is 'reasonable' and overly conservative, resulting in excessive restrictions on land use;
2. the somewhat arbitrary nature of the worst event, and potential inconsistency between installations in deciding which major event to use as a basis;
3. the difficulty of comparing the degree of protection with that which seems to be necessary or desirable for other hazards in life.

For these reasons, HSE's basis for advice on land-use planning will be quantified risk criteria. But all QRA estimates involve uncertainty and judgements and decisions need to be taken in the knowledge of these uncertainties.

Uncertainties may arise from various parts of an assessment. They include uncertainties related to:

- Failure rate data: Historical data are often sparse or of doubtful relevance, and needs to be supported by structured analysis of potential failure causes.

- Consequences: Consequence models are required to extend the available empirical information. Uncertainty arises from incomplete validation material for these models as well as from the inherent random nature of some phenomena (e.g. turbulence).
- Impact and injury: Prediction of injury and impact cannot be performed deterministically due to unknown differences in susceptibility.
- Human error: Human action influences all aspects of control, from project conception, through design, construction, commissioning, operation, inspection, maintenance and repair to the final stage of decommissioning. Thus there is scope for mistakes at all stages. Human error is unpredictable.

It is important that human error be taken into account as a cause of accidents, to give a full assessment of risks from an installation. This may be done implicitly (using data of failure-rates from all causes) or explicitly (by analysing the potential causes of failure including human error). The HSE methods rely mainly on the implicit approach, but assessors are able to analyse to greater depth where some particular aspect seems very sensitive to assumptions human error.

It is sometimes suggested that HSE assessors should include an adjustment to failure-rates to allow for some deviation from 'average' of the overall quality of the safety management at an installation. For the purpose of land-use planning, care would be needed to allow for the possibility of changes in management over the many years' lifetime of a planning decision.

HSE's present view is that any allowance for 'good' management should be app1ied if at all only within narrow limits. An allowance to reduce the predicted failure-rates because of good quality could well be optimistic, given the possibility of changes over time.

Several methods have been developed to cope with the effects of uncertainties in hazard and risk assessments. The two main approaches are:

- Pessimism: Here, it is necessary to ensure that any assumptions, whether explicit or implicit, err if at all in a pessimistic direction, i.e. they overestimate the risk. This should result in a value which is almost certainly not an underestimate, but which may possibly be a large overestimate of the risks. There may be considerable uncertainty as to the amount of the overestimate and its implications.
- Best estimate: Here, efforts are made to ensure that all assumptions are as realistic as possible. Again, there is uncertainty. It is not clear what the overall effects of the combinations of uncertainties are. It would not necessarily be known whether the results are an underestimate or an overestimate of the risks. It is important to test the sensitivity of the results as much as possible to minimise the uncertainties.

HSE currently uses an approach that may be described as 'cautious best estimate'. Every attempt is made to use realistic, best-estimate assumptions (whilst clearly defining the basis of the assumptions), but where there is difficulty in justifying an assumption, some overestimate is preferred. In such a case, the sensitivity of the overall results to that particular assumption might be tested, and further research work might be done to try to improve the realism of the results.

The 'cautious best estimate' approach helps to offset any uncertainty arising from the possibility of grossly abnormal human behaviour and other unquantified causes of accidents.

A feature of the HSE approach is that it makes an explicit allowance for mitigating factors such as people's ability to escape or to protect themselves in emergency. For example, for a toxic gas hazard, HSE assumes that people out of doors would try to escape indoors, with a probability of success, which depends on the concentration of gas out of doors.

As a consequence of this "cautious best estimate" approach, the UK HSE has taken an active role in the development and improvement of (software) tools for QRA, including consequence modelling. In that process, the HSE initiates and co-ordinates research in this field. A result of this effort is HSE's "RISKAT" package, a tool to perform QRA for chemical installations.

4 Industry-specific safety- and risk analysis approaches

4.1 Risk Assessment in the Offshore Industry

The text below is based on [32].

The attention of the risk management in the offshore industry is focused on safety of the crew and the installation, prevention of environmental damage and production of regularity. Unlike onshore process industry, the potential for threatening third party is quite limited for most offshore installations.

Early Norwegian offshore experience shows that the development was based on international practice. Several accidents in the 70ies, including a riser fire in 1975 and a blowout in 1977 on the Ekofisk field, demonstrated that more attention to safety was needed. The Norwegian Petroleum Directorate (NPD) issued their 'Regulations Concerning Safety Related to Production and Installation' in 1976. These included the requirement that if the living quarters were to be located on a platform where drilling, production or processing was taking place, a risk evaluation should be carried out. At that stage, such an evaluation would have been mainly qualitative.

In 1981 the NPD issued their "Guidelines for Safety Evaluation of Platform Conceptual Design". These were the world's first formal requirement for offshore QRA. The resulting studies became known as Concept Safety Evaluation (CSEs) and produced a major improvement in Norwegian platforms. The CSEs focused on availability of safety functions – escape routes, shelter area, main support structure and safety related control functions. No design accidental event should cause impairment of the safety functions. In principle, the design accidental events should be the most unfavourable situations possible relative to the safety functions. However, it was allowed to disregard the most improbable events, but the total probability of occurrence of each type of excluded situations should not by best available estimate exceed 10^{-4} per year.

Once the value of QRA had become apparent, Statoil and other Norwegian operators extended CSEs into more comprehensive Total Risk Analyses (TRAs). These differed from CSEs in the following respects:

- They were conducted during the engineering design phase, much later than CSEs. Consequently they addressed more detailed safety systems rather than the broad concepts in a CSE.
- They were much more exhaustive, including HAZOPs, reliability analyses, occupational risks and detailed hydrocarbon event modelling.
- They estimated the risks of fatalities rather than safety function impairments. This allowed comparison with other safety targets.

TRAs remain among the largest and most comprehensive offshore risk assessments ever carried out, and formed the basis for offshore QRA throughout the 1980s.

The original NPD guidelines set numerical criteria for acceptable safety levels, and expected operators to use QRA to demonstrate compliance. However, safety requires appropriate management attitudes. Therefore, the 1990 NPD regulations relating to implementation and use of risk analyses require the operator to manage safety systematically, using QRA as a tool, and defining their own safety targets and risk acceptance criteria. This might appear to be a relation of the regulations, but by making operators take greater responsibility for the safety of their own operations, they are expected to use QRA to greater effect.

QRA is no longer seen as an isolated activity, but as an integral part of an overall risk management strategy.

In 1993, the Norwegian Maritime Directorate (NMD) issued "Regulations Concerning Risk Analysis for Mobile Offshore Units". They require risk analyses at concept, design and construction stages for each mobile unit, but do not specify the precise form of the analysis, except that it is to include lists of dimensioning accidental events/accidental loads as well as recommendations related to possible risk reducing measures. The regulations specify that the overall risk to people, the unit and the environment is to be reduced as far as practicable, but the owner may specify additional acceptance criteria as well.

A reliability/vulnerability analysis is also required for specified systems important to safety on the unit. Acceptability criteria for these specify that single faults should not cause critical incidents, vital systems should be redundant, and the degree of redundancy should be related to the degree of hazard.

Many developments in QRA occurred in the offshore industries during the 1980s, particularly in the UK. Many UK operators used QRA methods as an integral part of the design process, but prior to the Piper Alpha accident, QRA tended to be applied to specific aspects of the design, rather than to overall risks. Consequently, it was mainly used as part of the detailed design when the scope for changes was limited. Examples include the prediction of the risks of ship-platform collision, and modelling of the risks in emergency evacuation. Several operators used the latter to assess and improve their arrangements for evacuation by lifeboat.

Other techniques were borrowed from the on-shore petrochemical industry, including hazard and operability studies (HAZOPs), techniques for modelling the consequences of hydrocarbon releases, and reliability analyses of key safety systems. Many of these form the building blocks of modern QRAs.

Under the UK safety case regulations each operator in the UK is required to prepare a Safety Case for each of its installations, fixed or mobile, to demonstrate that:

- The management system adequately covers all statutory requirements;
- There are proper arrangements for independent audit of the system;
- The risks of major accidents have been identified and assessed;
- Measures to reduce risks to people to the lowest level reasonably practicable have been taken; and
- Proper systems for emergency arrangements on evacuation, escape and rescue are in place.

QRA is one of the most important techniques used to identify major accident hazards and to show that the risks have been made ALARP (As Low As Reasonably Practicable), and is explicitly required under the regulations. Several other countries have followed the new UK approach, greatly increasing the requirement for offshore QRA worldwide.

Before an installation is allowed to operate, the Safety Case must be formally accepted by the Health and Safety Executive.

