EU Project No: SMT4-CT97-2169

The RASE Project

Explosive Atmosphere: Risk Assessment of Unit Operations and Equipment

Report:

Methodology for the Risk Assessment of Unit Operations and Equipment for Use in Potentially Explosive Atmospheres

Project Co-ordinator:

Dr. R. L. Rogers, INBUREX GmbH

Project participants:

INBUREX	**Germany**
HSE	**England**
FSA	**Germany**
INERIS	**France**
NIRO	**Denmark**
CMR	**Norway**

Date: 17th March 2000

Important Information for Readers

This report has been prepared as part of the RASE Project – "Explosive Atmosphere: Risk Assessment of Unit Operations and Equipment" A joint industry / European Commission Project under the dedicated call of the European Commission's Standards Measurement and Testing programme concerned with subjects relating to the standardisation activities of CEN.

The RASE project objective was to develop a Risk Assessment Methodology for Unit Operations and Equipment to help manufacturers of equipment and protective systems intended for use in potentially explosive atmospheres meet the requirements of the EU Directives 89/392/EC (machinery directive) and 94/9/EC (ATEX 100A). It will also be useful to satisfy the requirement in Directive 99/92/EC (ATEX 137A) for users of such equipment to produce an explosion protection document. It is intended that the results of the RASE project be incorporated into this standard by the relevant working group CEN/TC305/WG4.

In the project a review of the current status was carried out in which a questionnaire was developed and replies received from over 200 manufacturers and users and a review of existing risk assessment techniques carried out. A draft risk assessment methodology was developed and used in trials with equipment manufacturers. These showed that the basic framework of the developed methodology was suitable and that when the suggested proformas were used for recording the results, the risk assessment which has been carried out can be clearly followed. However it was clear from the trials that manufacturers have extreme difficulty in applying the methodology. as the subject of risk assessment is extremely complex and it is unlikely that someone without experience in the field can simply take the proposed draft and directly apply it to their problem. The project team therefore developed and included a 'User-Guide' which contains detailed examples of the use of the methodology for assessing the risk associated with different types of equipment and unit operations. The completed draft of the risk assessment methodology is now being widely circulated for comments and has been passed to the relevant technical committees of CEN and CENELEC for further development into a European standard.

The RASE project is co-ordinated by INBUREX in Germany with the participation of FSA Germany, INERIS France, HSE England, NIRO Denmark and CMR Norway. The project started in Dec 1997 and is due for completion in May 2000.

Further information about the RASE project can be obtained from the Project Co-ordinator:

Dr. R.L. Rogers
Inburex GmbH
Wilhelmstr.2, D-59067 Hamm, Germany
Tel +49 2381 271610 Fax +49 2381 271620
Email Richard.Rogers@inburex.com

In the interests of promoting process safety this document is provided for open circulation. Where the document of parts thereof are used the following acknowledgements should be made:

> *The RASE project (Risk Assessment of Unit Operations and Equipment) is a joint industry / EU Commission project carried out under Contract No: SMT4-CT97-2169. The project is co-ordinated by INBUREX in Germany with the participation of FSA, INERIS, HSE, NIRO and CMR.*

This document can be down loaded from the 'Library Area' of the SAFETYNET web site www.safetynet.de

RASE Project Participants

Dr. R.L. Rogers
Dr. B. Broeckmann
Inburex GmbH
Wilhelmstr 2
D-59067 Hamm
Deutschland

Tel: +49 (0) 2381 271610
Fax: +49 (0) 2381 271620
email:
Richard.Rogers@inburex.com
Bernd.Broeckmann@inburex.com

Ms N. Worsell
Health and Safety Laboratory
Broad Lane
S3 7HK Sheffield
England

Tel: +44 114 289 2635
Fax: +44 114 289 2444
email:
nicola.worsell@hsl.gov.uk

Prof. Dr. S. Radandt
Dr. K.-H. Grass
FSA eV
Dynamostr. 7-9
D-68136 Mannheim
Deutschland

Tel: +49-621-4456-3401
Fax: +49-621-4456-3402
email:
radandt@bgn.de
grass@bgn.de

Dr. J-P. Pineau
Ms C. Loyer
INERIS
Parc Technologique Alata B.P. 2
F-60550 Verneuil en Halatte
France

Tel: +33 3 44 55 65 14
Fax: +33 3 44 55 66 55
Email:
Jean-Philippe.Pineau@ineris.fr
Celine.Loyer@ineris.fr

Mr.C. Schwartzbach
Niro A/S
Gladsaxevej 305
DK-2860 Soeborg
Denmark

Tel: +45 3954 5437
Fax: +45 3954 5800
email: cs@niro.dk

Dr. K. van Wingerden
CMR
Fantoftvegen 38
N-5036 Fanthoft
Norway

Tel: +47 55 57 4316
Fax: +47 55 57 4041
email: kees@cmr.no

Contents

Informative Annexes

0 Introduction

Risks arising from the hazard of an explosion are described in the Machinery Directive and further developed in the ATEX Directive 94/9/EC. In terms of producing a safe machine, piece of equipment or protective system the principles of Safety Integration are the core of both Directives and should be fully understood before any work is started on the design. The strategy gives the following approach:

- Carry out a risk assessment to identify and evaluate any relevant hazard and on the basis of the risk assessment
- eliminate or minimise the risks by
  - Design measures;
  - Provision of protective devices;
  - Provision of information on residual risks;
  - Details of any precautions needed to be taken.

Essential Health and Safety Requirement 1.5.7 (Explosion) of the Machinery Directive overlaps the requirements of the ATEX Directive 94/9/EC. However, Article 1.4 of the Machinery Directive states that where there is another Directive dealing with a specific risk that Directive will take precedence over the Machinery Directive for that particular risk. Therefore in order to comply with the Essential Health and Safety Requirement 1.5.7 of the Machinery Directive, it is necessary to comply with the ATEX Directive. If there is an explosion risk which is outside of the scope of the ATEX Directive then the original Machinery Directive will apply.

The manufacturer can choose one of the two ways of conforming with the technical measures required by the Directive:

- Interpret the technical measures directly from the Essential Health and Safety Requirements or
- use a Harmonised European Standard produced by CEN/CENELEC under a mandate and placed in the Official Journal of the CEC.

For all machines, equipment and protective systems with a potential explosion hazard, compliance with the requirements of the Machinery Directive and the ATEX Directive can be achieved by following the principles contained in EN 292 Machinery Safety, EN 1050 Risk Assessment and EN 1127-1 Explosion Prevention and Protection.
This standard applies the principles contained in these standards to the specific requirement of carrying out a risk assessment considering the hazard of an explosion.

This type A standard describes principles for a systematic procedure for risk assessment of hazardous situations arising from explosive atmospheres in the following cases:

- an intended internal explosive atmosphere is present during normal operation or when a malfunction occurs, within the equipment causing a possible release to the surroundings,
- the explosive atmospheres pre-exist in the surroundings.

Such being the case, explosion risks shall be assessed overall.

This standard follows the Directive 94/9/EC, the so-called ATEX 100a - Directive. Its objective is to eliminate or at least minimise the risks resulting from the use of certain products in or in relation to a potentially explosive atmosphere. Therefore, ATEX 100a Directive is a risk-related Directive and consequently a risk assessment has to be made. This is a challenge, because the traditional approach to safety in the process industries was an ad-hoc one of learning from experience.

Compliance with the essential health and safety requirements of ATEX 100a Directive is imperative in order to ensure that equipment and protective systems do not pose a hazard in explosive atmospheres. The requirements are intended to take account of existing or potential hazards deriving from the design and construction. However, following the philosophy of ATEX 100a Directive the notion of intended use is also of prime importance. It's also essential that manufacturers supply full information which is required for the safe functioning of equipment and protective systems.

To meet the requirements of ATEX 100a Directive it's therefore absolutely necessary to conduct a risk assessment. Due to item 1.0.1 of Annex II manufacturers are under an obligation to design equipment and protective systems from the point of view of integrated explosion safety. Integrated explosion safety mainly refers to preventing the formation of explosive atmospheres as well as sources of ignition and, should an explosion nevertheless occur, to halt it immediately and / or to limit its effects. Thus the manufacturer must take measures to deal with the risks of explosion. In addition, as required in item 1.0.2 of the Directive, equipment and protective systems must be designed and manufactured after due analysis of possible operating faults in order as far as possible to preclude dangerous situations.

Bearing in mind these commitments resulting from the correct application of ATEX 100a Directive requirements, a methodology on risk assessment should

not only deal with designing and constructing aspects but also identify the information which has to be supplied for safe use.
Thus the risk assessment should cover all aspects of the use of the equipment including, for example, start up, shut down and possible disturbances to ensure that the various safeguards and / or safety barriers are effective and that the user/operator is aware of the safety concepts and their operation.

It is in both the manufacturer's and user's interest to establish a common methodology for achieving safety, reliability and efficacy in functioning and operating of equipment and protective systems with respect to the risks of explosion. In this respect, risk assessment is a tool which provides the essential link between manufacturers and users. Whereas the products must be used in accordance with the equipment group and category and with all the information supplied by the manufacturer, often the severity or consequences of an incident can only be defined by the users themselves. Thus both the knowledge base of the manufacturer plus the plant specific experience of users is required to carry out an effective risk assessment. Detailed harmonised standards cannot be developed for all types of assemblies, therefore this standard is intended to help the manufacturer carry out a risk assessment and to select one or more appropriate methods of risk assessment. The same methods may also be applied by the user, where he is responsible for designing and building a process plant, using components bought from many sources. In this case a risk assessment is also required as part of the explosion protection document required under the ATEX 137 Directive.

In this context this standard is a guideline for explosion prevention and protection by means of risk assessment. It sets the structure of what needs to be done with respect to the Risk Assessment of Equipment and Unit Operations for use in potentially explosive atmospheres and an indication of how to do this. A detailed description of how to carry out a Risk Assessment of a specific type of equipment will be reserved to Type C standards.

It's important to recognise that the ATEX 100a Directive defines various categories of equipment which must be capable of functioning to the required level of protection measures in conformity with the operational parameters established by the manufacturer.
It follows that the performance of the protection measures as well as the conditions of operation are aligned to the protection level required by the various categories. Therefore there exists a relation between categories, performance and conditions of operation (see table 1).

It is clear that before a risk assessment can be carried out, the manufacturer must decide which category of equipment is to be achieved taking into account the protection level required and its intended use.

The way in which the categorisation has been developed highlights one of the main distinctions of Group I and II.
For Group I, the categorisation depends on, amongst other factors, whether the mining equipment is to be de-energised in the event of an explosive atmosphere occurring.
For Group II, it depends on which “Zone” the equipment is intended to be used in, and whether a potentially explosive atmosphere is always present, or is likely to occur for a long or a short period of time.

The “Zone” indicates the likelihood that a potentially explosive atmosphere is present i. e. whether it is always present, present for a long period of time or seldom present. The definitions for the different zones for both gas and dust atmospheres is given in EN 1127-1.

LEVEL OF PROTECTION	CATEGORY Group I	CATEGORY Group II	PERFORMANCE OF PROTECTION	CONDITIONS OF OPERATION
Very High	M1		Two independent means of protection or safe even when two faults occur independently of each other.	Equipment remains functioning when explosive atmosphere present
High	M2		Suitable for normal operation and severe operating conditions	Equipment de-energised when explosive atmosphere present
Very High		1	Two independent means of protection or safe even when two faults occur independently of each other.	Equipment remains functioning in Zones 0, 1, 2 and 20, 21, 22
High		2	Suitable for normal operation and frequently occurring disturbances or equipment where faults are normally taken into account	Equipment remains functioning in Zones 1,2 and/or 21,22
Normal		3	Suitable for normal operation	Equipment remains functioning in Zone 2 and/or 22

Table 1: Various categories of equipment in conformity with certain levels of protection

1. Scope

A methodology on Risk Assessment should consider the risk of harm to human as well as environmental and property damage resulting from explosion risks. In the case of an undesired event the effective range of an explosion often depends on a multiplicity of factors some of which are not easy to anticipate.

This standard establishes general principles for the procedure known as risk assessment when explosive atmospheres are present for any reason and can create hazardous situations.

The knowledge and experience of the design, use, incidents, accidents and damage related to these situations are brought together in order to assess the risks during all phases of the life of an item of equipment or protective system.

The type of equipment that the methodology is aimed at comprises all products covered by the ATEX 100a Directive. The term “product” covers equipment, machines, protective systems, apparatus, devices, components and their combinations.

Products can be divided as follows:

1. Components, - these can be considered to include bearings, terminals, flameproof enclosure, heating elements

2. Equipment, – this can be considered to include small discrete items such as motors, gearboxes, brakes, switches, lights, pumps

3. Complete machines or equipment, – these can be considered to be characterised by fairly simple controls, such as vacuum cleaner, aerosol can filling machine, spray dryer, bucket elevator

4. Complex products, - these can be considered to be characterised by complex controls, perhaps with incorporated protective systems etc. and made up of several discrete items, such as petrol pump, self-contained distillation unit, lift truck, oilseed extraction plant

5. Autonomous protective systems,– these can be considered to include flame arrestors, pressure-relief systems, explosion suppression systems, explosion decoupling systems, etc.

The complexity of a risk assessment will be different for different types of products. For a simple product like a friction clutch, where all the failure modes can be readily identified, the risk assessment will be simple. Some of the more complex techniques described in this standard will then not be applicable, however the basic methodology described remains applicable and should be applied.

It should be recognised that components being safe and explosion proofed are necessary for the safe functioning of ATEX products. However, safe components do not guarantee explosion prevention and protection of ATEX products even if the components have undergone successful testing. Therefore, the ATEX 100a Directive requires in Annex II, 1.6: Integration of safety requirements relating to the system". This includes, for example, that the interface must be safe, when ATEX products are intended for use in combination with other equipment and protective systems. Furthermore, equipment and protective systems must be designed and constructed in such a way as to prevent hazards arising from connections.

In addition, the ATEX 100a Directive requires that any misuse which can reasonably be anticipated must be taken into consideration in the evaluation of the hazard.

The philosophy underlying the principles of explosion prevention and protection are described in chapter 4 of this standard while chapter 5 provides a detailed description of the steps involved in risk assessment.

A brief review of the different methods and techniques which can be used and their range of applicability is given in chapter 6. Annex VI gives information and examples on how the risk assessment methodology can be applied in practice.

	Explosive atmospheres – Explosion prevention and protection Part 1: Basic concepts and methodology
prEN 13463-1	Non-electrical equipment for potentially explosive atmospheres Part 1: Basic methodology and requirements
EN 50014	Electrical apparatus for potentially explosive atmospheres – General requirements
IEC 60812	Analysis techniques for system reliability-procedure for failure mode and effects analysis (FMEA)
IEC 61025	Fault Tree Analysis (FTA)
IEC 61882, Ed. 1	Hazard and operability (HAZOP) studies – Guide word approach

Note: This list is not exhaustive other normative references may also apply

3. Definitions

For the purpose of this standard the following terms shall have the meanings:

Risk: Function of Severity (elements: possible harm for the considered explosion hazard) and Probability of occurrence of that harm (elements: frequency and duration of exposure, probability of occurrence of hazardous event, possibility to avoid or limit the harm).

Risk Assessment: A series of logical steps to enable, in a systematic way, the examination of the hazards associated with unit operations and equipment.

Hazard Identification: A systematic procedure for finding all of the hazards which are associated with the unit operations and equipment.
The process of determining what, why and how things can happen.

Risk Estimation: Determination of the frequency at which the identified hazards could be realized and give rise to specified levels of severity.

Risk Evaluation: Comparison of the risk estimated with criteria in order to decide whether the risk is acceptable or whether the unit operations and/or equipment design must be modified in order to reduce the risk.

Risk Reduction Option Analysis: The final step of risk assessment is the process of identifying, selecting and modifying design changes which might reduce the overall risk from unit operations and equipment.

Residual Risk: The remaining level of risk after all actions have been taken to reduce the probability and consequence of risk.

Risk Factor: The individual elements which comprise and influence the likelihood of a certain event occurring, e. g.

- the frequency and duration of the exposure of persons to the hazard;
- the probability of occurrence of a hazardous event;
- the technical and human possibilities to avoid or limit the harm (e. g. awareness of risks, reduced speed, emergency stop equipment, enabling device).

Risk Management: The systematic application of management policies, procedures and practices to the tasks of identifying, analysing, monitoring and controlling risk.

Fatal Accident Rate: Number of fatalities per 100 million hours of exposure, interpreted for workers as the number of deaths per 1000 people involved in an activity during the working lifetime of 10^5 hours.

4. Aspects on how to influence explosion risks

In principle, an explosion can take place if a number of conditions are simultaneously satisfied. These conditions are dealt with by the ATEX 100a Directive which defines“explosive atmospheres” as:

Mixture with air, under atmospheric conditions, of flammable substances in the form of gases, vapours, mists or dusts in which, after ignition has occured, combustion spreads to the entire unburned mixture.

Consequently, any assessment of explosion risks shall be based on

- **the likelihood that explosive atmospheres will occur and their persistence,**
- **the likelihood that ignition sources will be present and become effective,**
- **the scale of the anticipated effects.**

In this respect the following items are of particular importance:

- ♦ design and construction of ATEX products
- ♦ substances used
- ♦ processes
- ♦ possible interactions

To help visualise what is going on, a generic fault tree of accident causation is provided (figure one).
It should encourage the analyst at a very early stage to speculate how a particular situation could arise or what may ensue from such a situation and hence identify causes or outcomes of undesired events.