4.2 Aerospace industry

The text below is based on [33].

Space systems are characterised by high cost and complexity, long development schedules, and high risks due to severity of the consequences associated with the non-achievement of the mission objectives. Space project risks are both programmatic (with resulting consequences affecting development cost and delivery schedule) and technical (with consequences affecting performance, mission objectives and human life).

The development of large space projects in the 1970s and 80s was initially accompanied by the availability of considerable budgets, so that achievement of the technical objectives was given priority compared to financial targets. However, progressive budget reduction introduced by all the space agencies and the use of space for commercial purposes, has created a demand to develop complex projects under increasingly severe financial constraints. The budget limitation associated with design, development and procurement approaches could lead to a lower space system quality with potential detrimental effects on the schedule, performance, mission success, and safety.

In this frame the concept of risk currently plays a fundamental role in decision making and QRA becomes a fundamental step to support a global Risk Management approach. The main objective of this process is to assure program success by meeting a defined proportion between technical, performance and programmatic requirements, within limited resources and project constraints.

Reliability, Availability, Maintainability and Safety (RAMS) becomes a key issue in QRA and therefore an important design and operations driver. Safety always takes priority.

The safety and mission success of the system can be achieved by application of engineering techniques and deterministic design provisions such as redundancy and failure tolerance, inhibits and safety margins, but it can be measured only in terms of probability of crew survival and mission success.

The capability to quantify crew survival and mission success by means of QRA allows to:

- Identify drivers and requirements supporting Risk Management policy definition;
- Drive definition of design and operations strategy from the early phases of the project;
- Support trade-offs and optimisation among alternative system design concepts and variables;
- Rank the risk contributors to modulate the risk reduction efforts;
- Verify adequacy of safety measures implementation;
- Justify design and operations with a view to probabilistic targets;
- Support Risk Management in selection of the most cost-effective application of engineering techniques and development approaches.

QRA is therefore a way to support the decision-makers to select and accept design and mission scenario concepts and technological implementation aspects.

The RAMS requirements are specified both in a deterministic and probabilistic way. The severity of hazardous events are categorised as follows (according to European Space Agency standards):

Catastrophic Hazards:

- Loss of life
- Life threatening or permanently disabling injury
- Occupational illness
- Loss of an element of the interfacing manned flight system
- Loss of launch site facility
- Long term detrimental environmental effects

Critical Hazards:

- Temporarily disabling (not life threatening injury)
- Temporary occupational illness
- Loss of, or major damage to flight systems, major flight system elements
- Loss of, or major damage to ground facilities
- Loss of, or major damage to public or private property
- Short term detrimental environmental effects

A similar categorisation is applied by NASA standards.

The identification of hazardous events, mission critical events and consequence assessment is performed by means of: Function Tree Analysis, FMECA (Failure Modes, Effects and Criticality Analysis), Hazard Analysis and other supporting qualitative analysis such as Caution and Warning Analysis, Zonal Analysis, Human Error Analysis etc.

The selection of the probabilistic risk assessment approach and system description technique depends mainly on the nature of the requirement and the experience of the RAMS engineer. The applicable requirement is always a basic element for decision making.

Fault Trees and Reliability Block Diagrams are being extensively used. The first approach allows managing those cases for which specific probabilistic requirements are assigned to an unwanted scenario (e.g., Loss of Crew, Loss of Spacecraft, On-ground population risk etc.). In this way the Fault Tree Analysis identifies all the events or event combinations that lead to the unwanted “Top Event”.

On the contrary, the Reliability Block Diagram is used when the requirements are given in terms of success (e.g., Probability of Safe Return, Probability of Mission Success, Launch Probability etc.) or availability (readiness or operational availability).

The other well known approaches are limited to particular RAMS applications (e.g., Event Trees applied to model sequence of combination of success and failure events belonging to different systems) or project specific requests (e.g., Failure Condition Diagrams).

These analyses represent only a basis for a deeper investigation and are only part of a more complex RAMS analysis. Other topics are crucial in characterising the level and accuracy of the assessments:

- Basic events quantification and uncertainty analysis
- Probabilistic dependency between basic events
- Multiphased mission
- Readiness and Operational Availability.

5 Decision criteria applied in European countries

The text in this chapter is mainly based on [2]

5.1 Human Health Risk Criteria

In general, the consensus is that there are three levels of risk:

- a level of risk which is so high as to demand immediate action, often referred to as an ‘unacceptable’, ‘intolerable’ or *‘de manifesti*s’ risk;
- a level of risk which is so low as to be regarded as trivial, referred to as an ‘acceptable’, ‘negligible’ or *‘de minimi*s’ risk; and
- a level of risk between these extremes, where consideration should be given to the costs and benefits of risk reduction measures.

With regard to protection of human health, although risk criteria are used in several countries to determine whether or not a risk is ‘unacceptable’, comparing one set of criteria with another is often a complex task. A distinction is made between risks to an individual and to society as a whole. Concerning risks to an individual, we may define individual risk as *the frequency (probability) at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards.* By way of example, the probability of an individual being killed by lightning in the UK is one chance in 10 million per year.

Concerning risks to society as a whole, the situation can become very complex. One attempt to categorise the risks of interest is provided by [34], as shown in Table 1.

Table 1 Risks to Society – A Possible Typology

Term	Nature of risk	Risk associated with		Possible basis for criteria
		‘Normal’ activities	Accidents	
Collective risks	‘Diffuse’ risks associated with exposure to hazardous materials	Yes	No	Individual risk – possibly aided by CBA, CEA or MCA*
Societal risks	‘Simple’ risks associated with hazardous installations/activities	No	Yes	Numerical criteria based on fatalities
Societal risks	‘Diverse’ risks associa-ted with hazardous installations/activities	No	Yes	Numerical criteria based on ‘harm’
Societal concerns	Overall impacts/risks of technologies/strategies	Yes	Yes	Political judgement – possibly aided by MCA

As can be seen from the table, the concept of societal risk is particularly important when considering the potential of incidents associated with hazardous activities that result in large numbers of fatalities. Examples of such activities include the operation of chemical and nuclear plants, transport of hazardous materials, operation of passenger aircraft, etc. In Europe, it is possible that the concept of societal risk might be extended to account for environmental damage resulting from major accidents in response to recent legislation (Seveso II Directive).

Concerning the use of chemicals and substances in ‘everyday life’, attention is usually focused on the level of individual risk, although risk assessment results can also be presented in the form of ‘collective risks’ by simply considering the level of individual risk and the size of the population at risk. For example, if the individual risk of developing a fatal cancer was one chance in 100 million per year and the population at risk was 100 million, the collective risk would be one cancer per year.

Estimated risk values are usually expressed as either chances per year or chances per lifetime. The latter particularly applies to the expression of cancer risks, in which the concern is often related to exposure and effects over a lifetime. Given a life expectancy of, say, 80 years, it can be seen that conversion from an annual to a lifetime risk can be achieved by dividing by 80, as shown in Table 2. For workplace risks, assuming a 45-year working life, the conversion requires division by 45.

Table 2 Individual Risk Conversion

Lifetime risk	Equivalent individual annual risk (per year over 80 years)	Equivalent individual workplace risk (per year over 45 years)
1 in 1,000	1 in 80,000	1 in 45,000
1 in 10,000	1 in 800,000	1 in 450,000
1 in 100,000	1 in 8 million	1 in 4.5 million
1 in 1 million	1 in 80 million	1 in 45 million

* CBA – Cost-Benefit Analysis, CEA – Cost-Effectiveness Analysis, MCA – Multi-Criteria techniques

A summary of some current individual risk criteria is presented in Table 3. It is important to stress that these criteria are, in effect, actual or implied government guidelines, which are applied with varying degrees of rigour. Furthermore, the criteria are applied to ‘members of the public’ rather than to ‘workers’. This distinction is sometimes made with reference to ‘involuntary’ and ‘voluntary’ risks. Broadly speaking, the limits for workers (who ‘voluntarily’ expose themselves to risks) are a factor of ten (or more) higher.

From Table 3 it can be seen that the criteria levels of acceptable/unacceptable risk vary by type of risk and by country. There is broad agreement that risks above 1 chance in 100,000 per year (1 in 10,000 for workers) are ‘unacceptable’. Risk levels of less than 1 chance in 100 million per year are ‘acceptable’, although a risk of 1 chance in 1 million per year is ‘acceptable’ in many places. Generally, the level of ‘unacceptable’ risk corresponds to about 10% of the risk level associated with normal ‘voluntary’ risks (driving, working, etc.) and is similar to the higher ‘involuntary’ risks (being murdered, hit by a car, etc.), as shown in Table 4. These figures represent the ‘average’, and clearly there will be significant lifestyle variations.