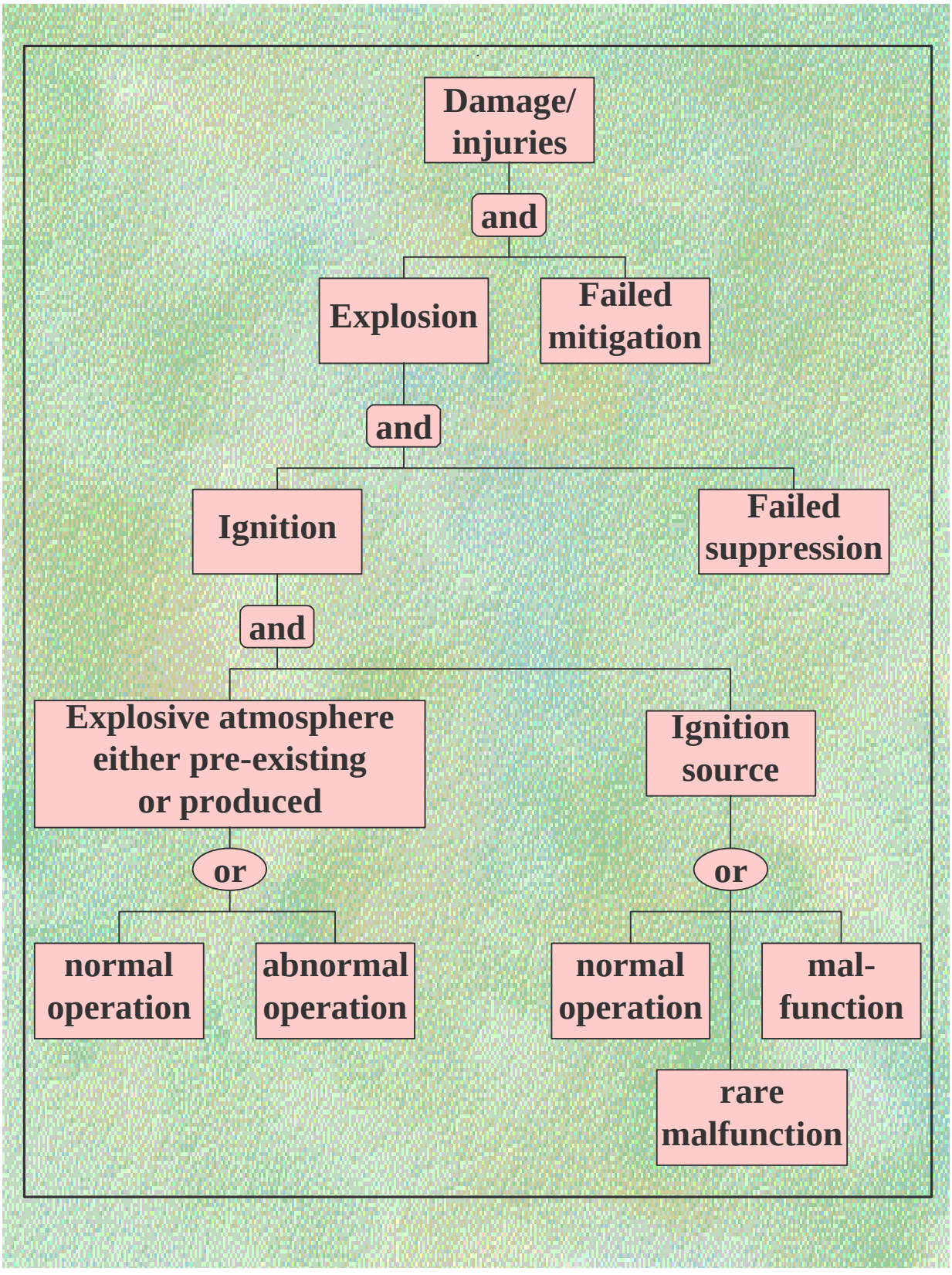


Figure one: **Generic Fault Tree of Accident Causation**

Before starting the analysis the following aspects need to be considered when establishing elements of risk:

- Persons exposed
- Type, frequency and duration of exposure
- Human factors
- Reliability of safety functions
- Possibility to defeat or circumvent safety measures

Persons exposed

Risk estimation shall take into account all persons exposed to the hazards. This includes operators and other persons for whom it is reasonably foreseeable that they could be affected by the explosion event.

Type, frequency and duration of exposure

The estimation of the exposure to the hazard under consideration requires analysis of and shall account for all modes of operation and methods of working. In particular this affects the need for cleaning, fault finding and maintenance. The risk estimation shall account for situations when it is necessary to suspend safety functions (e. g. during maintenance).

Human factors

Human factors can affect risk and shall be taken into account in the risk estimation. This may include some of the following aspects:

- interaction of persons with the ATEX products;
- interaction between persons;
- psychological aspects; (e. g. resistance to incentives not to deviate from prescribed and necessary safe working practices.)
- design of the products in relation to ergonomic principles;
- capacity of persons to be aware of risks in a given situation depending on their training, experience and ability.

Training, experience and ability can affect the risk, however none of these factors are to be used as a substitute for hazard elimination, risk reduction by design or safeguarding where these measures can be implemented.

Reliability of safety functions

Risk estimation shall take account of the reliability of components and systems. Those identified as part of safety critical functions need special attention. Estimation shall:

- identify the circumstances which can result in harm (e. g. component failure, power failure, electrical disturbance);

- when appropriate use quantitative methods to compare alternative safety measures;
- provide information to allow the selection of appropriate safety functions, components and devices.

When more than one safety related device contribute towards a safety function, the selection of these devices shall be consistent in terms of reliability and performance.

When safety measures include work organisation, correct behaviour, attention, application of personal protective equipment, skill or training, the relatively low reliability of such measures as compared to proven technical measures shall be taken into account in the risk estimation, and shall be considered when re-estimating the risk during risk reduction option analysis.

Possibility to defeat or circumvent safety measures

Risk estimation shall take account for the possibility to defeat or circumvent safety measures, whether, for example:

- the safety measure slows down production, or interferes with any other activities or a user's preferred way of working;
- the safety measure is difficult to use;
- persons other than the operator are involved (e. g. cleaning, maintenance)

Risk estimation shall consider whether the safety measures can be maintained in the condition necessary to provide the required level of protection.

5. Risk Assessment Procedure

A Risk assessment methodology should consider all risk factors including unexpected parameters. The methodology needs to answer the following basic questions:

- **What do we know? What is the risk?**
- **Do we have an incident waiting to happen?**
- **What action can we take?**
- **What can go wrong? What are the potential consequences?**
- **How likely is it to happen?**
- **What is the chain of events which could lead to harm?**
- **Can we tolerate the potential consequences at the estimated likelihood?**
- **What are the benefits and costs of alternative technologies?**

For the purpose of this standard risk assessment comprises in principle five steps including the determination of intended use (figure two):

- **Determination of intended use (Functional / State-Analysis)**
- **Identification of hazards, hazardous situations and hazardous events**
- **Risk estimation of consequences / likelihood**
- **Risk evaluation**
- **Risk reduction option analysis**

Risk Assessment should follow the step-approach in that order of preference given.

The first three steps of risk assessment (determination, identification, estimation) are often referred to collectively as risk analysis.

Risk assessment is an iterative process. If, after risk has been evaluated, the decision is made that the risk needs to be reduced it is necessary to re-estimate the risk. A decision can then be made as to whether the measures taken have reduced the risk to an acceptable level. It is also essential to check that the measures used to reduce risk have not themselves introduced any new hazards. Therefore a feedback loop from Risk Reduction Option Analysis to Hazard Identification has to be made.

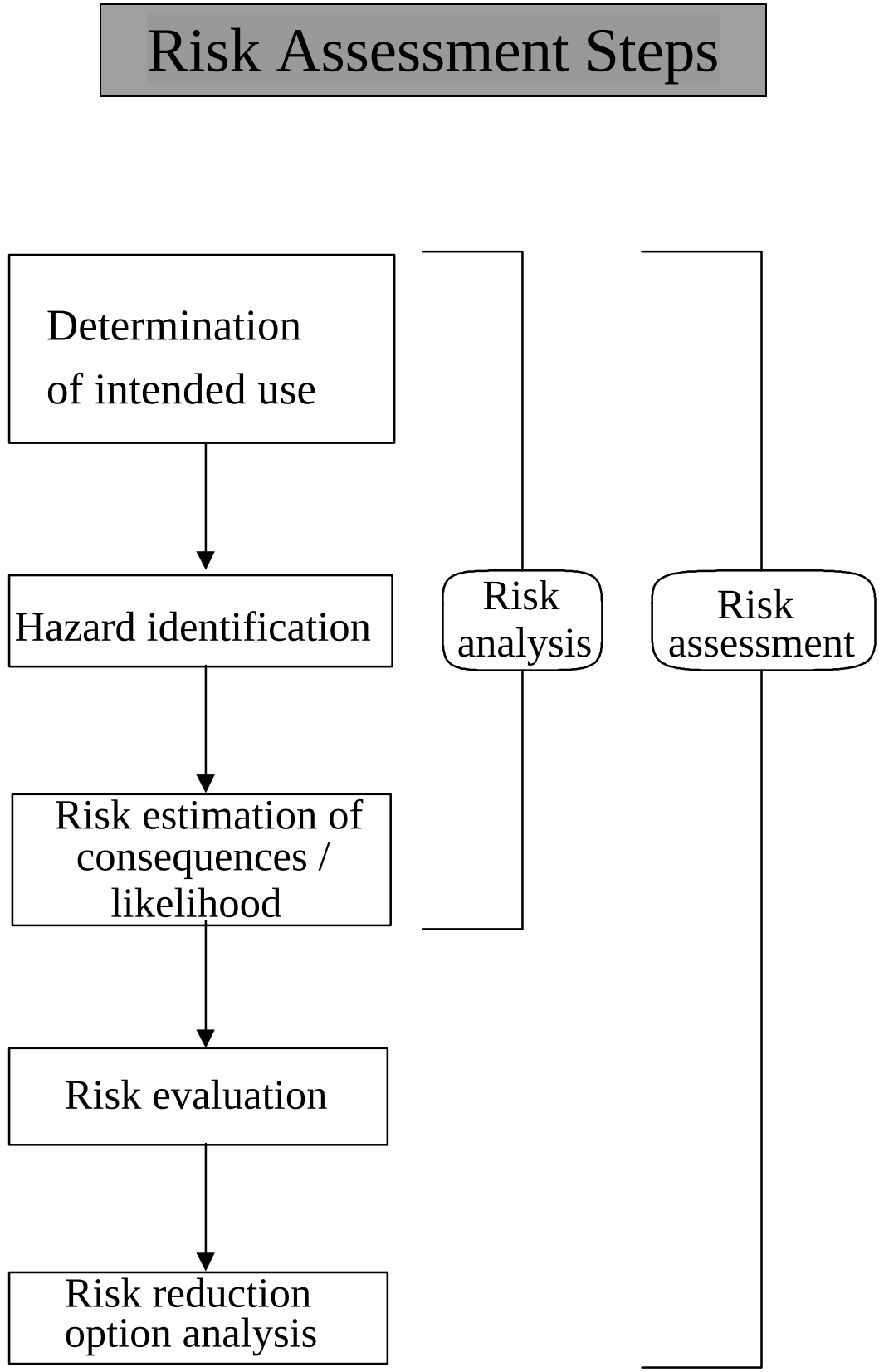


Figure two: – Fundamental Steps of Risk Assessment

5.1 Determination of intended use

The step-approach needs to be carried out with an understanding of the functioning of the equipment and/or unit operations and the way in which an incident or an accident develops.

5.1.1 Description of the system
The first stage in assessing the risk of a system or piece of equipment is to determine its intended use. As the risk of an explosion comes from both the equipment itself and the products being handled, both the characteristics of the equipment and those of the product need to be documented.

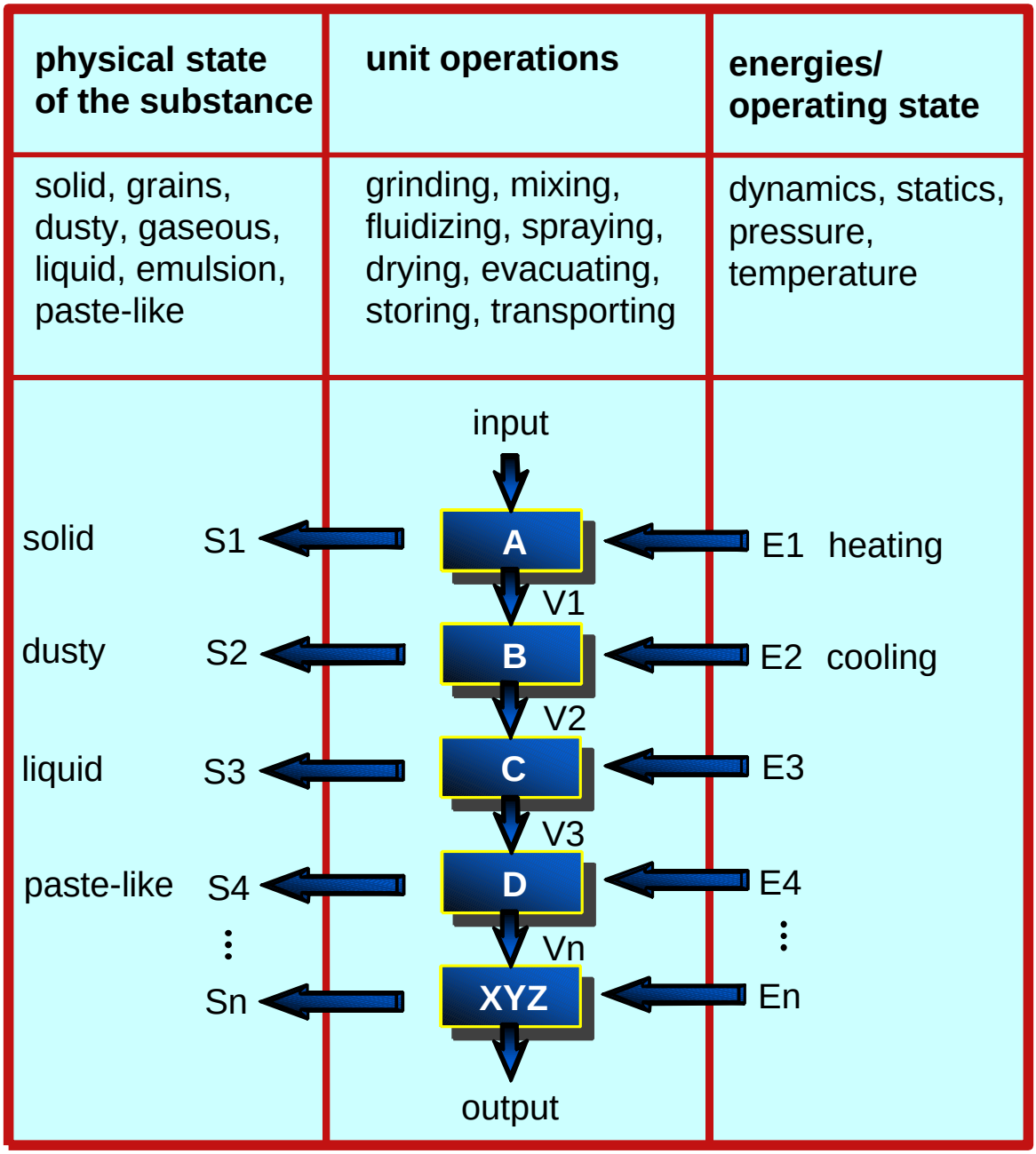
5.1.1.1 Equipment characteristics
The characteristics of the equipment relevant to achieving its desired function should be described – this should include aspects relevant to it acting as an ignition source including for example materials of construction and the formation of explosive atmospheres (see Annex I).

5.1.1.2 Product characteristics
The flammability and explosivity characteristics of the materials being handled should be listed (see Annex II).

5.1.2 Functional / State Analysis
For complex pieces of equipment it is an advantage to establish an Equipment / Process Flow_Diagram in the light of a Functional / State-Analysis with the inclusion of energy levels (i. e. temperatures, pressures etc.) for each phase of the equipment's operation. Such a diagram helps the assessor to consider and/or to define the status of the materials being handled and the availability of equipment itself being available (figure three).

In addition, such a flow diagram not only helps to define the intended use but can also be used as a key part of the iterative risk assessment process. It refers the ATEX product characteristics to energies involved and/or the operating state as well as the physical state of the substance. Following this approach there are linkages depending on function and / or depending on effects between the input and the output within such a risk assessment process. Thus the analyst is able to determine what, why and how things can happen, especially when dealing with complete machines or more complex products.

The diagram is based on the fact, that any ATEX product has limits to its functionality and to its use, especially the intended use, its lifetime and space it occupies (configuration).



S: physical state of the substance A...XYZ: unit operations
E: energy/operating state
V: linkage (depending on function/depending on effect)

Figure three: Functional Analysis of Unit Operations

These limits form part of **constituent elements or parameters** which need to be taken into account in any phase of the Functional/State-Analysis. These constituent elements can be used to evaluate for example,

- phases of equipment life
- limits in terms of use, time, space
- accurate definition of the function
- selection of material used to construct
- combustion properties

When defining these limits, the following items have an important impact, for example, in terms of use, time and space:

Intended use:
product, capacity, load rate of utilisation, foreseeable misuse

Life time:
abrasion, corrosion, parameters of process like ageing by temperature, pressure, vibration, characteristics of substances, maintenance, change of use, change of environment;

Configuration:
range of movement, space requirement, location, volume, confinement, weight, kind of interconnections

5.2 Identification of hazards, hazardous situations and hazardous events

There is rarely, if ever, a single cause of a hazardous situation or hazardous event. Although the immediate cause may be a simple hardware failure or operator error, other events will have also occured which assist the development of the accident. Such events include undetected failure of protective systems, ergonomic problems or an organisation in which safety is not given priority.

In many ways, hazard identification is the most important part of any risk assessment. However in order to successfully carry out this step the previous step must have accurately defined the equipment in sufficient detail. Once a hazard has been identified, the design can be changed to minimise it, whether or not the degree of risk has been estimated; unless the hazard is recognized it cannot be addressed in the design. A full understanding of its intended use and foreseeable misuse is also of prime importance during this step.

A project or a process has an acceptably safe design when one judges that adequate preventive or protective measures have been taken. The term "adequate measures", refers to generally accepted safety, engineering, scientific, production, operational, and maintenance procedures in relation to the risks involved. The risks considered may be of harm to people, or cause damage to the plant or environment.

The system should be examined to determine which ignition sources are present. Table 2a contains a list of possible ignition sources provided in EN 1127. Where such an ignition source can occur in the system this should be noted in the 'Relevant' column of the table. For example if there are no Ultrasonic discharges possible in the system then a 'No' would be entered in the 'Relevant' column. The relevant individual ignition sources should then be considered with respect to the potentially explosive atmospheres present and where appropriate a decision made as to whether they are significant to the complete system and must be considered in the risk assessment. For example if electrostatic brush discharges are possible in the system but there are no explosible gas or vapour atmospheres present and the ignition energy of the explosible dust atmosphere being handled is 100 mJ then a 'Yes' would be entered in the 'Relevant' column and 'No – MIE dust cloud 100 mJ' would be entered in the 'Significant' column.

The main aim of hazard identification is that all possible hazards are found and none are missed. This may be facilitated by the use of more than one method and/or technique. The main output from the hazard identification stage is a numbered listing of hazardous events recorded as in table 2b, which could result from the unit operations and equipment involved as an input to the risk estimation stage.

Ignition sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface		
flames and hot gases (including hot particles)		
Mechanically generated sparks		
Electrical apparatus		
Stray electric currents, cathodic corrosion protection		
Static electricity:		
Corona discharges		
Brush discharges		
Propagating brush discharges		
Cone discharges		
Spark discharges		
Lightning		
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz		
Electromagnetic waves from 3 x 10^{11} Hz to e x 10^{15} Hz		
Ionizing radiation		
Ultrasonics		
Adiabatic compression and shock waves		
Exothermic reactions, including self-ignition of dusts		

Table 2a: List of Ignition Sources

	Explosive Atmosphere			Ignition Source			
Ref.	Type	Frequency of occurence or release	Location	Type	Cause	Likelihood	Effective-ness of ignition sources
1	Mixture with air of flammable hexane vapour	for a short period only at the end of the filling	outside filling manhole	stirrer motor surface	overload of the motor	During malfunction	High as surface temperature > ignition temperature
2	Cloud of explosible sugar dust	Present frequently in normal operation	inside elevator housing	Friction sparks in bucket elevator	Baskets rubbing on housing	Occasionally in normal operation	Low due to slow bucket speed
etc.							

Table 2b: Record of Hazard Identification

The hazard identification should analyse the system to identify all possible occurrences of a potentially explosive atmospheres. the type of explosive atmosphere which could occur should be recorded in the ‘Type’ column of the table. The operation which causes its occurrence and an indication of the frequency or when it will occur is recorded in the ‘Frequency of occurrence or release’ column while the location where it occurs in the system is recorded in the ‘Location’ column. Similarly any significant ignition source which could cause the ignition of the explosive atmosphere should be entered in the corresponding ‘Type’ column together with the cause and likelihood of occurrence. Finally the effectiveness of the ignition source in causing ignition of the explosive atmosphere (ranked as high, medium, low) together with the reason is entered in the final column.
The likelihood of occurrence of the ignition source can be used as a means to determine the equipment category for the final classification of the equipment in terms of the ATEX 100a Directive.

Where the risk assessment of a protective system is to be carried out the risk assessment has to include the identification and possible consequences of faults in the operation of the protective system. The error types from HHEA techniques described in Annex V could facilitate this exercise. This should be carried out in addition to the hazard identification procedure outlined above to determine the possibility of the protective system causing ignition of the explosive atmosphere. The results of this assessment should be recorded in a table as follows:

Ref.	Deviation from intended operation	Possible reason	Consequence
1	No opening at defined pressure	Wrong spring mechanism	Overpressure to high
2	No opening at defined pressure	Jammed spring mechanism	Overpressureto high
etc.			

There might be subsidiary outputs from the hazard identification, for example, a list of possible protective measures against the hazards which have been identified. These lists can be used also in the risk evaluation and risk reduction steps of the risk assessment.
Identification shall always be carried out for each hazard, hazardous situation and hazardous event.

In the assessment of the combustion properties and the likelihood of occurrence of a hazardous explosive atmosphere logic diagrams are useful tools. They ask questions relating to the materials and substances processed, used or released by equipment.
Safety data always plays an important role in this context, for example, flammability limits or relevant data characterizing the behaviour of the explosive atmosphere (figures four and five).

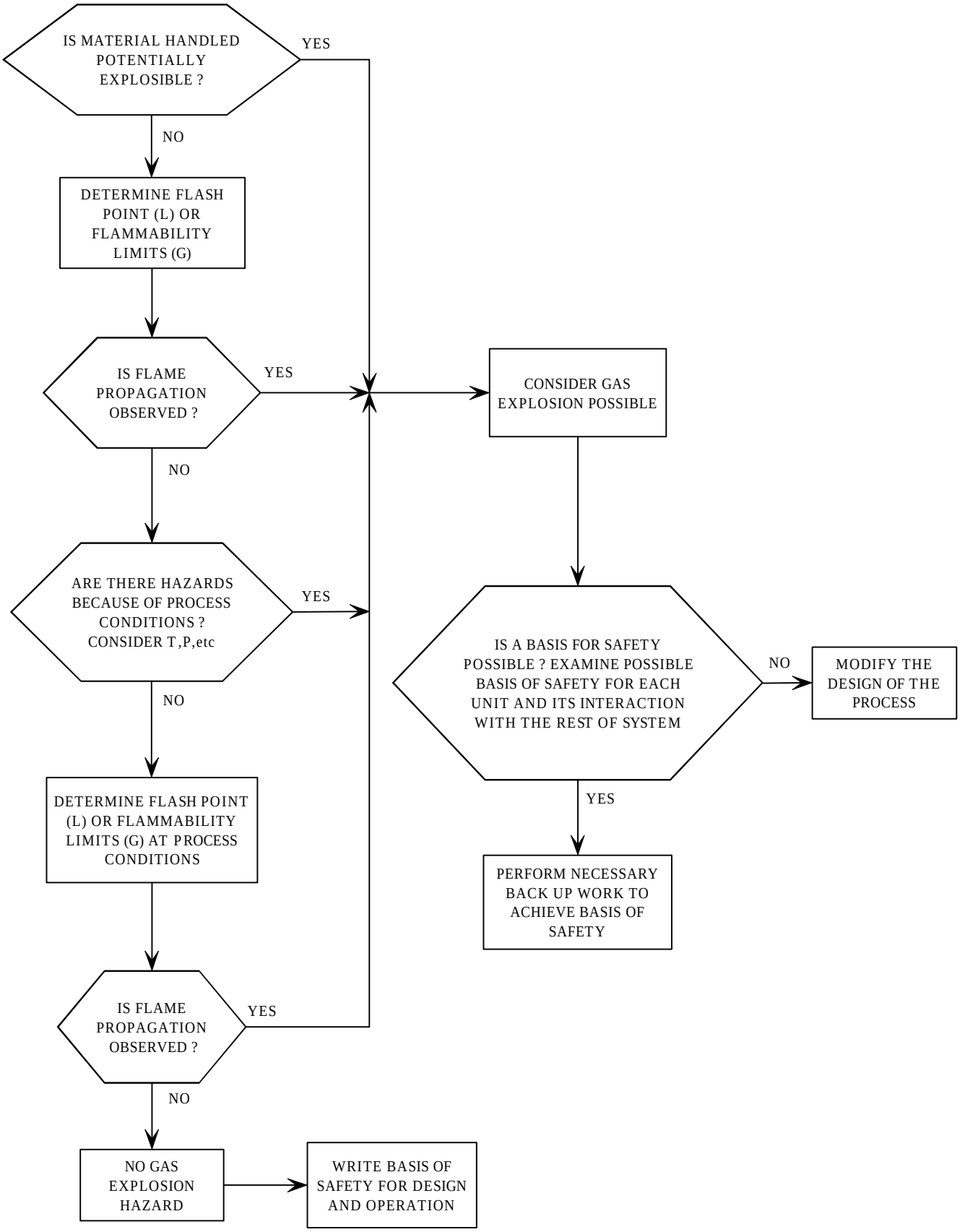


Figure four: Logic diagram for testing and design to identify gas explosion hazards

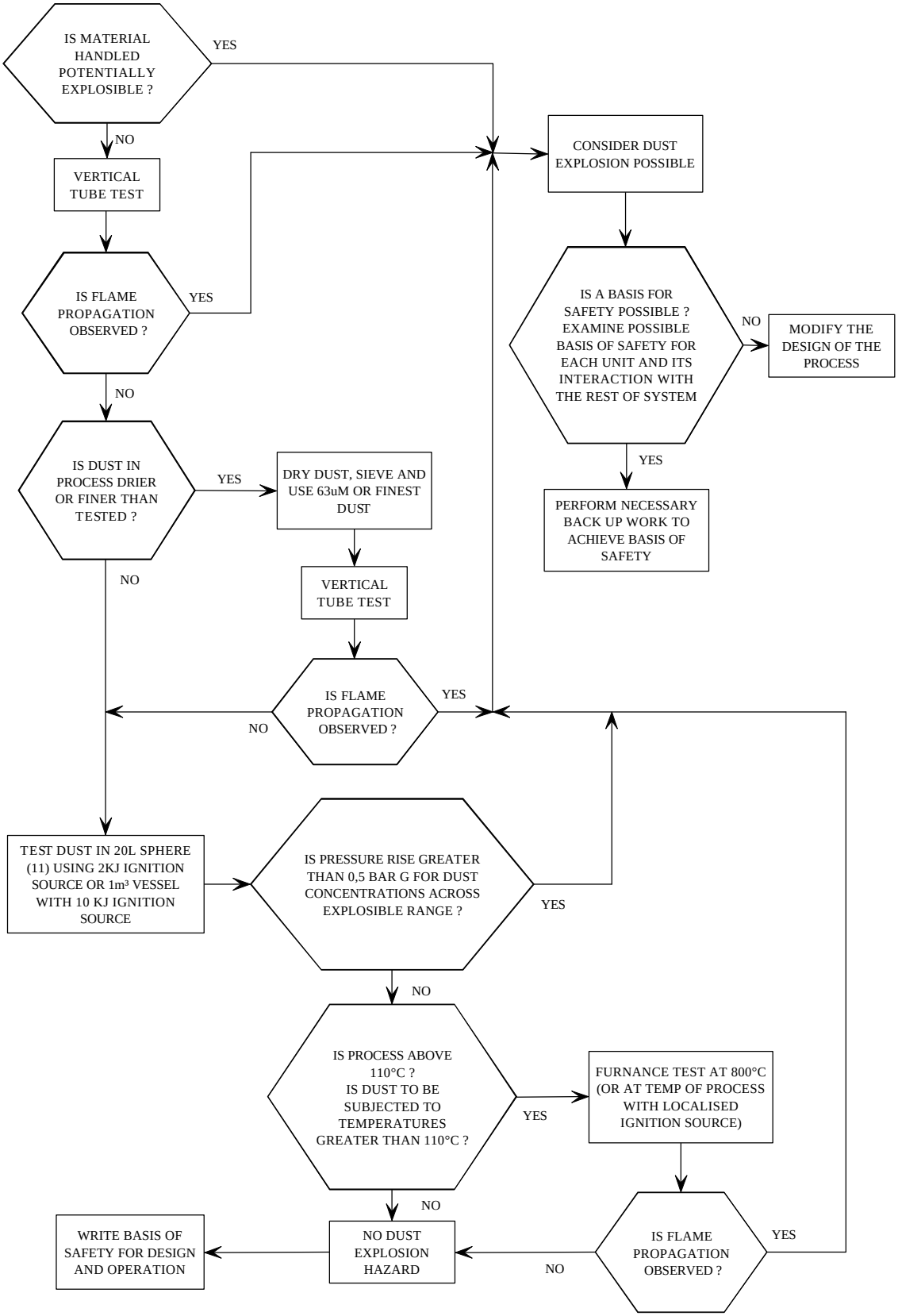


Figure five: Logic Diagram for testing and design to identify dust explosion hazards

5.3 Risk Estimation

In principle, Risk Estimation shall be carried out for each explosion hazard or every hazardous event in turn by determining the elements of risk (see definition in chapter 3) after Hazard Identification. The risk associated with a particular situation or technical process is derived from a combination of these elements.

Risk in terms of explosion safety is fundamentally made up of two elements: the severity of the possible harm and the probability of occurrence of that harm. The severity or consequence of an explosion can often be adequately characterized however the probability of its occurrence is usually more difficult to quantify.

Risk is usually expressed in one of 3 ways:

1. Qualitatively for example as high, medium, low, tolerable, intolerable, acceptable;
2. Quantitatively by calculating the frequency or probability of some determined event occurring;
3. Semi-quantitatively where elements of risk such as consequence, exposure and likelihood are given a numerical score which are then combined in some way to give a pseudo-quantitative value of risk which allows risks to be ranked one against another.

In many situations it is not possible to exactly determine all the factors that effect risk, in particular those which contribute to the likelihood of a specified event occuring. Thus risk is often expressed in a qualitative rather than a quantitative way.

Severity can be expressed as defined levels, one or more of which can result from each hazardous event. Thus in terms of injuries or damage to health or system damage severity can be expressed as follows (figure six):

- catastrophic
- major
- minor
- negligible

In order to estimate the frequency of each severity level a screening technique can first be applied to determine the probability of each hazardous event in turn.

The frequency of occurrence can be qualitatively expressed as:

- frequent
- probable
- occasional
- remote
- improbable

The definitions of the different severity levels and frequencies are given in figure six.
The linkage between severity levels on the one side and the frequency of their occurrence on the other leads to the matrix shown in figure six. The corresponding points in this matrix are allocated to the risk levels A, B, C, and D.

The risk levels represent a ranking of the risk which enables an evaluation of what further actions are needed if any.

Thus:

- risk level A:
- risk level B:
- risk level C:
- risk level D:

SEVERITY Description	Mishap Definition
CATASTROPHIC	Death or system loss.
MAJOR	Severe injury, severe occupational illness, or major system damage.
MINOR	Minor injury, minor occupational illness, or minor system damage.
NEGLIGIBLE	Less than minor injury, occupational illness, or system damage.

FREQUENCY Description	Specific Individual Item	Inventory
FREQUENT	Likely to occur frequently	Continuously experienced
PROBABLE	Will occur several times in life of an item	Will occur frequently
OCCASIONAL	Likely to occur sometime in life of an item	Will occur several times
REMOTE	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	So unlikely, it can be assumed occurence may not be experienced	Unlikely to occur, but possible

RISK LEVELS

Frequency of Occurrence	Severity			
	Catastrophic	**Major**	**Minor**	**Negligible**
Frequent	A	A	A	C
Probable	A	A	B	C
Occasional	A	B	B	D
Remote	A	B	C	D
Improbable	B	C	C	D

Figure six: Frequency-Severity Matrix relating to risk levels

5.4 Risk Evaluation

Following the estimation of the risk, Risk Evaluation shall be carried out to determine if Risk Reduction is required or whether safety has been achieved.

It is evident that if the risk estimation results in a risk level of A, the risk is so high as to be intolerable and additional risk reduction measures are required. Similarly a risk level of D can be considered to be acceptable and no further risk reduction is required.

Thus the risk can be described either as

Intolerable: If the risk falls into this category then appropriate safety measures must be taken to reduce the risk.

or as

Acceptable: If the risk falls into this category then no Risk Reduction is required and the Risk Assessment is complete.

Risk levels B and C are intermediate levels and will normally require some form of risk reduction measures to make the risk acceptable. However, the degree of these measures will be smaller and in the case of a risk level C, organisational risk reduction measues will often be sufficient.

Alternatively the process of Risk Evaluation can be carried out by comparing the explosion risks associated with equipment and unit operations with those of similar equipment. In this case it is essential that the following are comparable:

- hazards and elements of risk
- type of equipment, its technology and operational limits
- intended use and the conditions of use

The application of the comparison method does not preclude the need for conducting a Risk Assessment for the specific conditions of use.

5.5 Risk Reduction Option Analysis

Risk can seldom be reduced to zero in practice except by eliminating the activities. However, risks can often be reduced further in practice.

Options which address the hazardous events that make the greatest contributions to the total risk have the greatest potential to reduce risk. Effectiveness in reducing risk always starts with changes to the design concept, i. e. inherently safe design.

Once the risk has been estimated and evaluated the step of risk reduction option analysis shall lead to the final decision whether or not the solution found reduces the risk to an acceptable level. This decision includes both the technological and economical point of view based on an appropriate classification of equipment category. If the decision is that the risk has not been reduced to an acceptable level then the iterative process has to be done again after amending the safety concept.