In the US, the situation is somewhat different in two respects. Firstly, although the regulatory bodies do not use explicit risk criteria, estimated risk levels are often used to help justify specific regulatory actions in relation to chemical risk management. Secondly, the focus in the US is very much on ‘excess lifetime cancer risks’. However, in many past US regulatory decisions, limits of acceptability are in line with those presented in Table 3 (see, for example, [35]).

In summary, for existing technologies and ‘known’ risks, it is usually the case that legislation or current best practice (as prescribed in authoritative Codes of Practice) ensure that measures are considered for mitigating those risks that are likely to be regarded as ‘unacceptable’. Similarly, the presence of trivial risks is accepted as a matter of course. The concern is therefore over what approaches are to be used in mitigating the non-trivial risks, which fall into the ‘grey’ area where a balance needs to be reached between risks, costs and benefits, and other wider decision criteria.

Table 3 Examples of Actual and Implied Risk Criteria (per year of becoming a fatality or contracting a fatal risk)

Country	**Nature of risk**	**Limit of un-acceptability**	**Limit of acceptability**	**Criteria applied in between**
Netherlands	Residents close to hazardous facilities	1 in 1 million	None, but until recently: 1 in 100 million	ALARA*
Netherlands	Cancer risks	Not given	1 in 100 million	N/A
UK	Residents close to hazardous facilities	1 in 100,000	0.3 in a million	ALARP**
Australia (some states)	Residents close to hazardous facilities	Not given	1 in 1 million	N/A
Hong Kong	Residents close to hazardous facilities	1 in 100,000		N/A
*As low as reasonably achievable **As low as reasonably practical				

Table 4 'Everyday' risks in the UK

Level of individual risk	'Voluntary' activities	'Involuntary' activities
1 in 10,000 per year	Driving, working in non-office environment, being at home	
1 in 100,000 per year		Being murdered, being run over
1 in 10 million per year		Being struck by lightning

5.2 Sustainability and Other Decision Criteria

Sustainability and the sustainable use of chemicals are likely to form a background to most governments' decision making with regard to chemical risk management. Despite the fact that the term 'sustainable development' was first defined in 1987 by the World Commission on Environment and Development report *(Our Common Future,* the so-called 'Brundtland Report'), there is still considerable debate as to what this concept means in practice. The definition set out in the Brundtland Report is that sustainable development is:

development that meets the needs of the present without compromising the ability of future generations to meet their own needs

The implication of this definition is that, unless decisions are taken in the present to address either potential irreversible effects or those which may have a 'significant' impact at an intergenerational level, future generations either may not have the ability to address such effects or may face considerable costs in so doing. Within a generation, sustainability also implies particular concern for the most disadvantaged in society.

Extensive literature exists on the subject of sustainable development and how it should be interpreted, with many authors setting out general concepts and principles, and others suggesting indicators for measuring the degree to which it is being achieved.* From a regulatory analysis perspective, the concept of sustainability is perhaps best viewed as adopting objectives designed to achieve a sustained flow of economic, environmental and social benefits that will enhance the quality of life without reducing the long-term productive capacity of the resource base. The preferred regulatory measure (out of a set of alternatives) should then be that measure which best meets these objectives.

This view introduces questions about compensation and the tradability of economic, environmental, social and other goods. On the one hand, it is argued that sustainability should be interpreted as permitting free trade of all goods and services as long as the total value across all goods and services is not diminished. On the other hand, it is argued that not all goods and services are tradable, as there are certain economic, social, health and environmental considerations which must be preserved or protected.** With regard to chemical risk management, either concept concerning the degree to which different goods and services are tradable can form the context for undertaking a Socio-Economic Analysis (SEA),

* See, for example, Hart Environmental, 1996, OECD, 1995, Pearce et al., 1996, Schultink, 1992, UNEP, 1992, and WCED, 1987.

** For further discussion of different sustainability concepts, see Pearce et al., 1996, Rennings and Wiggering, 1997, and van den Bergh, 1996.

although the use of certain analytical approaches such as cost-benefit analysis tends to assume a greater rather than lesser tradability.

In addition to sustainability criteria, decision-makers are likely to consider a range of other criteria as part of chemical risk management (and these would feature in a good quality appraisal). Box 1 lists the decision criteria considered by Environment Canada to be relevant to chemical risk management [36].

Box 1: Wider decision criteria for risk management measures, noted by Environment Canada, include:

- competitiveness implications: to what degree will a measure minimise the financial burden to industry, and what will the impact on international competitiveness be?
- incentives: does the measure directly or indirectly stimulate creativity and innovation through some form of incentive to develop and implement cleaner technologies and ways of operation?
- enforceability and compliance: how easy will it be to enforce and monitor compliance with this measure?
- growth: can the measure be structured in such a way as to allow for economic growth (for example, the entry of new producers into an industry) while still meeting environmental requirements and policy commitments?
- speed: how quickly will the environmental objectives be reached through this measure?
- fairness: does this measure impose an unfair burden on certain individuals/sectors in the market?
- intrusiveness and flexibility: what level of regulatory knowledge and involvement will be required to effectively apply this tool? To what extent does this tool leave to producers and consumers the specific detailed decisions about how to achieve environmental objectives?
- data requirements: what will be the data requirements for implementation of this measure in terms of quality, intensiveness and availability?
- compatibility: will the application of this measure support or be in conflict with established jurisdictional responsibilities, existing regulations or other initiatives?
- public acceptability: will the use of this tool for environmental management be readily accepted by the public?

5.3 Decision-making based on costs and benefits

In selecting the methodology, which will provide the basis for the SEA, a number of factors should be considered:

- the stated objectives of the SEA and the requirements of decision makers with regard to having quantitative versus qualitative information (with these sometimes set by the relevant regulation);
- the number of costs and benefits of concern, and whether any specific health or environmental targets or thresholds have to be met for an option to be acceptable;
- the nature of the information available from the risk assessment (whether a full consequence analysis or more limited information on hazard or risk potential); and
- the period of time and resources (staff and money) available to the analyst.

These types of factors are also identified by the EC as important to the decision on the appropriate approach to the analysis. For example, Box 2 indicates the factors suggested in the *Technical Guidance on Development of Risk Reduction Strategies* [11] that should be taken into account when determining the form an SEA should take.

Box 2: Factors in Determining form of SEA

Directorate General XI of the European Commission in its Guidance on developing risk reduction strategies suggests that the form of any analysis, whether qualitative or quantitative, should consider factors such as:

- the severity and extent of the risk;
- the scale of the drawbacks;
- the balance between the likely advantages and drawbacks;
- the information available within a reasonable cost and a reasonable time frame; and
- the level of uncertainty surrounding the likely advantages and drawbacks.

Source: European Commission (1998)

In general, the greater the complexity of issues requiring examination, and the more quantitative the analysis is to be, the greater the elapsed time and level of resources required. The lower the level of quantification required (for example, where a target has been set or the risk assessment limits the degree of quantification) and the less complex the issues of concern are, the lower the level of resources required to complete the analysis. There will of course be exceptions to this general rule.

Of key importance is the need to recognise the multi-faceted nature of the decisions that will have to be made using the results of the analysis. A wide range of different issues need to be taken into account, stemming in part from the varying interests of the stakeholders, which in turn lead to varying priorities for risk management. For industry stakeholders, achieving effective risk management at a minimum cost will be a priority, while for others the priority may be to reach desired levels of environmental quality or worker safety regardless of costs. As a result, methods that assist in identifying the trade-offs between the various criteria are likely to be essential for most decisions. The method applied to a particular risk management problem, however, will depend upon the characteristics of the problem noted above and the extent of the differences in position among the stakeholder groups.

Depending on the requirements, an SEA may take one of three possible forms:

- a systematic qualitative analysis, where the magnitude, significance and relative importance of the risks, costs and benefits are described but not quantified;
- a semi-quantitative analysis, where some aspects of the risks, costs and benefits are assessed in quantitative terms while others are treated qualitatively; or
- a fully quantitative analysis, where all risks, costs and benefits are quantified in physical/natural units and/or, in some cases, in monetary terms.

A *qualitative* analysis will generally be sufficient where there are readily affordable solutions and there is common agreement that risk management is required. In other cases, a qualitative analysis may not be sufficiently detailed to show whether the benefits from risk management outweigh the costs. As a result, a more quantitative analysis is likely to be required, with this taking the form of either a semi-quantitative or a fully quantitative analysis. However, the potential savings, and greater assurance of meeting decision makers' and stakeholders' objectives through making a more informed decision, should justify the cost of undertaking a more quantitative analysis.