There are many factors to take into account when analysing the options for risk reduction. The most important is whether the amount of risk reduction is sufficient to reduce the risk to tolerable levels. The manufacturer or user may need to reconsider how much the safety of a design improves, if a particular safety feature is included. It is important during this assessment to properly take into account the effectiveness of the various options. This is in terms of the hierarchy given in the Essential Health and Safety Requirement 1.1.2, principles of safety integration, of the Machinery Directive. In general the removal of a hazard is more effective than safeguarding it, which in turn is more effective than use of personal protective equipment or safe systems of work. The reliability of any safeguard also needs to be taken into account as discussed earlier in section 4, in particular any incentives for them to be defeated or circumvented. The expected lifetime of the safeguard must also match that of the equipment and/or provision may need to be made for the monitoring and replacement of components which will wear out.

It is obviously also important to compare the cost effectiveness of the various options. In doing so the following issues, which may also have implications in terms of providing incentives to defeat a safeguard, need to be considered. Changes to:

- overall capital cost,
- productivity,
- energy efficiency,
- maintenance costs
- other operational costs.

Note that some options may actually have beneficial effects on some of these. A more reliable piece of equipment for example often has lower maintenance and operational costs as well as being more productive.

Other issues which may be relevant when comparing one option with another are:

- Legislative or code of practice requirements, if a particular option is required by the law then a very strong case would be needed to select an alternative. Codes of practice and industry guidance are also often invaluable sources of information about the most effective options for reducing specific risks.
- Expected lifetime of the hazard, in the situation where a hazard may only exist for a short period, a safeguard designed to exist continuously may be inappropriate.

In many cases, it is unlikely that any one risk reduction option will be a complete solution for a particular problem. Often Risk Assessment of Unit Operations and Equipment will benefit substantially by a combination of options. In this context the step of Risk Reduction Option Analysis becomes subject to Risk Management (see definition in chapter 3).

It’s necessary to deal with residual risks after all measures have been taken to reduce the probability and consequence of a specific hazardous event. The residual risks are those against which risk reduction by design and safeguarding techniques are not – or not totally – effective.

The users must be informed about residual risks. Instructions and warnings shall, for example, prescribe the operating modes and procedures to overcome the relevant hazards.

It’s an advantage to produce a written plan in order to document how the chosen options shall be implemented.

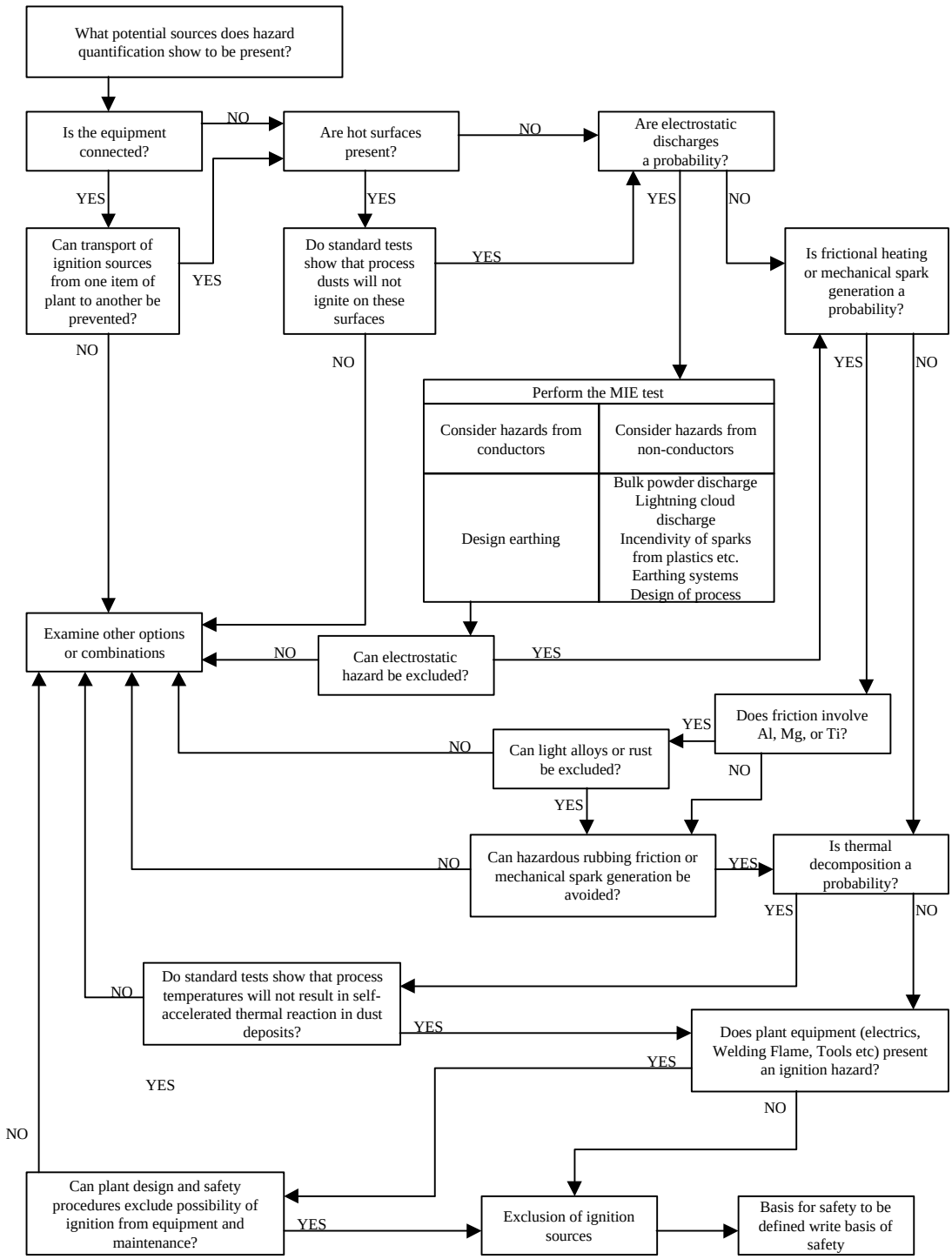


Figure seven: Logic diagram for minimizing of ignition sources

6. Methods and/or techniques that could favourably be applied

There is no golden rule as to which method and / or technique ought to be adopted. There are many possible methods and/or techniques for risk assessment, especially for hazard identification. A good hazard identification technique has the following attributes:

- it is systematic, i. e. it guides the users so that all parts of the system, all phases of use and all possible hazards are considered:
- it employs brainstorming;

In principle, the identification techniques fit into three family categories:

- comparative methodology, e. g. checklists, codes
- fundamental approach, e. g. HAZOP, FMEA
- failure logic diagrams, e. g. Fault Tree Analysis, Event Tree Analysis

The comparative methodology relies on experience, whereas the fundamental methodology aims to discover all possible conditions and deviations in order to identify those which may be hazardous. The failure logic diagram approach identifies and structures combinations or sequences of occurrences with accident potential.

In general, methods and / or techniques can be classified as:

- Qualitative: Both the input to the risk estimation in terms of categories for each unit operation and equipment and the output in terms of risk all consist of qualitative phrases such as “hazardous event is likely to occur”, “severe injuries”, “unacceptable risk”, “high risk”, “low risk” and so on.

- Quantitative: The incident scenario is modelled in detail, for example using fault tree analysis and event tree analysis, so that estimates can be made, using any available data or experience of the frequency or probability of all possible events which affect the overall frequency of a defined hazardous event or consequence. The results can be directly compared with accident statistics in order to either validate the method, or to make decisions as to whether the risk is acceptable.

- Semi-Quantitative: Input categories are combined numerically or diagrammatically to obtain a numerical (pseudo-quantitative) value of risk. These values are often then banded into categories which are defined qualitatively.

Figure eight reflects the typical considerations in selecting the type of analysis and depth of study.

In addition table 3 shows the objectives and attributes of each technique as an aid to selecting the most appropriate technique or techniques.

It should become clear that the limitations of one technique can be offset by the advantages of others.
By using more than one technique the possibility of overlooking any relevant hazards is minimised. However, the additional time employed in using more than one technique needs to be balanced against the increased confidence in the results.

Most techniques which contain criteria to enable risk to be evaluated cover both the risk estimation and evaluation step. Some go further and give recommendations for risk reduction.

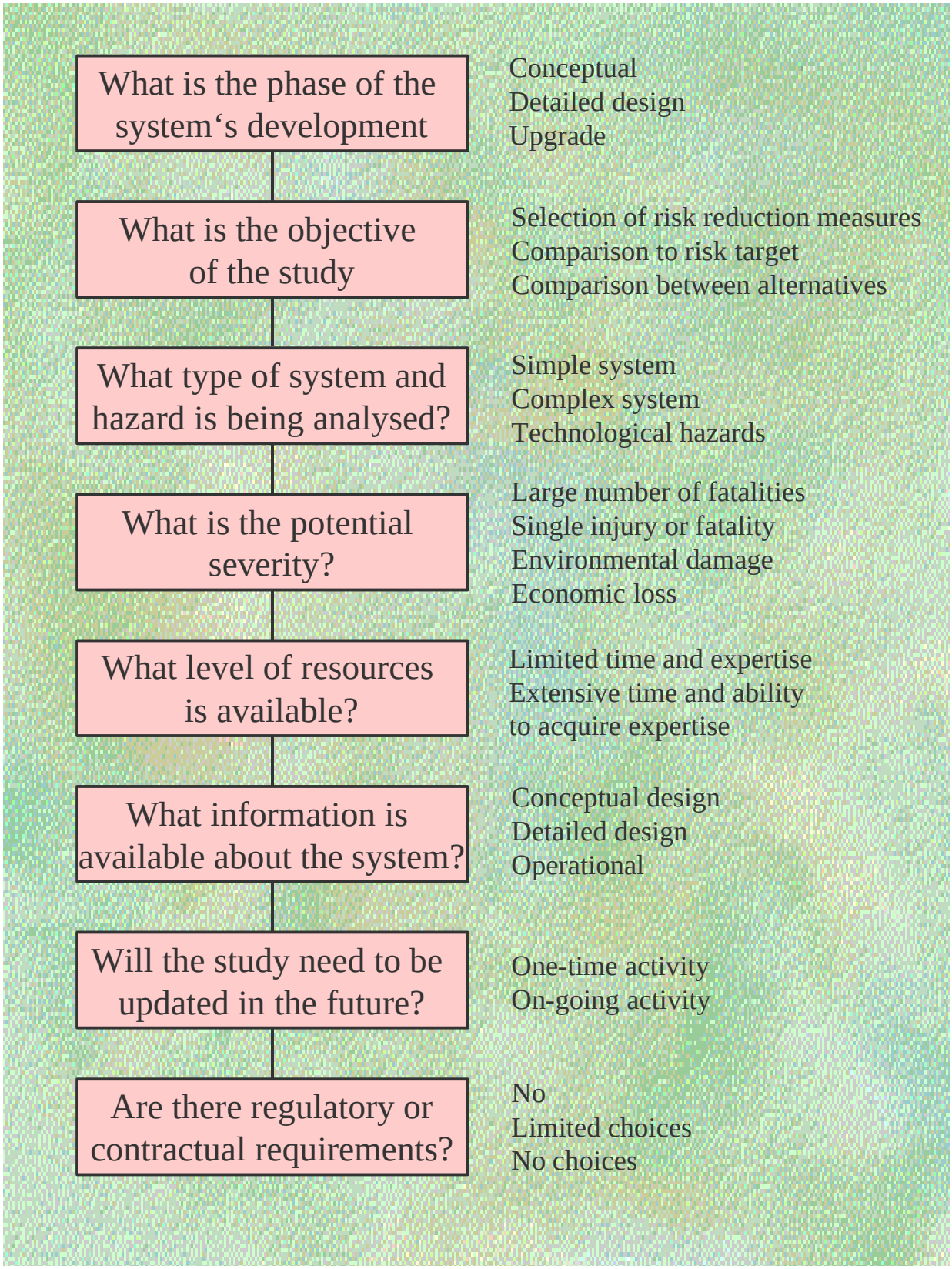


Figure eight: Typical Consideration in Selecting Type of Analysis and Depth of Study

Technique	Objective	Attributes
Checklists	to measure compliance with standard procedures usually prepared from prior experience; generally identify common hazards;	can be applied to all stages of a project and to plant operations; can be as detailed as necessary to satisfy the specific situation; can highlight a lack of basic information or a situation that requires a more detailed evaluation.
Machinery/Equipment concept hazard analysis **Preliminary hazard analysis**	to identify hazards that are inherent due to the design concept of machinery / equipment to be used early in the design stage to identify hazards and assess their criticality	an expert team applies a series of key words to each of the functional parts of the machine / equipment in order to facilitate brainstorming of possible hazards the effectiveness of this technique is dependent on the skill and expertise of the persons involved and the preparation work (drawing, record sheets etc.)
Hazard Exposure Index / Category Rating	a means of rating risks by the categories in which they fall in order to create prioritised groups of risk to rate the relative acute health hazard potential to people in neighbouring plants or communities from possible chemical release incidents	a simple technique which is consequence based and independent of the frequency of events results in an index that is suited for use as a screening tool for more sophisticated process hazard analyses

Table 3: Objectives and Attributes of Techniques

Technique	Objective	Attributes
Hazardous human error analysis **Human reliability**	to go systematically through the operating procedures and to consider any human error which could lead to realisation of a hazard deals with the impact of people on system performance and evaluates the influence	particularly good at identifying hazards which could result from human error or from the presence of the operator key tasks relating to the use of equipment need to be listed
Distribution Risk Evaluation	identification of hazards and risks associated with the distribution of products, by-products, purchased materials, solvents, catalysts, and modifiers	in-depth qualitative risk assessment. assessment is typically completed by a multi-functional team the Risk Review Team looks at each movement and assesses potential exposure
Fault Tree Analysis	focuses on one particular incident event and provides a technique for determining causes of that event can be used as a qualitative tool to break down an incident into basic equipment failures and human errors but can also be quantified if the base events are broken down into sufficient detail and data is available and used as part of a Quantified Risk Assessment (QRA)	graphic model that displays the various combinations of equipment and human errors that can result in the event the solution is a list of the sets of equipment and human errors that are sufficient to result in the incident event of interest allows to focus preventive measures on basic causes to reduce the probability of an incident

Table 3: Objectives and Attributes of Techniques (continued)

Technique	Objective	Attributes
Concept safety and Standards review	the review identifies the essential health and safety requirements which are relevant to unit operations and equipment identifies any relevant standard (national, inter-national, European) to encourage inherently safe design, gain an appreciation of the likely hazards associated with the design	can be carried out by an individual rather than a team can be used to ensure that the design is consistent with the published "state of the art" for that type of equipment at a very early stage in the design process
Hazard and Operability Study (HAZOP)	to identify the hazards in a design as well as anticipate any operational difficulties will only identify causes of loss of containment not causes of ignition sources.	formal systematic critical examination of the pro-cess, engineering, and operating intentions of new or existing facilities a multidisciplinary team systematically searches for deviations from design and operating intentions using a set of "guide words" this technique can be applied to any equipment or activity whose design intention can be defined

Table 3: Objectives and Attributes of Techniques (continued)

Technique	Objective	Attributes
"What – If" Analysis	to consider the results of unexpected events that could produce adverse consequences to understand of what is intended and the ability to mentally combine or synthesize possible deviations from the design intention which could cause an undesirable effect Particularly good at identifying equipment malfunctions which could lead to ignitions sources.	involves the examination of possible deviations from the design, construction modifiation, or operating intent the review is divided into specific areas such as personal safety, process safety, etc. a multidisciplinary team examines the process using "What-If"questions at each handling or processing step to determine the effect of equipment failure and operating errors
Failure Mode and Effect Analysis (FMEA)	Can be used to analyse the ways in which equipment, particularly mechanical, electrical and electronic can fail. It is particularly useful for looking at control systems.	standard reliability engineering technique, usually used by a team can be used for any system which can be broken down into components parts can be very time-consuming for complex systems
Common Mode Failure Analysis	to assess whether the coincidental failure of a number of different parts or components within a system is possible	provides information on the likely overall effect of coincidental failure within a system

Table 3: Objectives and Attributes of Techniques (continued)

Technique	Objective	Attributes
Consequence Analysis	to estimate the potential impact of an event on people, property or the environment this event might be, for example, a flammable material release	variables, such as release scenario, physical properties of the material, and atmospheric conditions, are used with mathematical models to calculate the potential impact, of the material as a function of distance from the release point
Event Tree Analysis	to translate different initiating events into possible outcomes	a hazard identification and frequency analysis technique which employs inductive reasoning
Reliability Block Diagram	to evaluate the overall system reliability	a frequency analysis technique that creates a model of the system and its redundancies
Delphi Technique	to combine expert opinions	a means that may support frequency analysis, consequence modelling and / or risk estimation
Monte-Carlo simulation and other simulation technique	to evaluate variations in input conditions and assumptions	a frequency analysis technique which uses a model of the system for evaluating variations
Review of Historical Data	to identify potential problem areas	a hazard identification technique that can provide an input into frequency analysis based on accident and reliability data etc.

Table 3: Objectives and Attributes of Techniques (continued)

Addressing the main fields to be analysed and to link them with the fundamental steps of risk assessment a simplified Risk Assessment Process could be helpful (figure five). Starting from "Function/Task/Intended Use" the main fields to be analysed are considered as:

- Equipment characteristics
- Operational Aspects and Influences
- Human Factors and organisational Aspects

Then, the main fields to be analysed are each of them composed of the constituent elements dealt with in the corresponding annexes I to IV.

In addition to the constituent elements also dealt with in Chapter 5.1 there are many **factors and/or relationships** which could influence the risk and which need to be considered **case by case**. For example, to prevent dust explosions the thickness of deposits need to be dealt with.

The performance influencing factors are often subject to investigations by means of special methods and/or analysis techniques. The specific techniques all have characteristics which makes their application more appropriate in some circumstances than others. Being aware of this requisite the tables listed in Annexes I to IV offer methods and/or techniques that could favourably be applied. This allocation doesn't imply any priority nor any ranking.

Sometimes the constituent elements of the different main fields to be analysed must be considered in combination with each other. For example, the "phases of equipment life" needs to be assessed taking into account the "selection of material". In this respect, the analyst should be aware that there are cross-references between the main fields to be analysed.

Many of the methods/techniques used require information to be gathered from different sources and by different individuals. Often a team approach is necessary when analysing the information particularly if complex structures are being assessed.

A description of techniques is listed in Annex VIII which proved to be efficient in mechanical electrotechnical and chemical engineering. They are likely to be favourably applied to equipment for use in explosive atmospheres in a modified way. Some of the techniques provide suitable tables for recording the results of the analysis, other require diagrams to be drawn and examples are given of what these should look like.

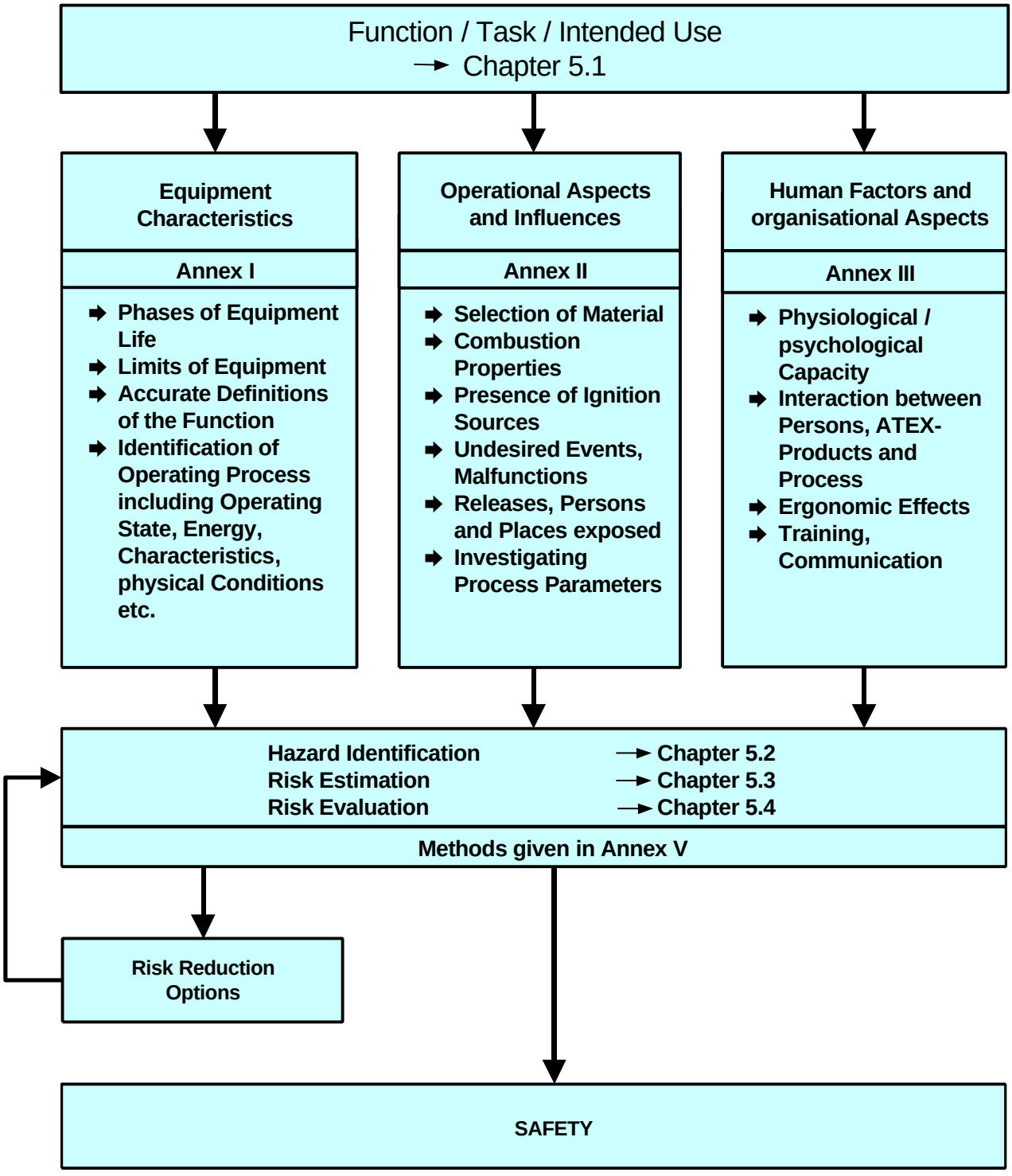


Figure nine: SIMPLIFIED RISK ASSESSMENT PROCESS
- Iterative Process to achieve Safety -

Annex I: Equipment characteristics

Constituent Elements / Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
Phases of equipment life ♦ construction ♦ transport and commissioning ♦ intended use ♦ de-commissioning, dismantling, disposal Limits of equipment / unit operations ♦ use limits ♦ space limits ♦ time limits Accurate definitions ♦ function ♦ task ♦ intended use ♦ normal operation ♦ energy / power flow ♦ material / substances handled ♦ signal / information processed ♦ performance levels	assembly, installation, adjustment setting, teaching / programming, operation, cleaning, fault finding, maintenance; external effets: humidity, vibrations, contaminations, extraneous voltages; surrounding area conditions: severe operating conditions, rough handling, changing environmental conditions; physical geometry and arrangements; actions to be performed within proper time, in correct order and completely; energy balance, buffer timing exposure of other persons to the process / hazards; safe functioning for the intended purpose including process change-over;	**Functional / State – Analysis:** to define the status of the materials being handled and the equiment itself being available A complex function / task is broken down into a number of more simple sub-tasks. Each sub-task may then be broken down into further sub-tasks. This process is continued until the sub-tasks reach the level of individual tasks. **Additional Hazard Identification Techniques:** - checklists - Hazard and Operability Study (HAZOP) - Concept Safety Review - Preliminary Hazard and Consequence Analysis

Annex I: Equipment characteristics

Constituent Elements / Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
Identification of operating process including those conditions which are not considered to be part of normal operation, e. g. • standstill • start-up • breakdown • releases caused by accidents • failures which involve repair • shut-down	Operating state • energy (heat, temperature, pressure, cold) • characteristics (mixing, spraying, transporting etc.), • physical condition of the substance (solid, grained, dusty etc.)	**Reliability Block Diagram** **Failure Mode and Effect Analysis (FMEA)**

Annex I: Equipment characteristics

Constituent Elements/Parameter to be considered as a screen	**Factors/relationships which could influence the risk**	**Methods / Techniques following Annex V that could favourably be applied**
Construction of equipment with due regard to technological knowledge of explosion protection and quality assurance.	Quality objectives and the organizational structure, responsibilities and powers of the management with regard to product quality; Establishing and updating of technical documentation, such as description of the equipment, conceptual design and manufacturing drawings, results of design calculations made; Monitoring the effective operation of a quality system; To carry out periodically audits;	**Application of moduls** laid down in Directive 94/9/EC whereby the manufacturer ensures that the equipment satisfy the requirements of the Directive: - internal control of production - product quality assurance - conformity to type - product verification - production quality assurance combined with specific technology related to explosion prevention and protection

Annex II: Operational aspects and influences

Constituent Elements/Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
Selection of material used to construct equipment, protective systems and components	material must not trigger off an explosion, taking into account foreseeable operational stresses, physical and thermodynamic properties, flammability, reactivity, characteristics, corrosivity, structural strength; it must not be possible for a reaction; to take place between the materials used and the constituents of the potentially explosive atmosphere; predictable changes in material's characteristics and their compatibility in combination with other materials will not lead to a reduction in the protection afforded;	**Concept Hazard Analysis** is particularly good at identifying hazards that are inherent due to the design concept of unit operations and equipment
Combustion properties taking into account materials contact or mixing with the air (see Logic Diagrams for Testing and Design in Annex V)	substance's burning behaviour, e. g. flash point, explosion limits, limiting oxygen concentration; explosion behaviour, e. g. maximum explosion pressure, maximum rate of explosion pressure rise, maximum experimental safe gap;	**Relevant Data Review** providing appropriate information relating to the integrity and safety of products involved

Annex II: Operational aspects and influences

Constituent Elements/Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
Presence of potential ignition sources capable of igniting the atmosphere taking discrete items and their possible interactions into consideration (see Logic Diagram for exclusion of ignition sources in Annex VI) Undesired events: Dangerous disturbances, operating faults, overloading of equipment and unit operations	Hazards arising from different ignition sources becoming effective such as sparks, flames, electric arcs, high surface temperatures, acoustic energy, optical radiation, electromagnetic waves and other ignition sources; Forming of products which promote the ignition of the original atmospheres; Temperature increases due to chemical reactions, moving parts, poor lubrication, ingress of foreign bodies etc.; Ignition caused by portable equipment, or outside influences; Beside normal operation dangerous events as a result of malfunctions and incidents; Consideration by means of integrated measurement, regulation and control devices (cut-off switches, limits, monitors etc.)	**Hazard and Operability Study (HAZOP)** for identifying those process variables which can lead to hazards and/or operability problems **Failure Mode and Effect Analysis (FMEA)** to go through the system component by component asking questions about the failure mode and it's cause and effects

Annex II: Operational aspects and influences

Constituent Elements/Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
Manufacturing process including access to the inspection, testing and storage premises.	Quality records, such as inspection reports and test data, calibration data, reports on the qualifications of the personnel concerned; Examinations, verifications and tests to be carried out relating to the anti-explosive protection aspects and its efficacy; Professional integrity and technical competence of inspection staff. To possess the necessary facilities for performing properly the administrative and technical tasks connected with verification and quality assurance;	**Standards Review** Design details and test results are compared with the requirements of standards to ensure that the design and the manufacturing process are consistent with the published "state-of-the-art" for that type of product,

Annex II: Operational aspects and influences

Constituent Elements/Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
release of flammable gases or dusts relating to the system	to employ, wherever possible, enclosed structures for avoiding the release of flammable gases or dusts; openings or non-tight joints with view to developing gases or dusts (safe opening); escapes of flammable materials during filling or draining.	**Event Tree Analysis** to analyse the consequences of the top event of a fault tree (e. g. an Event Tree for Flammable Release)
places exposed to hazardous explosive atmosphere	explosive atmosphere to occur in such quantities as to require special precautions; cleaning of equipment and protective systems; thickness of deposit to prevent a heat build up on surfaces;	**Classification of hazardous plants** to determine the extent of measures, the hazardous places are classified into zones based on the frequency and duration of occurance of a hazardous explosive atmosphere

Annex II: Operational aspects and influences

Constituent Elements/Parameter to be considered as a screen	**Factors/relationships which could influence the risk**	**Methods / Techniques following Annex V that could favourably be applied**
elimination or minimization of dangerous events by investigating process parameters	coincidence of an explosive atmosphere and the effective ignition source; substitution or reduction of amount of substances capable of forming explosive atmospheres; reliance on the automated process control systems to insure the safe operation	**What–If-Analysis** supplemented by **check-lists** of questions to ask about specific items of unit operations and equipment (e.g. blockages, partial failures) **Fault Tree Analysis** to identify the individual events and the logic which links them in order to realise a hazard.
maintenance activities	diagnosis of underlying failure; preparation required for repair; checks to be required after maintenance; normal operation to be restored.	**Maintenance Analysis** to allow maintenance strategy and procedures to be optimised for safety, availability and efficacy

Annex III: Human factors and organisational aspects

Constituent Elements/Parameter to be considered as a screen	Factors/relationships which could influence the risk	Methods / Techniques following Annex V that could favourably be applied
human performance shaping factors (external/internal)	• lack of communication, training, • inadequate management of change procedures, • organisational preconditions (hierarchies), technical predictions • physiological/psychological capacity, • fitness, willingness,resources, • interaction between persons/ with the equipment	**Task Analysis** to allow complex tasks to be analysed in detail **Human Reliability Analysis** to predict the frequency of human failure supplemented by other techniques
human intervention	• level of confidence in carrying out the required tasks without intentional or unintentional deviation • awareness of risks • difficulty of tasks • design of the products in relation to ergonomic principles	**Action Error Analysis** to form basis for quantitative analysis

Annex IV: Risk estimation and evaluation

Constituent Elements / Parameter to be considered as a screen	**Factors/relationships which could influence the risk**	**Methods / Techniques following Annex V that could favourably be applied**
Severity of the possible harm which can result from each hazardous event (fatality)	nature of what is to be protected (persons, property, environment); severity of injuries or damage to health (reversible, irreversible, death); extent of harm (explosion behaviour, persons exposed)	**Failure Mode** and **Effect Critically Analysis (FMECA)** by ranking the hazards arising from the failure mode identified in either a qualitative or a quantitative way.
Probability of occurrence of the harm considered Possibilities of avoiding or limiting harm (see Frequency-Severity Matrix in Annex VII)	type, frequency and duration of exposure to detect failure sufficiently rapidly and accurately by appropriate technical means, such as safety devices, controlling devices, regulating devices; to secure equipment/operations in the event of safety device failure; the presence and reliability of protective systems provided; human possibility of avoidance or limiting harm;	**Short Cut Risk Assessment** to obtain a measure of the risk on a quantitative scale based on a largely qualitative assessment of the risk.

Annex IV: Risk estimation and evaluation

Constituent Elements / Parameter to be considered as a screen	**Factors/relationships which could influence the risk**	**Methods / Techniques following Annex V that could favourably be applied**
Risk for each severity level to be evaluated against corresponding criteria	values shown for the worst severity level; tolerability of risk; various injury compensation schemes; additional protective or safety measures; possibilities for any new hazards to be introduced by the modification to the design; to revisit the hazard identification step;	**Comparison of risks** Based on specific conditions of use and comparable technical targets Supported by techniques, such as **MOSAR, FMECA** and **Quantified Risk Assessment (QRA)**

Annex V

List of Risk Assesssment Techniques

1. Hazard and Operability Study (HAZOP)

Purpose: Hazard Identification

Limitations: Qualitative technique. Very time-consuming and laborious for complex systems. Requires detailed design drawings. Guide words would need to be developed for explosive atmospheres applications.

Advantages: Systematic and comprehensive technique.

Description of technique: HAZOP is carried out by a team of usually 4-6 people including a trained leader (with safety and reliability experience) and those involved in the design and the operation of the process to be studied. A detailed Piping and Instrument (P&I) diagram of the plant is required for the HAZOP so that the design needs to be well-advanced but still capable of change at the time that the HAZOP is performed.

The team look at each line of the P&I in turn, and systematically apply a set of guide-words to each of a set of process variables. For a chemical process, the process variables would include: PRESSURE, TEMPERATURE, FLOW, REACTION, LEVEL, COMPOSITION. Typical guide-words are NO/NOT/NONE, MORE, LESS, PART, REVERSE, OTHER THAN, AS WELL, SOONER, LATER. For each combination of process variable and guide-word, the team ask whether this can occur, whether it would be a hazard (or an operability problem) if it did, and, if so, what protects against it happening and is the level of protection sufficient. This is a very detailed and time-consuming process. Note that operability problems are also potential safety problems because the operator will find a way around the problem, probably in a way that the designer did not intend.

Records are kept of the HAZOP and computerised systems for doing this are available. The essential records are a list of agreed actions to sort out problems which have been identified. A system is required for ensuring that these actions are carried out, and the design modified as necessary. HAZOP review meetings are one way of achieving this. Attention can be given in these meetings to whether the modification has introduced further hazard or operability problems. It is also possible to keep records for lines which do not require action, and whether or not this is done tends to be a matter of individual company policy.
Different companies have developed different variations on the process variables and guide-words to suit their particular industry.

Products applicable to: complex items of process plant

This technique focuses on what happens to the substance being processed and how loss of control of process conditions can lead to undesirable events, in particular loss of containment. It is based around Piping and Instrumentation diagrams for process units or entire plants. Whilst it is invaluable for identifying process parameters which can lead to loss of containment events it would need significant modification to enable the identification of ignition sources. We also consider it to be over complex for discrete items of equipment. If this technique is kept then it needs to be made clear that it will only identify the potential for the creation of an explosive atmosphere through loss of containment and will not identify ignition sources. It also needs to be pointed out (under limitations subheading) that those doing a HAZOP must be competent and trained in the technique for it to be used effectively.

2. Fault Tree Analysis

Purpose: Identifying the individual events and the logic which links them in order to realise a hazard (top event). Can be used to predict frequency of the top event if quantitative data is available.

Limitations: Time-consuming for complex systems. Training is required in the technique otherwise errors in the logic can easily be made. Requires data for all the separate events eg component failure rates, human error, probability of exposure, fractional dead time of protective systems etc.

Advantages: Quantitative technique. It is the only technique available for predicting hazard frequency for novel systems and also proves useful for complex systems.

Description of technique: A fault tree is a method by which a particular undesired system failure mode can be expressed in terms of component failure modes and operator actions. The fault tree would set out the logic for all the ways in which this could occur. This is recorded on a fault tree diagram.

A fault tree diagram contains two basic elements: "gates" and "events". Gates allow the passage of fault logic up the tree and show the relationships between events which are needed to cause the occurrence of a higher event. The two main types of gate are AND and OR. An AND gate indicates that all the events entering the gate are required to occur at the same time in order to cause the higher event. An OR gate indicates that only one of the events entering the gate is required to cause the higher event. There are also a number of other types of gates which are required less frequently to represent logic.