In general, the more *quantitative* the approach, the more informative the analysis is likely to be, but also the more resource-intensive. Any analysis will inevitably involve management of uncertainty and will require informed, professional judgements to be made. As a result, achieving a balance between the thoroughness of the analysis and practical limits to carrying out an analysis will be essential.

A study undertaken for the Nordic Council of Ministers [37] promotes a stepped approach to SEA, starting with the application of qualitative assessment techniques. Semi-quantitative or more fully quantitative techniques are then applied as warranted by the magnitude of the trade-offs involved in selecting one course of action over another. The study goes further, to suggest that, given the complexity of the decisions and the number of factors that need to be taken into account, for many risk management problems the combined use of a number of techniques may prove the most valuable.

Table 5 provides an overview of the main semi-/fully quantitative methodological frameworks which can provide the basis for the SEA: Cost - Effectiveness Analysis (CEA), Cost-Benefit Analysis (CBA) and Multi- Criteria techniques (MCA). In general, the principles underlying CBA appear to provide the preferred framework for many countries that currently have established programmes involving the application of SEA to chemical risk management.

Table 5 Key aspects of decision-making based on costs and benefits

Methodology	Principles	Qualitative vs. quantitative data	Advantages	Disadvantages
Cost-effectiveness analysis	Based on principles of economic appraisal, but the aim is to find the least- cost method of achieving standards.	Only costs are usually estimated in money terms. Where targets are set, these are usually quantitative, but other effects may be assessed either qualitatively or quantitatively.	Allows selection of the lowest-cost alternative to achieve pre-set level of protection. Often used when benefit measures cannot be monetised.	Provides less information than CBA on the most efficient level of control. Unlike CBA, does not provide information on whether the benefits gained by an action will be greater than the costs of adopting that action. Thus, alternatives that ensure positive net benefits cannot be identified.
Cost- benefit analysis (or risk-benefit analysis)	Based on principles of welfare economics. Assumes that society's values are reflected in individuals' willingness to pay.	Analysis may contain qualitative, quantitative (quantified but not necessarily monetised) or fully monetised information. Rarely will it be possible to value all impacts.	Use of familiar and common unit of measure. Provides information on whether the benefits of an action outweigh the costs, and the level of risk reduction that provides for the greatest level of benefits over costs. Allows direct comparison of regulatory decisions.	Monetary valuation of all costs and benefits is likely to be costly. Some question the validity and reliability of such valuations.
Multi- criteria techniques	The more complex techniques have a basis in utility theory; simpler methods stem from the need to convey information in a readily accessible form.	Can assess impacts using either qualitative or quantitative indicators of effect and significance.	Multi- attribute nature of problem is respected. Allows distinction to be made between impact and importance of impact to decision.	Difficulties in defining agreed scoring and weighting systems. Problems with double counting in some past applications. Aggregation to a single unit of measure (or a small number of indicators) is meaningless outside specific study.

5.4 Barrier Method to Decision-Making

The barrier diagram method is a graphical approach for describing accident scenarios and evaluating the safety measures (barriers) present to interrupt the accident sequence. The method originally was developed as part of a project for the Danish Environmental Agency to serve as documentation of the safety in plants handling hazardous substances ["Miljøprojekt Nr. 112 - Kvantitative og kvalitative kriterier for risikoaccept" published by Miljøstyrelsen (in Danish) - 1989]

Barrier diagrams should be kept simple, and may exclude insignificant information, as the main purpose of the diagrams is to create the overview. The information for constructing the barrier diagrams usually is taken from the hazard identification meeting notes, e.g. HAZOP sheets. Barrier diagrams serve two main purposes:

1. Evaluations of whether safety measures are adequate and where new safety barriers preferably could be introduced, i.e. barrier diagrams can be used in accident prevention work.
2. Communication to all stakeholders incl. the public. Providing that the barrier diagrams are made fairly simple, they are excellent for illustrating the possible accident scenarios and the safety measures taken to prevent them.

Barriers

Barriers can be defined as measures present to interrupt an accident event sequence, i.e. prevent the end event of the accident scenario in occurring. Examples of barriers are given below:

- An alarm for instance for high level in a tank.
- A sprinkler system in a building to prevent fires in developing.
- A dike surrounding a tank, designed to contain accidental spillage from the tank.

Barriers can be of different types. One may consider the following types:

- active versus passive barriers
- automatic versus manual barriers

Active barriers are barriers that include an action to be in effect. For instance a shutdown valve is an active barrier. The valve has to be activated and close to be effective, i.e. one or more actions have to be made for the barrier to be effective. The actions may be operator dependent or automatic. Passive barriers on the other hand are effective without any action. An example of this is a tank dike. Assuming that it is designed correctly and is not defect, it will always be able to contain an accidental spill from the tank. Passive barriers are generally considered more reliable than active barriers.

Construction of barrier diagrams

The construction of barrier diagrams consists of 4 steps:

1. Construction of the event chains
2. Inclusion of the barriers.
3. Evaluation for each barrier of what would happen assuming that the barrier is effective and construction of relevant event chains from the evaluation.
4. Classification of barriers according to type or evaluated reliability of the barrier (optional).

An example of the event (cause-consequence) chains of a barrier diagram is shown in Figure 2.

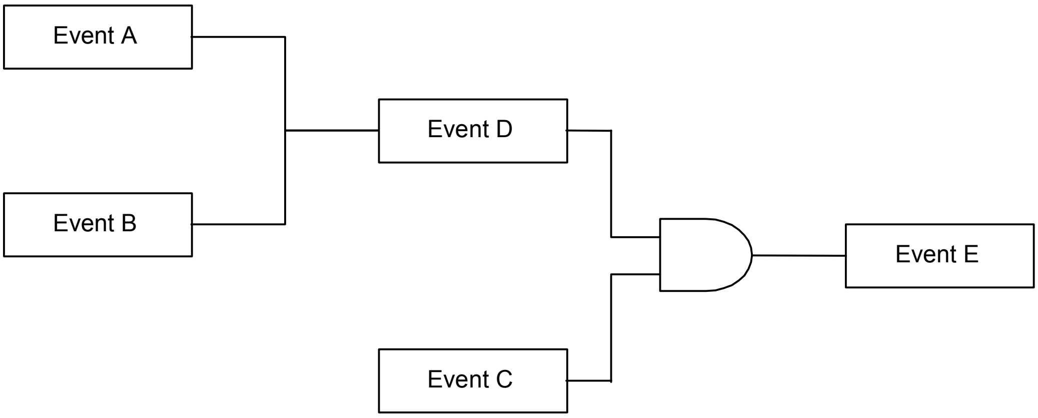


Figure 2 An example of the event chains

The barrier diagram shows the events in boxes. Chronology in the barrier diagrams goes from the left to the right. For instance event A will have happened before event D, but not necessarily before event C. This is similar to most event trees.

Lines from two or more event boxes joining to one line has the meaning of an "OR" connection in a fault tree. "AND" connections are shown with an "AND" box similar to the one used in fault trees.

The next step is the inclusion of the barriers at the chronologically right points in the diagram. This is shown in the figure below. For instance barrier a will prevent event A from developing into event D, assuming that it works.

As step 3 it is evaluated whether any of the barriers will lead to other events that should be described. In the diagram in the figure below barrier c will lead to event F given that the barrier works. For instance, if a pressure safety valve on an ammonia system is venting to the atmosphere it may prevent the equipment from rupturing due to overpressure, but it will then generate a toxic ammonia cloud.

Finally, step 4, the barriers have been coloured to illustrate which barriers are automatic (including passive barriers) and which demand operator intervention to be effective. Usually one will make the automatic barriers black and the manual barriers white, as the automatic barriers are generally considered more reliable (see Figure 3).