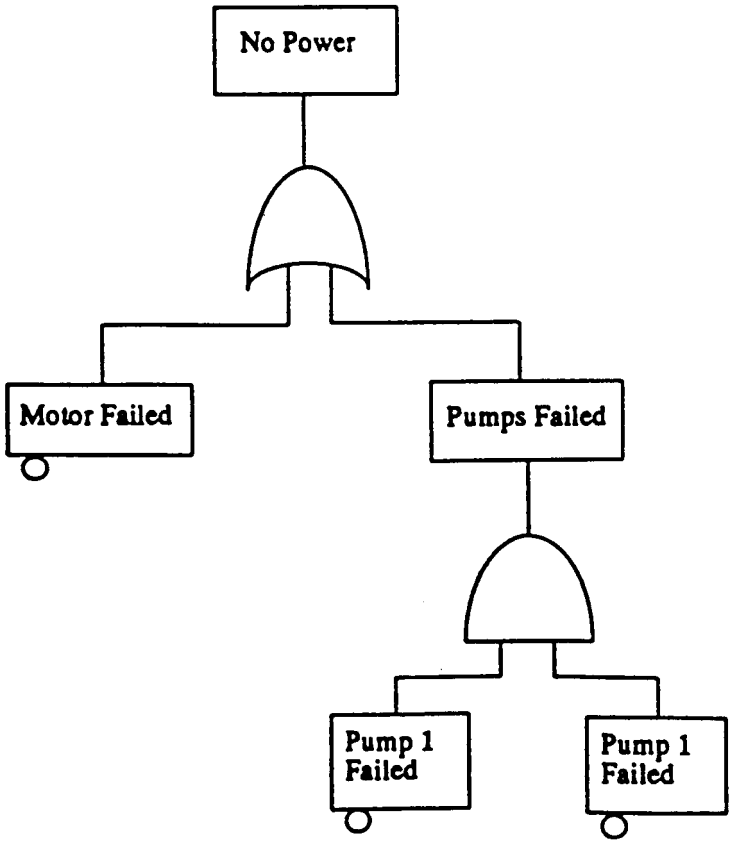
Once the logic has been written down in a fault tree, the frequency of the top event can be calculated, given data on the frequencies/probabilities of events at the lowest level on the tree. Such frequencies/probabilities will usually apply to failure rates of electronic, electrical or mechanical components, and such data may be available from databases. The probability of failure of human operators to act as desired can also be predicted. Fault tree arithmetic, which has a basis in Boolean algebra can then be used to calculate the frequency of the top event. At any OR gate frequencies can be added together. At any AND gate, one frequency and any number of probabilities can be multiplied together (as a first order approximation). In evaluating a fault tree it is important to be clear about which data are frequencies (units of events per unit time) and which are probabilities (dimensionless). There are also specialist techniques for evaluating large and complex fault trees, such as the technique of minimum cut sets.

Fault tree analysis is usually best done by specialists as there are potential pitfalls. If the logic represented by the fault tree is incorrect then the calculated frequency will also be incorrect. It is also quite easy to get the algebra wrong specially if the occurence of a Common Mode Failure is not taken into account.

Products applicable to: discrete items, complete machinery, and assessing the reliability of protective systems.

Would be over complex and prohibitively time-consuming for more complex machinery except when used, without quantification, to give a high level overview of the interaction between different components, functions. For a fuller description of this technique try IEC 61025: Fault Tree Analysis (FTA)

Figure A.1 - A Fault Tree Showing Failure of Power Supply



3. Event Tree Analysis

Purpose: Consequence analysis and frequency prediction.

Limitations: Probabilities of different events leading from the hazard/top event of the fault tree are required for quantitative analysis.

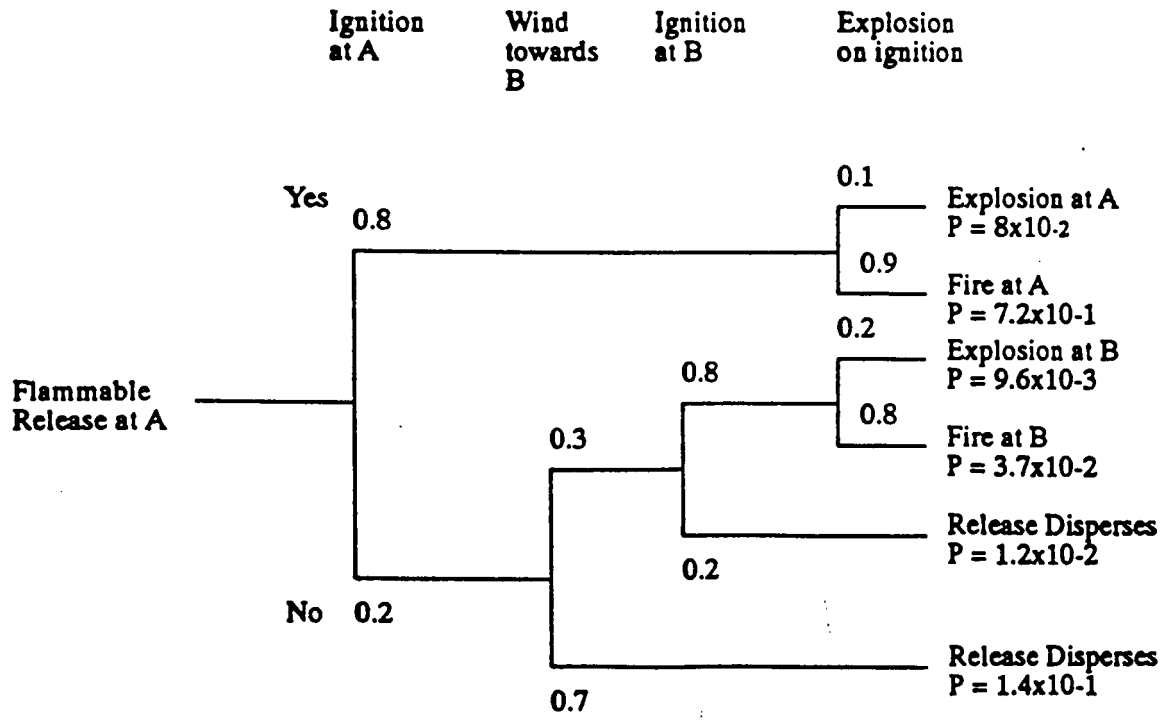
Advantages: Relevant when a hazard (top event) can have multiple consequences.

Description of technique: Event trees can be used to analyse the consequences of the top event of a fault tree. The starting point of the event tree is therefore the finish point of a fault tree. It shows the probabilities of different scenarios, each with a different consequence, which could be generated by the earlier identified hazardous event. For example in the chemical industry a release of flammable gas could give rise to any of the following scenarios:

no ignition and safe dispersal, a jet fire, a flash fire, a vapour cloud explosion

An event tree is constructed from left to right. Each node is a possible event and there are two branches from each node: one in which the event did occur and one in which it did not. Probabilities can then be put onto the occurrence or non-occurence of each event. Simple arithmetic can then be used to determine the probability of each consequence.

Figure A.2 – An Event Tree for a Flammable Release



4. Preliminary Hazard and Consequence Analysis

Purpose: Identifying the underlying causes of a top event.

Limitations: Requires a knowledge of the major hazards and a team. Will not identify all the causes.

Advantages: Can be done at concept design stage so encourages inherently safe design. Systematically identifies the events and factors involved in an accident scenario in chronological order from initiation of the accident to its final consequences. Facilitates the building of fault trees and event trees.

Description of technique: This analysis is done in two parts. The first part deals with the scenario from immediate causes through to the significant event. The study is conducted by a team using the first of the forms overleaf. One form would be used for each significant event already identified by a concept hazard analysis. In the chemical industry for example one such event would be vessel rupture. The columns for dangerous disturbance and hazardous disturbance could then be filled in. For vessel rupture they would be over-pressure and high-pressure respectively. The remaining three columns would then be filled in with all the events that could lead to the hazardous disturbance, the reasons why this could progress to an dangerous disturbances and how recovery failed allowing the realisation of the significant event. The second part is the analysis of the potential consequences through various levels of escalation using the second of the forms overleaf. For use with equipment the headings of the table would need some modification perhaps so that there were more levels available up to the significant event and less after for consequence analysis. The first form can then be used to build a fault tree and the second to build an event tree.

Products applicable to: Complete machines, complex products and interaction with protective systems

This is actually two related techniques Preliminary Hazard Analysis (PHA) and Preliminary Consequence Analysis (PCA). PHA is used as an aid to drawing a fault-tree for the loss of containment top event taking the results of a HAZOP as a starting point. If kept the same cautions given under HAZOP regarding the fact that only considering the loss of containment event are required. PCA is an aid for drawing an event tree starting with the loss of containment event. It is probably less helpful except in cases when there are a range of possible consequences and when taking into account the effects of suppression and protective systems. The manufacturer, particularly of discreet items, is unlikely to have the necessary information. It is therefore only appropriate for complex equipment where there is close liaison between user and manufacturer about the exact operating conditions under which is going to be used. Again this technique needs to be treated with some caution as it focuses on hazards essentially initiated by loss of containment (i. e. not normally occuring flammable atmospheres).

Plant: **PRELIMINARY HAZARD ANALYSIS SHEET** **Date:**

MPI:

IMMEDIATE CAUSES	INADEQUATE CONTROL	HAZARDOUS DISTURBANCE	INAD. EMERGENCY CONTROL	DANGEROUS DISTURBANCE	FAILURE TO RECOVER	SIGNIFICANT EVENT
RECOMMENDATIONS, COMMENTS, ACTIONS						

Plant: **PRELIMINARY CONSEQUENCES ANALYSIS SHEET** **Date:**

MPI:

SIGNIFICANT EVENT	FAILURE TO MITIGATE OR AVOID ESCALATION	CONSEQUENCES OF SIGNIFICANT EVENT	FAILURE TO PREVENT FURTHER ESCALATION	CONSEQUENCES OF ESCALATION	FURTHER ESCALATION
RECOMMENDATIONS, COMMENTS, ACTIONS					

5. Quantified Risk Assessment (QRA)

Purpose: Frequency prediction, consequence prediction

Limitations: Very time-consuming unless, and even when, computerised. Requires skilled practitioners and failure data.

Advantages: Quantitative technique.

Description of technique: QRA puts together fault tree analysis, event tree analysis and numerical modelling of each type of consequence in order to obtain hazard ranges. It is best used when an objective criteria exists for the risk of certain events. The QRA calculates a risk for comparison with the criteria.

Input to the model is information on the hazards: sources of leak of hazardous materials to the environment, together with flowrates and frequencies. The model provides output in terms of risk versus distance contours for particular levels of harm.

There are a number of uncertainties in QRA. The three main areas in which uncertainties exist are:

1. In the historically derived failure frequencies;
2. In the consequence models which predict hazard ranges;
3. In the prediction of the harm which a given level of exposure will do to a person.

A computerised model is not essential for QRA, but without one the process is extremely time-consuming and tedious, and is subject to numerical errors.

6. Short Cut Risk Assessment

Purpose: Frequency and consequence estimation.

Limitations / Advantages: Screening technique.

Description of technique: A short-cut risk assessment is a method of obtaining a measure of the risk on a quantitative scale, based on a largely qualitative assessment of the risk. The Dow and Mond indices, once used extensively in the chemical industry for ranking of risks prior to more exhaustive analysis, are examples.

One such method, developed for use in the chemical industry, is as follows:

Target risk is defined by Target risk $= \log_{10}10^{L} + \log_{10}10^{S}$
$= L + S$

where L is the exponent of the likelihood (measured by frequency – negative value) and S is the severity ranking.

The scale for severity is chosen so that the target risk is only acceptable if it is less than or equal to zero. A preliminary estimate of the risk can be obtained by using experienced judgement about the severity, and getting a rough estimate of the frequency from published data.

TABLE 1 – SEVERITY RANKINGS

CATASTROPHIC CONSEQUENCES: **Severity 5**

Catastrophic damage and severe clean-up costs
On-site: Loss of normal occupancy > 3 months
Off-site: Loss of normal occupancy > 1 month
Severe national pressure to shut-down
Three or more fatalities of plant personnel
Fatality of member of public or at least five injuries
Damage to SSSI or historic building
Severe environmental damage involving permanent or long-term damage in a significant area of land
Acceptable frequency 0.00001 per year

SEVERE CONSEQUENCES: Severity 4

Severe damage and major clean-up
Major effect on business with loss of occupancy up to 3 months
Possible damage to public property
Single fatality or injuries to more than five plant personnel
A 1 in 10 chance of a public fatality

Short-term environmental damage over a significant area of land
Severe media reaction
Acceptable frequency 0.0001 per year

MAJOR CONSEQUENCES: Severity 3

Major damage and minor clear-up
Minor effect on business but no loss of building occupancy
Injuries to less than five plant personnel with 1 in 10 chance of fatality
Some hospitalisation of public
Short-term environmental damage to water, land, flora or fauna
Considerable media reaction
Acceptable frequency 0.001 times per year

APPRECIABLE CONSEQUENCES: Severity 2

Appreciable damage to plant
No effect on business
Reportable near missincident under CIMAH
Injury to plant personnel
Minor annoyance to public
Acceptable frequency 0.01 times per year

MINOR CONSEQUENCES/NEAR MISS: Severity 1

Near-miss incident with significant quantity released
Minor damage to plant
No effect on business
Possible injury to plant personnel
No effect on public, possible smell
Acceptable frequency 0.1 times per year

7. Concept Safety Review

Purpose: Hazard Identification.

Limitations: Initial review only.

Advantages: Done at concept design stage so encourages inherently safe design.

Description of technique: This is used in the chemical industry at a very early stage in the design of a chemical plant – before the flow-sheet has even been developed. It looks at the options available, considers general organisational issues. A general information gathering exercise is undertaken regarding previous incidents both within and outside the organisation, the hazardous properties of those chemicals likely to be used and any alternatives.

The team looks at the objectives of the project, at possible process routes and at the chemicals that would be used for each route and the effluents generated. The objective is to obtain an appreciation of possible hazards in the process, of whether one chemical route would be expected to be better than another in terms of hazards, and of what legislation will be relevant to the proposed plant. This is the point when the extent and timing of all further safety reviews should be set. This review should be a means by which improvements in design procedures are made known to the designers and by which it is ensured that current thinking on ways of improving the design practice are implemented.

Products applicable to: All (particularly if combined with comparison with standards technique)

This is a useful technique and encourages inherent safety. It is very much aimed at the concept phase of a project. The inherent hazards of substances are considered in terms of the health and safety of personnel and the public and the environmental impact. Inherent safety is achieved by considering first whether a safer substance can be substituted and then whether inventories can be reduced. Additional guidance and worked examples would be required to show how it can be applied to Atex type products.

8. Concept Hazard Analysis

Purpose: Identification of major hazards.

Limitations: Concentrates only on major hazards.

Advantages: Done at concept design stage so encourages inherently safe design.

Description of technique: This can either take the form of a simple initial review of hazards or a more formal detailed review of hazards, their causes and possible safeguards. In both cases the plant is broken down into mangeable chunks each of which are considered using keyword such as EXPLOSION to stimulate discussion. In the case of the initial review each keyword is recorded along with the discussion and any recommendation/actions in a simple three columned table. In the case of the more formal analysis the table is broken down into six columns with the heading Ref No, Keyword, Dangerous Disturbance (Hazard), Cause/Consequences, Suggested Safeguards and Comment/Action.

Products applicable to: All except components

This is the most obviously useful technique. However appropriate keywords and an appropriate format for recording the analysis need to be developed. Clear guidance on how to use this technique with examples is also needed. However as the keywords will be along the same lines as the checklist this technique may be indistinguishable.

9. Critical Examination of System Safety (CEX)

Purpose: Hazard Identification

Limitations: Qualitative technique requiring a team approach which would need to be adopted as part of the design process. To be effective a number of departments would need to be involved eg design, service, safety.

Advantages: Allows and overall appreciation of hazards. Encourages innovation and inherent safety by design.

Description of technique: This method was the precursor of HAZOP in the chemical industry.

The method uses a team in brainstorming mode. It can be carried out at an early stage in the design, earlier than HAZOP. The method asks a series of questions about aspects of the safety system such as: What, When, How and Where, and these could be enhanced by the questions: Why, Why then, Why that way, Why there.

The questions can be used to create answers about the proposal (eg what is to be achieved by the safety system), alternatives (what else could be achieved), and conclusions (what should be achieved). The answers can then be used to specify the safety system, and implement it preferably by an inherently safe design.

10. Check-lists

Purpose: Hazard Identification

Limitations: Depends on relevance of check-list.

Advantages: Simple, can be used by individual or team.

Description of technique: A list of possible hazards is taken and each item on the list is considered in terms of whether it applies to the system being studied.

Check lists are a Comparative Method and may be derived from experience alone (including codes of practice and standards) or may be derived for a particular type of plant from application of the fundamental techniques, avoiding the need to repeat the whole study when a very similar design is to be considered.

Check lists are essentially a simple and empirical means of applying experience to designs or situations to ensure that the features appearing in the list are not overlooked.

Lists are the most basic method of hazard identification. They may relate to material properties or, for example, they may be equipment specific.

A check list will serve as a list of subject pointers which will require attention at each stage in the life of equipment and unit operations. They are most effective when used to stimulate thought and enquiry through open ended questions rather than in the form that requires yes/no answers.

11. Standards (comparison of designs with known safety standards)

Purpose: Hazard Identification

Limitations: Careful consideration needs to be given to the scope of application of standards to ensure that they apply. They can be time consuming to understand and many standards may be necessary to cover all aspects.

Advantages: They provide authoritative guidance, particularly to the integrity of detailed designs, and they can provide a quick check on safety requirements or factors which need to be considered. Most designers appreciate the value of standards and use appropriate ones on a regular basis.

Description of technique: Design details are compared with the requirements of standards. The standards may be written by groups of experts to give International or national requirements or they may be developed in-house to accepted, well established standards.

12. Sneak Analysis

Purpose: Hazard Identification

Limitations: Qualitative technique requiring skilled practitioner. Time-Consuming for complex systems.

Advantages: Takes account of topography/layout.

Description of technique: Sneak analysis is a technique which aims to identify hazards associated with the topography of process plants – i.e. how the different components are connected together. It is a development of Sneak Circuit Analysis which is used for electronic circuits.

The objective is to identify sneak paths, i.e. paths by which material or energy can unintentionally flow between different parts of the system. The method can be simplified by the use of "clues" which are statements about common topologies and the sneaks that can be associated with them. Such clues can form effective check-lists.

A "sneak" is a condition which allows an action to take place along an unintended path. A path is defined as the way in which things move from one place to another, including electric current in wires, fluids in pipes, information in an organisation, data and control in a computer program. Unintended paths are ones which the designers did not intend to exist. Such paths may be the result of design error, failure of components or actions of personnel.

Sneak analysis is done by a team in a similar way to a HAZOP. It is an addition rather than an alternative to a HAZOP and it has been suggested that it has particular advantages for batch plants.

13. Task Analysis

Purpose: Hazard Identification

Limitations: Only applicable to human error analysis. Very time-consuming except for very simple tasks.

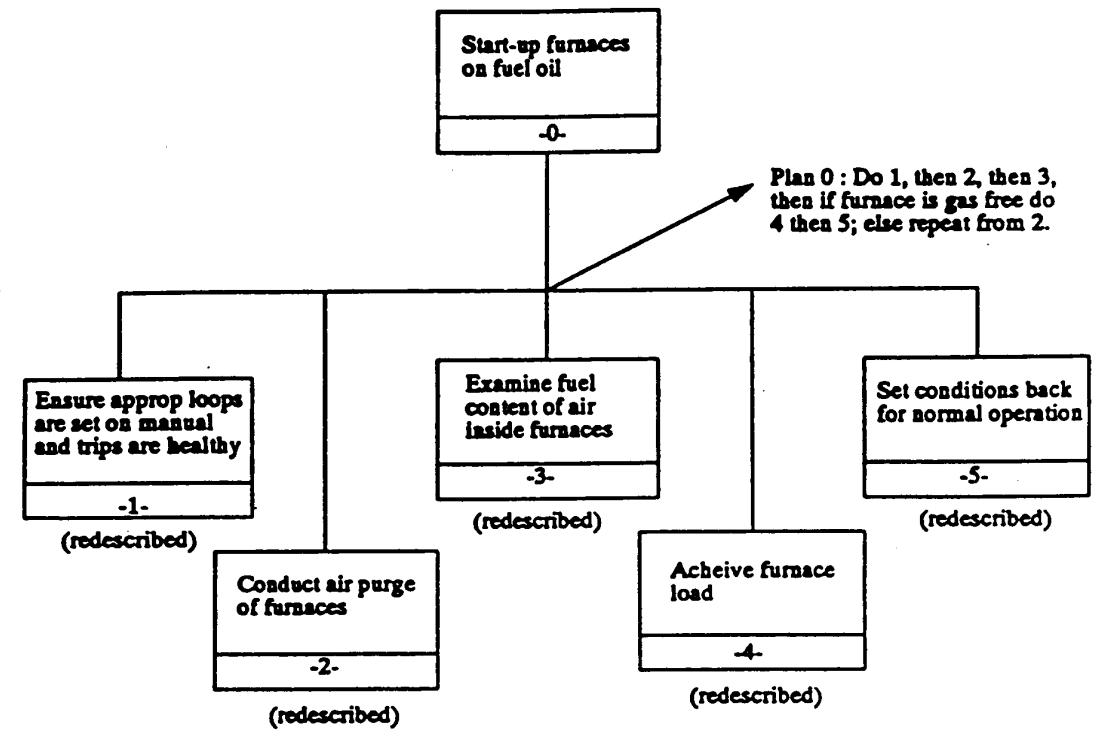
Advantages: Allows complex tasks to be analysed in detail and understood.

Description of technique: Task analysis derives from method study techniques. It is a systematic method for analysing a task into its goals and the actions and plans required to achieve these goals.

The overall task first needs to be described in terms of its goals, actions and plans. One technique is hierarchical task analysis (HTA) where a complex task is broken down into a number of more simple sub-tasks. Each sub-task may then be broken down into further sub-tasks. This process is continued until the sub-tasks reach the level of individual tasks.

The hierarchical task analysis is recorded as a tree structure showing this break down i.e. all tasks entering a sub-task at the next level of the tree have to be done in order to achieve that sub-task. The plan for each operation can also be recorded on the tree (see diagram). Task analysis can be used for developing operating procedures and training, job aids, and as an input to human error analysis.

Figure A.3 – Hierarchical Task Analysis



14. Hazardous Human Error Analysis (HHEA)

Purpose: To identify hazards associated with human interaction with equipment

Limitations: Focuses on the operator and may neglect other persons at risk. Only takes into account equipment failure in a limited way.

Advantages: Fully takes into account human factors including foreseeable misuse. Can be used equally well for all phases of use from commissioning through maintenance and decommissioning.

Description of technique: This is a new technique, developed by the risk assessment section of the UK Health and Safety Laboratory, HSE, takes elements from Task Analysis and Action Error Analysis and combines them. It is best carried out by a team of not less than 3 persons and no more than 8. Rather than keywords as such, key questions and a list of human-error type classifications (from Action Error Analysis) are used as discussion points to "brainstorm" ideas. Record sheets in the form of tables are also used to structure the discussions and keep a record of them. The effectiveness of the analysis is dependent on the skill of the chairperson who has to ensure that the team is thorough whilst not getting bogged down in detail.

It is particularly important when carrying out a HHEA to have at least one person in the team who has a detailed appreciation of how the machine is likely to be operated. This can for example be an experienced operator of this type of machinery or someone who has a lot of contact with the operators, such as a service engineer.

Before starting the analysis it is important to clearly define all the relevant phases of machinery life. Any user manual or instructions for use would be a particularly good starting point for this technique.

The key tasks relating to the use of the machine then need to be listed. This is best done as a brainstorming session by the chairperson writing them down on a wipe-board or flip-chart as they are called out. They will then need organising into a logical order and any duplicates removed. Some of the tasks listed may be sub-tasks of others and should be organised to reflect this fact. It is important that these sub-tasks are not simply deleted.

Each key-task should then be considered in turn and broken down into more detailed sub-tasks and numbered. The human error type classifications listed overleaf are then used, in a similar way as keywords, to brainstorm a list of potential human errors that can be made in carrying out the task and moreover, the hazards that these errors will expose the operator to.

Error type	Explanation
Error of omission	Failure to perform an action, absence of response.
Error of time	Action performed but not at or within proper time.
Extraneous act	Unnecessary action not required by procedure
Transposition	Correct action on wrong unit, system, train or component.
Error of selection	Incorrect selection control

Error of sequence	Performance of correct actions in wrong order if this is significant for success of the task.
Miscommunication	Failure to communicate or receive information correctly.
Qualitative errors	By excess or by default (perform action incompletely).
Other	Anything else.

Each error is given a unique reference number and discussed in turn by the team to consider:

- What hazard the human error would expose the operator or any bystanders to?
- What is the range of consequences, from most usual to worst, likely to result?
- What factors could increase the risk of harm?
- What actions/factors could decrease the risk of harm, including existing safeguards which will protect against the error being made, or the hazard thus exposed causing harm?
- What safeguards are suggested to protect against the error being made or the hazard thus exposed causing harm?
- Finally, are there any further comments that need to be made or any actions that need to be carried out, and by whom?

The record sheets for use with the analysis described above is shown at the end of this appendix. Each sheet is headed “HAZARDOUS HUMAN ERROR ANALYSIS” and has space at the top for recording:

- the machine on which the analysis is being carried out;
- the key-task to which the sheet relates;
- the date of the analysis;
- the sheet number and the total number of sheets used.

It is recommended that a fresh record sheet be used for each key task. There are a total of eight columns in the table on the sheet which are used as follows:

“SUB-TASK” is used to record the sub-task and its number;

“REF-NO” is for a unique reference number for each identified potential human error that could be made whilst carrying out the sub-task under consideration;

“POTENTIAL HUMAN ERROR” is used to record each human error that the team thinks could be made whilst carrying out the sub-task under consideration;
“HAZARD EXPOSED TO” is used to record information about the hazards that each error would expose a person to;

“CONSEQUENCES” is used to record a brief description of what could happen should the hazard be realised in terms of the range of possible consequences from the most likely to the worst case, whether these are RIDDOR reportable, and how many people may be involved;

“INCREASING FACTORS” is used to record what factors or actions could increase the likelihood of the error occurring and/or the risk of harm;

“DECREASING FACTORS” is used to record what factors or actions could decrease the likelihood of the error occurring and/or the risk of harm, including any existing or proposed safeguards;
“COMMENTS / ACTION” is used to record any additional information which doesn really fit anywhere else, any references (particularly standards) considered to be useful and any actions – usually to look at something in more detail at a later date
Note when recording actions it is important to make sure that it is clear who is expected to carry them out.

15. Human Reliability Analysis

Purpose: Frequency prediction for human failure.

Limitations: Time-consuming. Relies on availability of human failure rate data for the lowest level individual tasks. Requires a skilled human factors practitioner.

Advantages: Quantitative technique allowing limited prediction of human error.

Description of technique:The first steps in this are hierarchical task analysis and action error analysis. It is important to note for each task analysed what the effects of error at this stage would be, and whether or not it would result in a hazard. For those errors which would result in a hazard, is error recovery possible? Probabilities are then assigned for each human error in the hierarchy which would lead to a hazard. This would usually be on the basis of historical data for the same error mode.

The probabilities would be modified on the basis of the evaluation of:

- Performance influencing factors (PIFs). These range form environmental and ergonomic factors to the safety culture of the organisation.

- Recovery factors (RFs). The likelihood that the operator will notice and recover from the error.

- Error Reduction Strategies (ERSs). These are usually a redesign of the task/environment as a result of the above analysis.

The analysis would need to be carried out by a human reliability specialist, usually with computerised support. This type of analysis can be very time-consuming.

16. What-If ? Analysis

Purpose: Frequency prediction for human failure.

Limitations: Qualitative technique requiring suitable check-list.

Advantages: Easy to use.

Description of technique: A what-if analysis is carried out by a team and asks questions relating to specifc aspects of the design intent (e.g., in the chemical industry, such aspects as blockages, leaks, corrosion, vibration, partial failures, external events).

The experience of the team members can be supplemented by checks lists of questions to ask about specific items of equipment. The answers to the questions may reveal hazards that require elimination or protection.

What-if List for Compressors

What if high temperature in compressor?
What if loss of cooling?
What if excessive recycle around compressor?
What if loss of lubrication?
What if compressor valve failure?
What if insufficient flow through compressor?
What if excess compression ratio?
What if increase in feed temperature?
What if compressor subjected to local fire?

What if entrained liquid in feed?
What if contaminants or solid particles admitted to unit?
What if air entry due to vacuum or maintenance?

What if excessive speed or reverse rotation?
What if suction valve fails open?
What if excess recycle flow?
What if blocked discharge?
What if overpressure of compressor?
What if excess back pressure?

What if increase in feed pressure?
What if lack of demand for output stream?
What if failure of pressure control?
What if suction valve closed?

What if low feed pressure or feed line fails?
What if underpressure due to underspeed?

What if compressor stops or performance degraded?
What if mechanical deterioration in the compressor?
What if coupling to driver fails?

What if vibration loosens coupling?
What if deterioration of construction materials or seals?

What if inadequate isolation for maintenance?
What if inadequate procedures for maintenance and restart?
What if control system fails?

What if emergency control system fails?
What if relief system fails to reduce overpressure?
What if relief valve fails open?
What if relief valve fails closed?
What if inadequate flow through relief line?
What if failure of services?
What if compressor subjected to external cause?
What if freezing conditions or other environmental extreme?

Products applicable to: All

This technique is a brainstorming approach and is a particularly useful technique. It is best performed by a group of people who are familiar with the equipment, and consequently it would not be practical to suggest a generic What-if? list. This means that clear guidance is required, illustrated by examples, to show how a manufacturer can draw up a What-if? list for their products.
The 'What if..?' technique can be combined with the checklist analysis to increase the efficacy of the hazard identification. This combination of techniques is a method which is advocated by Det Norske Veritas and is referred to as SWIFT (structured what if checklist).

It is intended that the 'What if...?' questions are asked within categories, although there is no need to stick to this rigorously, suggested categories are [5]:

- Material problems
- External factor influences
- Operating error and other human factors
- Equipment/instrumentation malfunction

- Process upsets of unspecified origin
- Utility failures
- Integrity failure or loss of control
- Emergency operations

Alternatively the What-if? categories could be simpler for example using the PEEP concept (as described) in 'A guide to the Machinery Directive'):

- People (considers the interaction of personnel with the equipment)
- Equipment (hazards which are inherent to the equipment)
- Environment (considers the environment the equipment is to be used in)
- Process (the materials which are to be handled by the equipment)

At its simplest the technique generates a list of questions and answers, however a more detailed study could involve taking the analysis further for example identifying mitigating factors.

17. Reliability Block Diagram

Purpose: Hazard Identification

Limitations: Trivial except for complex systems.

Advantages: Can be used as a starting point for other techniques.

Description of technique: A reliability block diagram is a block diagram showing components in a system. It shows the logic of which components are required by other components in order for the system to work. It is capable of showing that some components are duplicated.

A reliability block diagram is in some ways similar to a fault tree, but has less capability for showing logic and is not focused on particular hazardous events. Reliability block diagrams are primarily tools for estimating the reliability of a system and rather than ist hazards.

Figure A.4 – Block Diagram of Power Supply

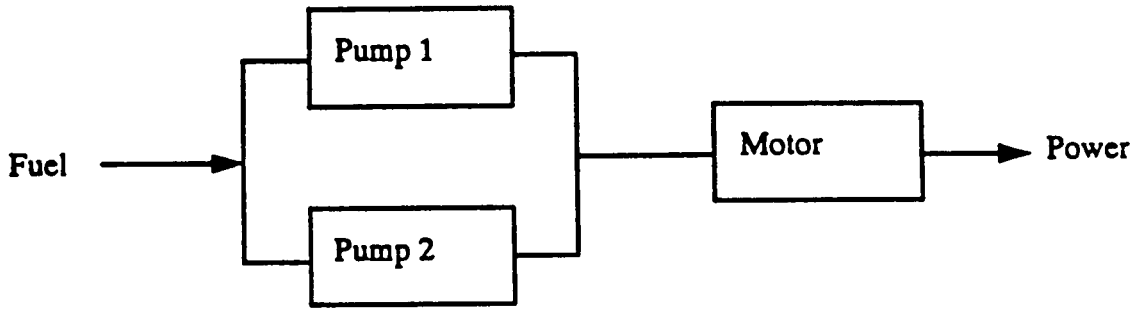
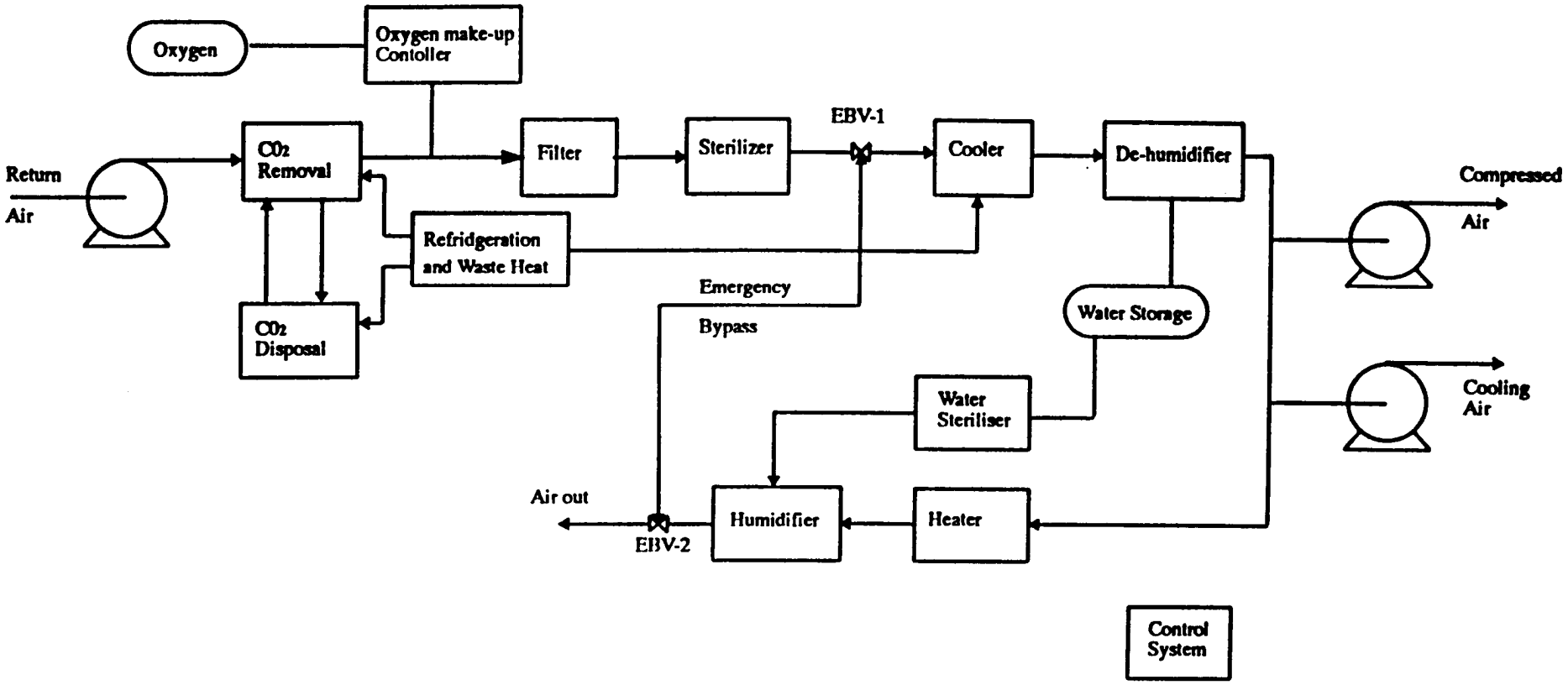


Figure A.5 – Reliability Block Diagram



18. Failure Mode and Effect Analysis (FMEA)

Purpose: Hazard Identification and consequence prediction

Limitations: Qualitative technique which is time-consuming to use, particularly if a complex systems is being analysed.