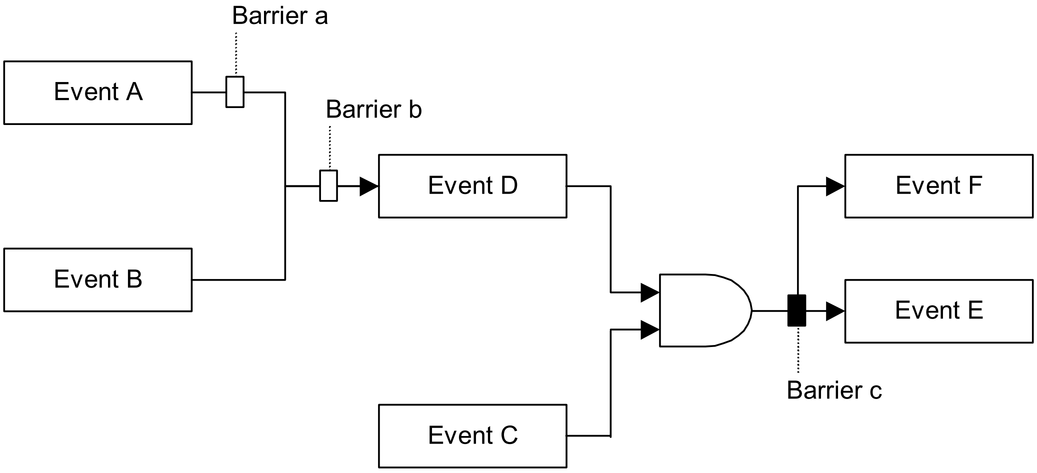


Figure 3 Example of a barrier diagram

Evaluation of barrier diagrams

Once the barrier diagram is finished, the level of safety should be evaluated. This may be done qualitatively or semi-quantitatively. The semi-quantitative method will not be described here.

The purpose of evaluating the barrier diagrams is to determine whether there are sufficient barriers against the undesired events happening, i.e. is the design sufficiently safe.

When evaluating the diagram one must consider:

- The frequency/probability of the initiating events
- The severity of the end events (consequence assessment)
- The number, coverage and reliability of barriers in each of the event chains in the diagram

It is important to evaluate all event chains separately. It may be that the diagram as a whole includes a large number of barriers and that the barriers generally have a good reliability. Still the situation is not satisfactory, if for instance one chain contains only a few or unreliable barriers, or if the success of one barrier leads to another undesirable event.

6 Summary

The way in which risks are assessed still shows a very wide range of approaches within the industry. A number of different approaches to risk assessment have been developed including deterministic, semi-quantitative and quantitative risk techniques. Today some companies and countries make use of all of these whereas others favour the use of Qualitative Risk Assessment [38].

In Germany and France deterministic approaches are used almost exclusively and these are briefly described in the current report.

Probabilistic approach, Quantified Risk Assessment, is favoured by authorities in the Netherlands, the UK and Norway, and sometimes is employed by the authorities and institutions of other European countries. In addition, a number of major companies also find the approach of value. Its greatest value is in plant siting decisions and in the assessment of off-site risks. It may also be of value in assessing more significant on-site risks. Since it concentrates on more severe hazards, the QRA is generally based on a top-down process of hazard identification using what-if or similar techniques. Major hazards such as toxic gas release, explosion etc. can be identified in this way.

In general at the time being the following techniques are used for Hazard Identification: HAZOP, What-If, Checklists, FMEA (Failure Mode and Effect Analysis), functional modelling and concept hazard analysis, fault and event tree analyses. Details on these methods see in Appendix I. Fault and event tree analyses are not described anyhow in the Appendix assuming they are well known and comprehensively described in numerous literatures.

As for the assessment of consequences and effects, the most serious concerns are generally those involving Loss of Containment. In these cases a failure scenario, such as pipeline fracture etc. is postulated and the physical/chemical processes involved are studied. The principle effects considered include release conditions (e.g. adiabatic flash, aerosol formation, rain out etc.), pool fires, jet fires, flash fires, Boiling Liquid Expanding Vapour Explosions, confined explosions (gas and vapour), vapour cloud explosion, dust explosion, gas dispersion and heavy gas dispersion.

Over the last 20 years considerable attention has been devoted to improving the understanding of these processes. Large-scale tests have been undertaken and a number of computer programs have been developed to model the processes involved.

The major problem in the probabilistic approach is the estimation of event probabilities. As with most other forms of risk assessment the events being considered are very rare and 'hard data' on event frequencies is usually not available. The assessment of event likelihood may be made in one of two ways: synthesis (construction of event or fault trees or both) or by the use of generic failure rates.

In recent years there has been an increase in the use of semi-quantitative approach to risk assessment. These generally involve the construction of a 'Risk Grid' or 'Risk Matrix' with one axis as consequences and the other as frequency or likelihood. The 'consequence' axis is usually divided into broad regions such as minor injury, major injury, single fatality and multiple fatalities. The 'frequency' axis is also divided into broad regions such as frequent, occasional, remote, improbable, most improbable. Standard descriptions of each of these categories are then prepared. Once a hazardous event is identified the team uses their judgement to make an assessment of its likelihood and consequences and these are plotted onto the grid. The position is then compared to a criteria line.

7 Acknowledgements

The writing of this report has been partly funded by the SOS-1 project under the Nordic nuclear safety research (NKS), which is gratefully acknowledged.

The description of the Barrier method for decision-making was taken from a text written by COWI Consulting Engineers and Planners A/S as a contribution to a course compendium produced together with Risø National Laboratory. The permission to use the text is gratefully acknowledged.

8 References

1. Jürgen Wettig, New Developments in Standardisation in the Past 15 Years – product versus process related standards, In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
2. Framework for Integrating Socio-Economic Analysis in Chemical Risk Management Decision-Making, OECD Environmental Health and Safety Publications. Series on Risk Management, No. 13, Paris, 2000.
3. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. Official Journal L 183, 29/06/1989 p.1-8.
4. Papadakis G. A. and A. Amendola (Eds.) (1997): Guidance on the preparation of a Safety Report to meet the requirements of Council Directive 96/82/EC (Seveso II). EUR 17690 EN. JRC Ispra.
5. N. Mitchison and Sam Porter (Eds.) (1998): Guidelines on a major accident prevention policy and safety management system, as required by Council Directive 96/82/EC (Seveso II). EUR 18123 EN. JRC Ispra.
6. J. Wettig, N. Mitchison (Eds.) (1999): Explanation and guidelines for the application of the dispensation rule of article 9(6) of Council Directive 96/82/EC (Seveso II), Report EUR 18124, Office for publications for the EC, Luxembourg.
7. Christou, M.D., Porter, S. (1999) Guidance on land use planning as required by council directive 96/82/EC (Seveso II), Report EUR 18695, Office for publications for the EC, L-2985 Luxembourg.
8. B. De Marchi, S. Funtowicz (1994): General Guidelines for Content of Information to the Public. Directive 82/501/EEC - Annex VII. EUR 15946.
9. Papadakis G. A. and Porter, S. (Eds.) (1999): Guidance on Inspections as Required by Article 18 of the Council Directive 96/82/EC (Seveso II). EUR 18692. JRC Ispra.

10. Guidance on the Preparation of a Safety Report to meet the Requirements of Council Directive 96/82/EC (Seveso II), edited by G.A. Papadakis, A. Amendola, EUR 17690 EN.
11. Technical Guidance on Development of Risk Reduction Strategies, Directorate General XI, European Commission, Brussels, 1998.
12. M. Considine, Quantifying Risks in the Oil and Chemical Industry. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
13. C. Kirchsteiger and G. Cojazzi, Summary paper of "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
14. Control of Urban Development Around High-Risk Industrial Sites. Industrial Environment Department, France, 1990.
15. DIN/VDE 31 100, part 2 (Deutshe Norm), Begriffe der Sicherheitstechnik, Beuth Verlag, Berlin 1987.
16. Ullmann's Encyclopaedia of Industrial Chemistry, Volume B8, Environmental Protection and Industrial Safety II, Plant and Process Safety, 1995
17. K.A. Ruppert, The application of the Term "Risk" from the Viewpoint of German Chemical Industry. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
18. B.J.M. Ale, Risk Assessment Practices in the Netherlands. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
19. Integrale Nota LPG, Tweede Kamer der Staten General, vergaderjaar 1983-1984, 18233 nrs 1-2, SDU, Den Haag, The Netherlands.
20. Premises for Risk Management, Second Chamber of the States General, session 1988-1989, 21137 no. 1-2.
21. J.C.H.Schuller at al. Methods for determining and processing probabilities. "Red Book", (CPR 12E) RIVM, 1997
22. P.A.M. Uijt de Haag and B.J.M. Ale, Guidelines for Quantitative Risk Analysis. "Purple Book", (CPR18) RIVM, 1999.
23. Methods for the calculation of physical effects. "Yellow Book", Part 1, (CPR 14E), RIVM, 1997 (Third edition).
24. Methods for the calculation of physical effects. "Yellow Book", Part 2, (CPR 14E), RIVM, 1997 (Third edition).
25. Methods for the determination of possible damage. "Green Book", (CPR16E), RIVM, 1992.
26. B.J.M. Ale and M. Piers, Dealing with third party risk around a major airport, in L.H.J. Goossens (ed.) Risk Analysis, Facing the New Millennium, Delft University Press, Delft, 1999, ISBN 90 407 1954 3.
27. B.J.M. Ale and M. Piers, The assessment and management of third party risk around a major airport, JHazMat, vol. 71 nos. 1-3, p. 1-16, 2000, ISSN 0304 3894.
28. E. Smith, Risks to Third Parties in the Vicinity of Airports – the Aircrash Program. In A. Mosleh and R.A. Bari (eds.), Probabilistic Safety Assessment and Management, Springer, September 1998.
29. Cowell et al, A methodology for calculating individual risk due to aircraft accidents near airports, NATS R&D Report 0007, January 2000.
30. CUR, Civieltechnisch Centrum Uitvoering Research en Regelgeving, Kansen in de civiele Techniek, Uitgave Directoraat Generaal Rijkswaterstaat, Den Haag, 1997.
31. A guide to the Control of Major Accident Hazards Regulations 1999 (COMAH), Guidance on Regulations, Draft 24/2/1999, HSE
32. A.Brandsæter, Risk Assessment in the Offshore Industry. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
33. A.Altavilla and L.Garbellini, Risk Assessment in the Aerospace Industry. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.
34. D.Ball and P.Floyed, Societal Risks. Report to the UK Health and Safety Executive, Risk and Policy Analysts Ltd, Norwich, 1998
35. R.Travis et al., Cancer Risk Management, Environmental Science and Technology, vol. 21, No. 5, 1987, pp. 415-420.

36. Environment Canada. Generic Outline for an Options Evaluation Study, Economic Analysis Branch of Environment Canada, Environment Canada, Ontario, 1994.
37. J.Hokkanen and J.Pellinen. The Use of Decision-aid Methods in the Assessment of Risk Reduction Measures in the Control of Chemicals, Nordic Council of Ministers, Copenhagen, 1997.
38. R.D. Turney, Application of Risk Assessment in the Process Industry. In Proceedings "Promotion of Technical Harmonisation on Risk-Based Decision-Making", 22-24 May 2000, Stresa/Italy.

Appendix I

Hazard identification techniques

What-if/Checklist analysis

What-if/Checklist analysis consists of two analysis types combined, What-if and Checklist. The methodology has a wide area of applicability. It can be used at all stages of a project from the beginning at the conceptual design.

The what-if part of the analysis is a brainstorming based analysis, which however is somewhat structured. A group of experienced persons familiar with the processes analysed is encouraged by the study leader to raise questions and concerns about the design analysed. Typically the questions raised will be starting with "What if .... ?". Examples may be "What if the compressor is filled with air during start-up?". The concerns may however be raised in any form, regardless of whether it includes a "what if" phrase.

The analysis normally includes the following steps:

1. Raise questions for any part of the system that come to you easily.
2. Divide the questions into types or large process sections.
3. Raise new questions going through the sections one at a time.
4. Answer the questions one by one regarding causes, consequences, and safeguards.
5. Formulate actions where appropriate.

The basis of the analysis should be the latest process and layout drawings, procedures, descriptions etc. The team analysing the process should include expertise within all relevant fields, e.g. process, instrumentation, operation, and maintenance. At this type of analysis it is very important that the team members are very competent, whereas the leader may be less experienced than for instance the HAZOP leader.

The results are recorded in schemes like the one below:

What-if	Causes	Consequences	Safeguards	Actions

The checklist analysis is a systematic approach based on safety standards and experience. A checklist consists of a number of items to check concerning specific features, e.g. concerning specific process equipment or substances.

An example may be concerning pressure and vacuum relief: "Is the relief system designed for two-phase flow, and should it be? "

Checklists can be found in relevant literature, for instance (CCPS 1992) or (Lees 1996).

Hazard identification based on plant functional modelling and CHA.

Ideally, hazard identification should begin as early as possible in the design and then expanded, as more detail becomes available: unfortunately, the majority of existing hazard identification methods do not allow this. HAZOP requires at least a definition of the design to flowsheet level. Conversely, those methods intended for the conceptual stages of design, such as checklists and "What If?" are difficult to expand once more detail is available.

Furthermore, the emphasis of these methods is on the identification of hazards closely related to the plant hardware.

One way to structure the concept hazard analysis is to prepare a system model that can form the basis for the subsequent hazard identification. The system models can be based on the concept of functional modelling which has been applied in several research projects and practical examples, and it has been found that the modelling techniques offer a complete and consistent representation of a complex system (Rasmussen & Whetton 1997). The concept creates a frame in which structural, operational and managerial aspects can be integrated, performing a systematic and comprehensive description of a complex industrial installation. The hierarchical form of the model provides a good basis for getting an overview of safety issues and it will form a suitable basis for internal and external dialogues on safety matters and planning.

The plant model follows a general framework as indicated in Figure 1. The basic idea is that a set of plant functions links together hardware, software, operations, work organisation and other aspects of the plant.

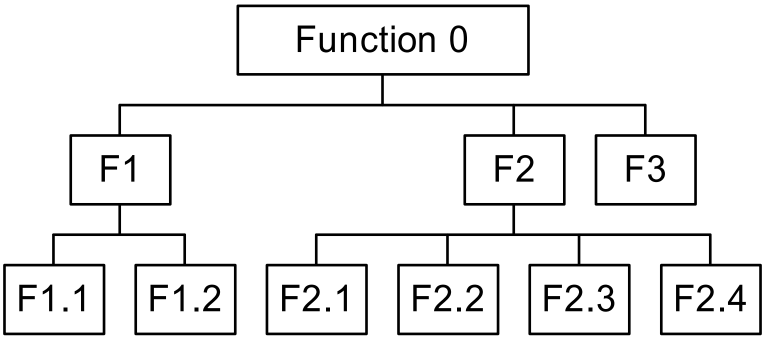


Figure 1.Functional decomposition of a process plant as a hierarchy of functional objects

The principle of functional modelling is that any aspect of the activity can be represented by an object based upon an Intent or goal and associated with each Intent are Methods, by which the Intent is realised, and Constraints, which limit the Intent. The Methods and Constraints can themselves be treated as objects and decomposed into lower-level Intents (hence the procedure is known as functional decomposition), so giving rise to the method's hierarchical structure. A diagrammatical model is presented in Figure 2, which follows the usual conventions of the SADT (Structured Analysis & Design Techniques) method of systems analysis.

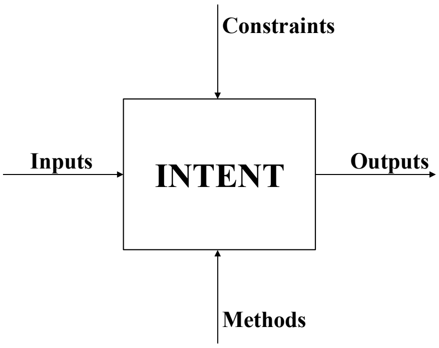


Figure 2. Diagrammatical functional model

In the plant functional model, a function is an object comprising an Intent, a list of one or more Methods, which are used to satisfy that Intent, and a list of zero or more Constraints, which impose restrictions upon the Intent. A simple semantic model is:

<Intent> by <Method> with <Constraints>

Hence, the functional model contains objects whose elements can be classified as follows:

- Intents representing the functional goals of the specific activities in question.
- Methods representing items (hardware, procedures, software, etc.) that are used to carry out the Intent or operations that are carried out using those items.
- Constraints that describe items (physical laws, work organisation, control and protective systems etc.) that exist to supervise or restrict the Intent.
- Inputs are the necessary conditions to perform the Intent and the link to the previous Intent. Inputs can be either transformed or used during the performance of the Intent in order to produce the Outputs.
- Outputs show the outcome produced by the Intent and the link to the subsequent Intent.

The modelling principle is a top-down approach, which ensures a logical functional model of the activity. The usual starting point will be a process flowsheet and from this, the functional decomposition is performed, ensuring that all relevant activities are considered. The main purpose of the functional model is to provide a frame for high-level hazard identification, in which case the model may be stopped at one of the higher levels. The intention is to identify at each level those parts of the system where further analysis is required, meaning that the degree of detail will differ for the different parts of the system. The basic principle of the functional modelling in which any aspect of the plant can be represented as *Intent by Method with Constraint* is a valuable way of thinking to ensure that all safety aspects have been considered. It cannot be over-emphasised that it is more important to ensure that all those objects, which affect safety, are included than to be concerned as to whether or not they are included exactly in the right place.

The system model can be developed and presented in two different ways: tabular or graphical form. Choosing a tabular presentation form will make it easier to develop a frame for the overall hazard identification as the worksheet from the functional model can easily be linked to the worksheet of a Concept Hazard Analysis, CHA, see e.g. Wells, 1996.

The functional model can be contained in a three-column worksheet as shown on the left-hand side in the table where the "Ref" column is used for numerical reference. The "T" column is used to indicate the type of object (I for Intent, M for Method, C for Constraint). The "description" column contains an imperative statement that forms the Intent, Method or Constraint.

Function			Concept Hazard Analysis				
Ref	T	Description	Keyword	Main variance (dangerous disturbance)	Conse-quences	Mitigation	Notes

Tabular presentation form.

Having a system model the next step is to perform the preliminary hazard identification in the form of a Concept Hazard Analysis (CHA, see e.g. Wells, 1996) which can be carried out in structured group sessions. Checklists and keywords guiding and structuring the analysis will support the users in the group session. Typically ten to twenty keywords are selected in order to carry out a preliminary hazard identification which is performed in the following way:

- Keywords are taken from a prepared list and applied to each selected plant section in turn. By discussion amongst the team, this is used to generate a “main variance” on the analysis form.
- Each item is checked for known hazards.
- Identify the consequences of each main variance or disturbance,
- Determine if the hazards can be designed-out or if the hazards can be otherwise reduced or eliminated.
- Determine any controls or mitigation.
- Determine any comments and actions.

Table 1. Keywords in Concept Hazard Analysis (Wells, 1996)

Substances and reactions	substances separations reactions
Fires and explosions	fires explosions
Release and discharge	flammables thermal radiation toxics bacteria radioactivity pollutants noise adverse discharge handling electrical/radiation
Dangerous disturbances	exceeding mechanical limitations physical explosions chemical explosions reaction overtemperature overpressure undertemperature underpressure overload/stress/tension impact blow/drop critical defect in construction abnormal opening adverse change in product discharge
Notable disturbances	equipment problems reactions material problems utility problems mode of operation
External threats	extreme weather force majeure, sabotage

Table 1 contains a list of generic keywords. This list can be extended as needed, but as occurs in all such methods there is a tendency for the number of keywords to be increased until eventually the method begins to lose its value.

As an example, we show part of the CHA based on functional modelling of the production of PMP (formula: $C_{16}H_{16}N_2O_4$). The overall plant Intent has been defined as Produce PMP. The Methods and Constraints related to the overall Intent have been defined on basis of the overall plant structure. This has resulted in the following first level objects in the functional model of the PMP plant:

Intent	Produce PMP
by	
Method	Provide raw materials
Method	Pre-treatment
Method	Reacting
Method	Post-treatment
Method	Store final product
Method	Manage the operation
Method	Support the operation
with	
Constraint	Protect the environment from the plant
Constraint	Protect the plant from the environment

The following table presents the results for the Method “Provide NaOH”, which is a subdivision of the Method “Provide raw materials”.

Function			**Concept Hazard Analysis**				
Ref	**T**	**Description**	**Keyword**	**Main variance (dangerous disturbance)**	**Consequences**	**Mitigation**	**Notes**
1.4.0	I	Provide NaOH					
1.4.1	M	Warehouse operations	Chemicals: Corrosion	Release during storage	Chemical exposure, corrosion	Regular inspection of storage	
1.4.2	M	Load NaOH drum onto truck		Release during handling		Handling procedures	
1.4.3	M	transport by truck to local storage		Release during transport		Transportation procedures	
1.4.4	M	Unload from truck into local storage		Release during handling		Handling procedures	
1.4.5	C	Operation manual	Working practice	Procedures not followed			

HAZOP Study

HAZOP (HAZard and OPerability) study was developed by ICI in the late 1960s. The technique was developed to identify hazards in a process plant and to identify the operability problems that though not hazardous could compromise the plant’s ability to achieve design productivity. Operability includes such matters as the ability to start-up, to shut-down, to control the operations and to maintain the facility.

Different types of HAZOP studies exist.

-Process HAZOP study
-Procedure HAZOP study
-HAZOP study of emergency systems
-HAZOP study of computer based systems

The most commonly used for process plants is the Process HAZOP study. This method is mainly concerned with the processes and the process equipment. By using this study method, most situations in which the plant will not function well can be found, both relating to normal operation, to system interactions and to disturbances. Human error due to maloperation of the plant is more difficult (but not impossible) to find by this method.

In a Procedure HAZOP the procedures for operating the plant are studied. This method is very useful for finding possible operating errors, e.g. due to incomplete procedures. This method will not be described further here.

Process HAZOP study

The approach taken is to form a *multidisciplinary team* that works together to identify hazards and operability problems by searching for causes and consequences of process deviations from design intents. An experienced team leader systematically guides the team through the plant design using a set of guide words.

The team will normally consist of 4-10 persons including a HAZOP leader, HAZOP secretary, and relevant persons representing operation, maintenance, process, instrumentation, and health, safety and environment.

The process is systematic and it is helpful to define the terms that are used:

- ***Study nodes / sections*** The locations (on piping and instrumentation drawings) at which the process parameters are investigated for deviations.
- ***Intention*** The intention defines how the plant is expected to operate in the absence of deviations at the study nodes. This can take a number of forms and can either be descriptive or diagrammatic, e.g. flowsheets, line diagrams, P&IDs. It is recommended, that as a minimum a descriptive intention is stated on the HAZOP work sheet.
- ***Guide words*** These are simple words that are used to qualify or quantify the intention in order to guide and stimulate the brainstorming process and so discover deviations. Each guide word is applied to the process variables at the point in the plant (study node) which is being examined (e.g.; "no", "high" etc.).
- ***Deviations*** These are departures from the intention which are discovered by systematically applying the guide words to the process variables (e.g., “high pressure”).
- ***Causes*** These are the reasons why deviations might occur. Once a deviation has been shown to have a credible cause, it can be treated as a meaningful deviation. These causes can be hardware failures, human errors, an unanticipated process state (e.g., change of composition), external disruptions (e.g., loss of power), etc.
- ***Consequences*** These are the results of the deviations should they occur (e.g., release of toxic materials). Trivial consequences, relative to the study objective, are dropped.
- ***Safeguards*** These are, for instance, the safety equipment incorporated in the design of the plant. This could be alarms, shutdown valves, emergency equipment etc. Process equipment designed for instance to regulate the flow in a pipeline is not considered safety equipment. However it is regarded as a safeguard if its function is independent of the cause of the deviation.

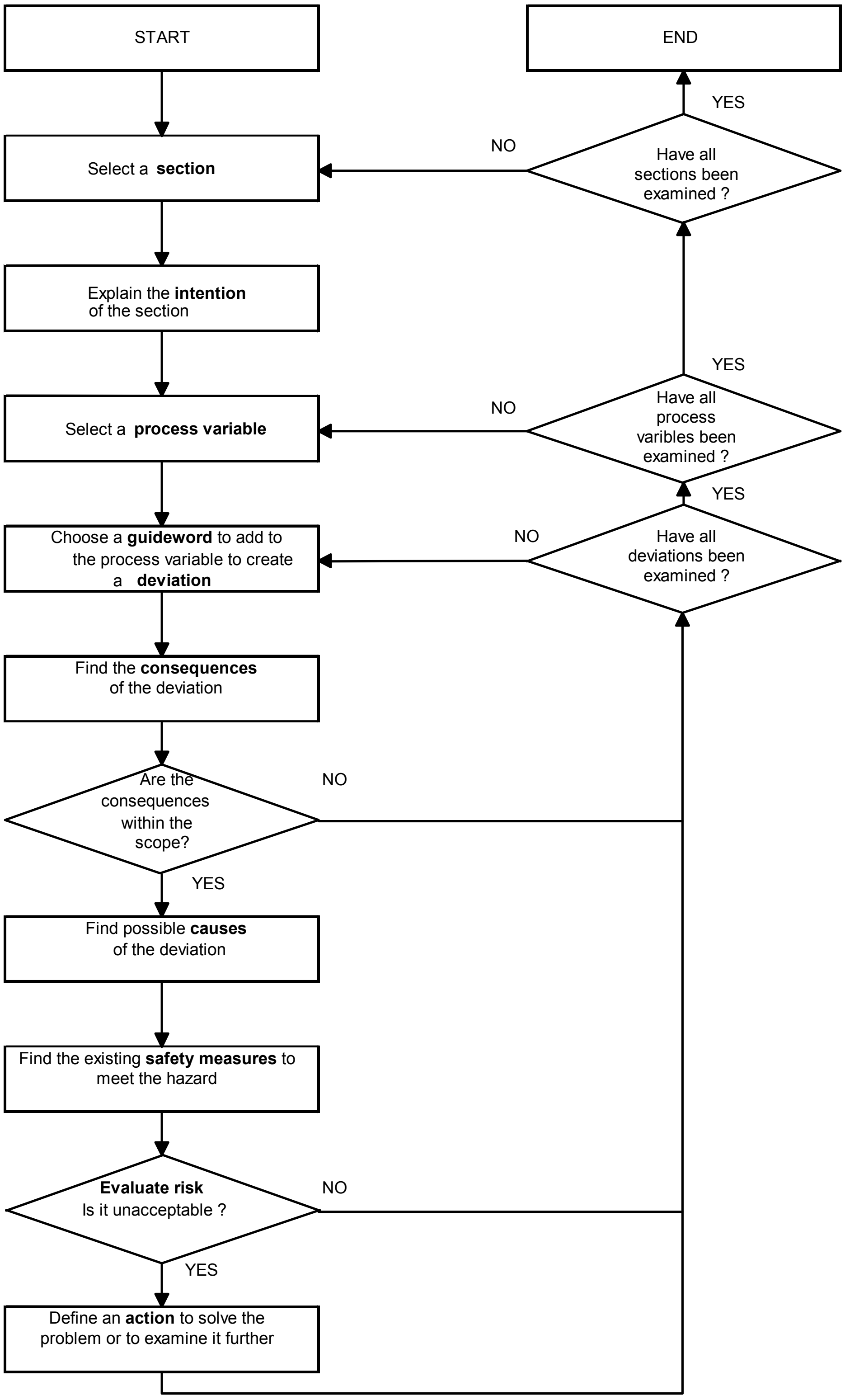
The guide words normally used and process variables are shown in the table below together with the resulting deviations.

Guide word Process-variable	No	Low	High	Part of	Also	Other than	Reverse
Flow	No flow	Low flow	High flow	Missing ingredients	Impurities	Wrong material	Reverse flow
Level	Empty	Low level	High level	Low interface	High interface	-	-
Pressure	Open to atmosphere	Low pressure	High pressure	-	-	-	Vacuum
Tempe-rature	Freezing	Low temp.	High temp.	-	-	-	Auto refrigeration
Agitation	No agitation	Poor mixing	Excessive mixing	Irregular-mixing	Foaming	-	Phase separation
Reaction	No reaction	Slow reaction	"Runaway reaction"	Partial reaction	Side reaction	Wrong reaction	Decom-position
Other	Utility failure	External leak	External rupture	-	-	Start-up Shutdown Maintenance	-

A HAZOP study requires access to detailed plant descriptions, such as drawings, procedures and flow charts. A HAZOP also requires considerable knowledge of the process, instrumentation and operation, and the team members usually provide this information. The results of the study are normally qualitative including:

- Identification of hazards and operability problems
- Actions related to recommended changes in design, procedures etc.
- Actions related to recommendations for follow-up studies where no conclusions were possible due to lack of information or knowledge. Follow-up studies may also be further hazard analysis by use of fault trees, event trees, or consequence assessment.

The HAZOP methodology is shown schematically in the figure below.



START
END
YES
NO
Select a section
Have all sections been examined ?
Explain the intention of the section
YES
NO
Select a process variable
Have all process varibles been examined ?
YES
Choose a guideword to add to the process variable to create a deviation
NO
Have all deviations been examined ?
Find the consequences of the deviation
Are the consequences within the scope?
NO
YES
Find possible causes of the deviation
Find the existing safety measures to meet the hazard
Evaluate risk Is it unacceptable ?
NO
YES
Define an action to solve the problem or to examine it further

Documentation of HAZOP

The HAZOP analysis is documented in a HAZOP-worksheet.

The following example is taken from (CCPS 1992). The following table presents a sample HAZOP worksheet for a specific node in a process unit for Di-Ammonium Phosphate, DAP production, considering the deviation *High flow*.

Deviation	Causes	Consequences	Safeguards	Actions
High flow	Ammonia feed to line control valve A fails open Operator sets ammonia flow rate too high Flow indicator fails	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Periodic maintenance of valve A Ammonia detector and alarm	Ensure periodic maintenance and inspection for valve A is adequate Consider adding an alarm/ shut-down of the system for high ammonia flow to the reactor

Example of HAZOP worksheet (CCPS, 1992)

This example is however very simple. Information about what have been analysed, intention of the section, design- and operating conditions, who have participated in the analysis, who are responsible for carrying out actions shall preferably be stated in the HAZOP worksheet.

Failure mode and effect analysis (FMEA)

FMEA is a tabulation of the system/plant equipment, their failure modes, each failure mode's effect on the system/plant, and a critical ranking for each failure mode. A FMEA study starts from the single component. The failure mode is a description of how equipment fails (open, closed, on, off, leaks, etc.). The effect of the failure mode is the system response or accident resulting from the equipment failure. Human errors are generally not examined systematically in a FMEA. FMEA represents a "bottom up" approach and one of the drawbacks of a FMEA is that it examines just one plant component at a time, and does not treat multiple failures, or the effect of latent failures. A FMEA can be presented in a tabular form as illustrated in the table. Usually FMEA is used in combination with a Fault Tree Analysis.

The FMEA method is more often carried out for electrical systems than for process systems, for which the HAZOP method is more common. FMEA can be carried out by a single analyst, but better results are obtained with a small group (CCPS, 1992).

Component	Failure mode	Cause	Effects and detection	Measures

Selection of hazard analysis method for a given case

Each of the hazard analysis methods mentioned in this chapter has its strong and its weak points. The decision of which method to use in a given case, therefore, will depend much upon the problem to be analysed. Below we give some general hints to help in the selection. A more detailed description can be found in (CCPS 1992).

Some main categories of factors that can affect the selection of analysis techniques are the following:

- Motivation for the study (e.g. risk management purposes or fulfilment of regulatory requirements)
- Type of results needed (e.g. list of hazards, potential accident situations, risk reducing measures, input for quantitative risk analysis)
- Type of information available to perform the study (P&I diagrams, drawings, operational experience)
- Characteristics of the analysis problem (e.g. complexity, size, type of process, type of operations, inherent hazards)
- Perceived risk associated with the subject process or activity (the higher the perceived risk, the more important to assure completeness of the hazard identification)
- Resource availability (analyst's skills, financial)
- Analyst's preference

One very decisive factor in the selection process is the type and amount of information available for the study. This factor in itself depends on the stage of the plant's lifetime being considered. The table below shows a general picture of which methods are suited for use at different stages.

	Functional modelling	Checklist	Relative ranking	Preliminary hazard analysis	What-if	What-if/ Checklist	HAZOP	FMEA	Fault tree analysis	Event tree analysis	Cause-consequence analysis
Conceptual design	X	X	X	X	X	X					
Pilot plant operation	X	X		X	X	X	X	X	X	X	X
Detailed engineering		X		X	X	X	X	X	X	X	X
Construction/Start-up	X	X			X	X					X
Routine operation	X	X			X	X	X	X	X	X	X
Expansion or modification	X	X	X	X	X	X	X	X	X	X	X
Incident investigation					X		X	X	X	X	X
Decommissioning		X			X	X	X				

References

- CCPS (Center for Chemical Process Safety) (1992). *Guidelines for Hazard Evaluation Procedures.* American Institute of Chemical Engineers, New York.. ISBN 0-8169-0491-X
- Lees, F.P. (1996) Loss Prevention in the Process Industries. Butterworth & Co.
- Rasmussen, B.; Whetton, C. (1997). “Hazard identification based on plant functional modelling”, *Reliability Engineering & System Safety,* 55, 77-84.
- Wells, G. (1996), *Hazard identification and risk assessment,* Institution of Chemical Engineers, Rugby, Warwickshire CV21 3HQ, UK.

Bibliographic Data Sheet **NKS-21**

Title	Safety- and risk analysis activities in other areas than the nuclear industry
Author(s)	Igor Kozine, Nijs Jan Duijm and Kurt Lauridsen
Affiliation(s)	Risø National Laboratory, Roskilde,Denmark
ISBN	87-7893-071-5
Date	December 2000
Project	NKS/SOS-1
No. of pages	46
No. of tables	10
No. of illustrations	6
No. of references	38+4
Abstract	The report gives an overview of the legislation within the European Union in the field of major industrial hazards and gives examples of decision criteria applied in a number of European countries when judging the acceptability of an activity. Furthermore, the report mentions a few methods used in the analysis of the safety of chemical installations.
Key words	Seveso directive, risk analysis, safety analysis, hazard identification techniques, decision criteria, chemical industry, off-shore industry

Available on request from the NKS Secretariat, P.O.Box 30, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@catscience.dk, www.nks.org.