Advantages: Systematic and comprehensive technique.

Description of technique: FMEA is a qualitative technique for examining a system and identifying all the failure modes and their effects on the system. It is most usually used for electronic, electrical or mechanical equipment. The starting point of an FMEA would usually be a reliability block diagram for the system. A team would go through the system component by component asking questions about the failure modes for each component and the cause and effect of each failure mode. Methods of prevention or compensation for failures with significant hazardous effects would also be considered, so that the FMEA exercise would usually lead to a modified, safer design.

Products applicable to: Components, discreet items, simple protective systems
FMEA is a useful, wellknown technique and documented technique. For more detailed description try IEC60812 – Analysis techniques for system reliability – procedure for failure mode and effects analysis (FMEA). This technique is particularly useful for identifying failure modes which could lead to the creation of intermittent and permanent ignition sources or the failure of protective systems. FMEA could also be used to identify failures leading to loss of containment. However other techniques may be more appropriate. The purpose subsection should therefore be altered to reflect this. i. e. **purpose**: to identify failure modes that can lead to the creation of an ignition source.

Full blown FMEA is likely to be overly complex and time-consuming for complete or complex items of equipment and anything but the most simple protective systems. However in these cases Functional FMEA may be used.
A functional FMEA consist of the following steps:

1. Identify the functions of the equipment
2. What happens if the equipment fails to achieve each of its functions?
3. What are the mechanisms by which this failure can occur?
4. How do you recognise the failure?
5. Are there any recovery mechanisms?

Unlike the conventional FMEA study the equipment isn't broken down into single components, instead it is broken down into the functions which it is to perform. As an example a flammable gas detection and automatic isolation might be broken down into:

- Detection of flammable gas
- Transmit signal to ASOV (automatic shut-off valve)
- Valve closes and isolates flow

This method could be used at the beginning of the study to help the analyst produce a set of questions for the 'What if...?' study.

19. Failure Mode and Effect Criticality Analysis (FMECA)

Purpose: Hazard Identification, consequence and frequency prediction

Limitations: Time-consuming for complex systems

Advantages: Gives semi-quantitative ranking of risk.

Description of technique: This is similar to FMEA but goes further by ranking the hazards arising from the failure modes identified in either a qualitative or a quantitative way. There are a number of possible variations on the method.

Qualitative method

One method (DEF-STAN 00-41 – US Defence Standard) requires a qualitative probability of occurrence to be assigned to each failure mode. These are as follows:

	Level	Probability of Occurence, P
A	Frequent	1.0 > P > 0.2
B	Often	0.2 > P > 0.1
C	Occasional	0.1 > P > 0.01
D	Remote	0.01 > P > 0.001
E	Unlikely	0.001 > P > 0

Criticality number

A quantitative method from DEF-STAN 00-41 is to assign a criticality number to either a failure mode or a component.

Failure mode criticality number = abcde

where a = failure mode ratio = proportion of the failure probability for the component which is due to this failure mode.

b = conditional probability of mission loss (or that failure behave in a hazardous way).

Actual loss	b = 1
Probable loss	0.1 < b < 1
Possible loss	0 > b < 0.1
No effect	b = 0

c = failure rate modifying factor, if the failure rate used needs to be modified due to the particular environmental conditions in which the component is operating.

d = part failure rate = failures per hour of the component in the failure mode specified, preferably taken from operating experience in a similar environment, or else from a suitable database.

The item criticality is the sum of the failure mode criticalities for the item in question.

Risk Priority Number

Another semi-quantitative method for FMECA is the Risk Priority Number (RPN) method.

Three numbers are allocated for each failure mode and its effect:

1. Occurence of failure, on a scale of 1 to 10 where 1 is unlikely.
2. Severity of failure, on a scale 1 to 10 where 1 indicates minimal consequence.
3. Detection of failure, on a scale 1 to 10 where 1 indicates a high likelihood of fault detection and recovery.

The RPN is the product of the three numbers, and allows the effects of different failure modes to be ranked.

Failure Rate/Severity Method

For this method an FMEA is carried out, with columns asking questions about:

a) failure mode
b) failure cause
c) failure effect – especially whether it is local or effects the whole system
d) prevention/compensation what stops failure from effecting the whole system?
e) failure rate – taken from a suitable database
f) severity – a category is assigned

Category	I	Catastrophic.	Loss of life
	II	Critical.	Causes severe injury
	III	Major.	Causes minor injury
	IV	Minor.	Requires unscheduled repair

20. Maintenance Analysis

Purpose: Hazard Identification and frequency prediction for maintenance activities.

Limitations: Time-consuming. Requires skilled analyst.

Advantages: Maintenance problems looked at systematically using qualitative or quantitative techniques.

Description of technique: This is usually concerned with ensuring equipment availability, but could be relevant if there were particular hazards associated with maintenance.

The analysis can be done in either a qualitative or a quantitative way. The quantitative methods obtain a value for the availability of equipment given the need to periodically maintain it.

Maintenance analysis asks questions about:

- what failures can occur,
- how a fault would be identified/detected,
- how the underlying failure could be diagnosed,
- what preparation is required for repair,
- what resources are required for repair,
- how the failed part should be removed, repaired if possible, and replaced,
- what checks are required after maintenance,
- how normal operation should be restored.

21. Structural Reliability Analysis

Purpose: Hazard Identification consequence assessment.

Limitations / Advantages: Structural steelwork.

Description of technique: This is a method of looking at structures in order ro determine the safety margin present in structures and the effects of partial failure on the overall structure. The methods have application, for example, in analysing the safety of offshore oil or gas platforms in a variety of weather conditions.

22. Techniques based on Fuzzy Sets and Fuzzy Logic

Purpose: Quantisation of frequency and consequences.

Limitations: Requires experts

Advantages: Quantifies qualitative opinion.

Description of technique: These methods operate on "linguistic variables" in order to produce a quantitative output from a qualitative input. They might be useful in cases where the only data available is subjective judgement from people not able to put it into quantitative terms.

23. DEFI method

Purpose: Hazard Identification

Limitations: More a way of assessing the reliability of hardware rather than predicting hazards. Hardware needs to have been constructed to allow the technique to be used.

Description of technique: DEFI is a method which uses the injection of faults into a computerised system to determine the rate of failure to danger.

24. Delphi Technique

Purpose: Frequency prediction.

Limitations: Requires experts.

Description of technique: This is a technique which formalises the process of obtaining estimates for failure rates, frequencies of hazardous events etc., by expert judgement. A large circle of experts are questioned several times, each time the estimates and comments obtained previously are summarised and fed back. This continues until agreement is reached. It has been used in the US nuclear industry to estimate failure rates of various components. An essential feature is that the values suggested by one expert are presented anonymously to the other participants. Comments are also anonomised. It is important that participants only comment and provide estimates in areas where they have experience themselves and this should be made clear at the outset.

25. Method Organised Systematic Analysis of Risks (MOSAR)

Purpose: Hazard Identification, frequency & consequence prediction.

Limitations: Time-consuming.

Advantages: Systematic risk analysis technique.

Description of technique: This is a systematic approach which uses a series of steps to look at the safety of a system. The system is seen as a series of interacting subsystems. A number of tables are filled in by the team carrying out the analysis.

1) Hazard identification
2) Adequacy of prevention
3) Interdependency
4) Operating safety study using FMEA or HAZOP
5) Logic trees
6) Severity table
7) Linking of severity with protection objectives
8) Technological barriers (no human intervention)
9) Utilisation barriers (with human intervention)
10) Acceptability table for residual risks

26. Goal Oriented Failure Analysis (GOFA)

Purpose: Hazard Identification

Limitations: Time-consuming. Difficult to learn. Scope of application is limited to the failure goals considered.

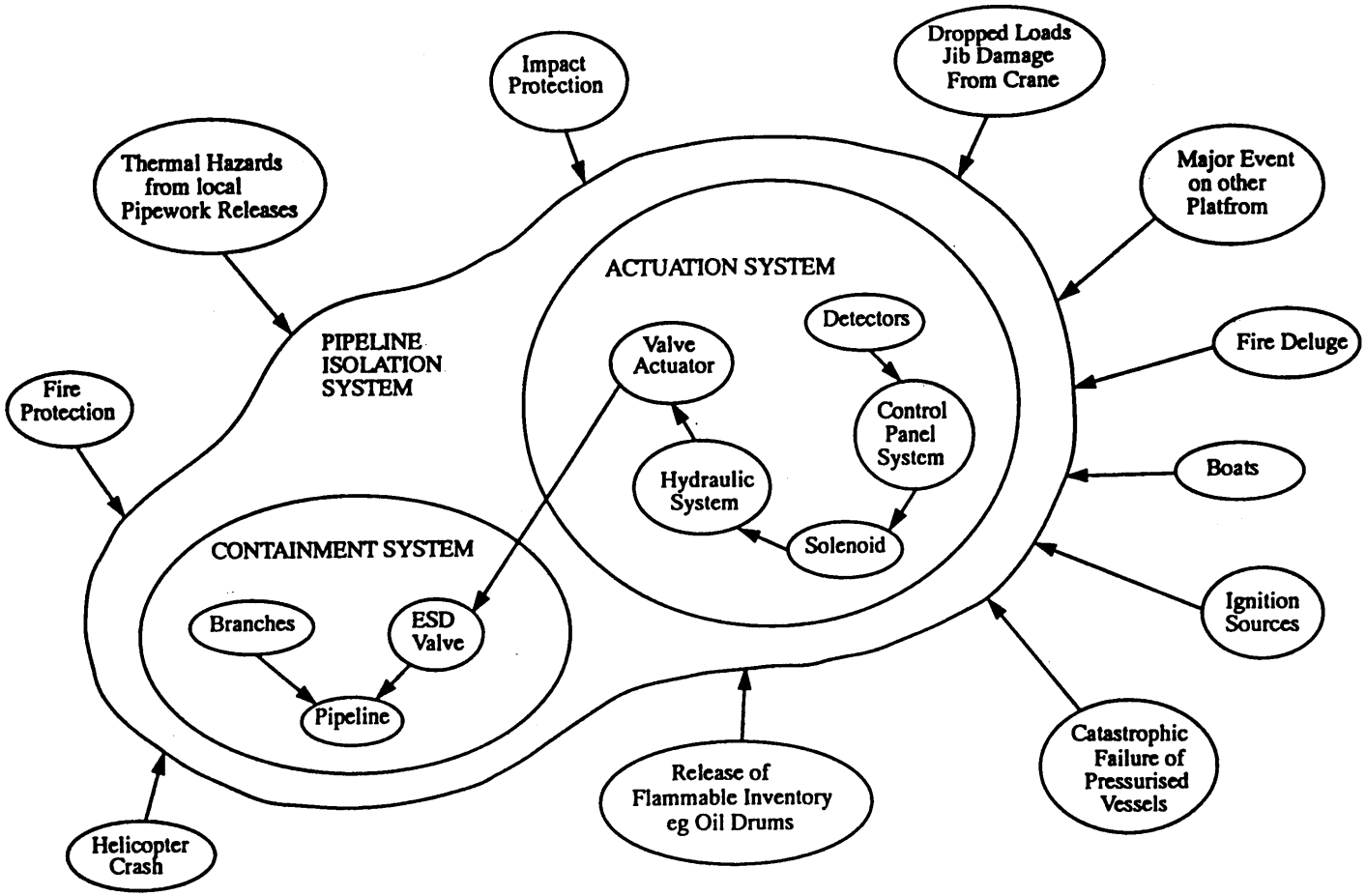
Advantages: Provides a practical approach to identifying the factors which can lead to the realisation of a hazard.

Description of technique: GOFA uses a systems analysis approach and develops a systems diagram for the hazard identification process. GOFA is a top-down technique (i.e. focused on a particular top event) which is intended to be a hybrid of FMEA and fault-tree analysis.

The systems diagram is created by a team for a specific failure goal (e. g. emergency isolation system fails to operate during an emergency).

The steps in the process are:

1) Define the failure goal.
2) Draw up and agree the systems diagram.
3) Determine the fault modes for each component in each subsystem of the systems diagram, using check-lists for support.
4) Choose a component for detailed study.
5) Choose a fault mode for this component.
6) Identify failure mechanisms for the chosen fault mode.
7) Choose a failure mechanism.
8) Identify the failure causes for this failure mechanism. These may be external to the systems diagram or internal if caused by other components.
9) Return to step 7 until complete.
10) Return to step 5 until complete.
11) Return to step 4 until complete.


Impact Protection
Dropped Loads Jib Damage From Crane
Thermal Hazards from local Pipework Releases
Major Event on other Platfrom
ACTUATION SYSTEM
Detectors
Valve Actuator
Fire Deluge
PIPELINE ISOLATION SYSTEM
Fire Protection
Control Panel System
Hydraulic System
Boats
Solenoid
CONTAINMENT SYSTEM
Branches
ESD Valve
Ignition Sources
Pipeline
Catastrophic Failure of Pressurised Vessels
Release of Flammable Inventory eg Oil Drums
Helicopter Crash

Annex VI

Application of the risk assessment methodology

Introduction

This Annex provides information on how to perform a risk assessment on a piece of equipment or unit operation using the methodology described in this standard. The user should be clear that risk assessment can often be a complex process requiring specific expertise and it is unlikely that someone without previous experience will be able to carry out a satisfactory risk assessment solely by following this standard.
Examples are provided which describe how the risk assessment methodology has been applied to the following systems:

A pneumatic powder transfer system
A paint spray booth
Oil seed extraction unit
Spray Dryer for Milk
Protective system – An explosion venting door
Exhaust System of Gas Engine

The risk assessments described are purely illustrative and should not be used as a complete risk assessment for an actual system without further consideration. In addition it should be recognised that this methodology has been designed to assess the risks relating to explosions which can arise in the use of equipment. Additional risk assessments will be necessary to determine possible risks relating to other hazards, for example protection of operators etc.

Use of the methodology

As described in Section 5, a risk assessment should be carried out using a series of logical steps following the definition of the intended use of the equipment or unit operation. Where a complex system is being assessed, it is often useful to divide the system into individual items or groups of items that perform discrete operations, however in such cases extreme care must be taken to ensure that any interrelationship between the risks for each item is fully considered.

Determination of intended use

The correct definition of intended use is critical to performing a successful risk assessment as it provides boundaries within which hazards need to be identified and the possible risks assessed.

Description of the system

This should include a general description of the system, its means of operation to achieve the desired function.

Equipment characteristics

The system should be described in sufficient detail such that any possible ignition sources can be identified. The description should include where appropriate, sizes, throughput, material of construction etc.

Product characteristics

The flammability and explosibility characteristics of the products being handled should be listed.

Functional / State Analysis

The Functional / State analysis described in Section 5.1 can be used where there are uncertainties in how and where a piece of equipment will be used. It is important that the definition of intended use clearly specifies the nature and type of explosive atmosphere which may be present and considers the state of the equipment not only during normal operation but also during start-up and shut-down. During the course of a risk assessment procedure it is often found that the intended use has to be changed. This occurs particularly with respect to the nature of the explosive atmosphere in which the equipment is to be used.

Hazard Identification

Once the intended use of the equipment has been initially defined, the process of hazard identification can be carried out. During this step all possible hazards which may occur must be identified. The aim is to determine whether the equipment or unit operation can present a potential ignition source and to identify whether a potentially explosive atmosphere is present. The evaluation usually starts with the consideration of the equipment in normal operation and is then extended to consider expected malfunctions and rare malfunctions depending on the intended final classification of the equipment i.e. the equipment category (see Section 0). An assessment has to be made of the probability that the ignition source will occur and its effectiveness in igniting the explosive atmosphere, this requires detailed information on the flammability and explosive characteristics of the explosive atmospheres. The results of this analysis must be recorded using the form in Section 5.2.

Risk Estimation

Once all the hazards have been identified, an estimate of the severity of the possible harm which can arise and the probability of the occurrence of each hazard has to be made in order to rank the risks. The severity is ranked in four levels ranging from ’catastrophic’ to ‘negligible’ while the probability of an event occurring is expressed in five stages from frequent to improbable. A qualitative estimation of the resulting risk level is then made using the matrix given in Section 5.3. This results in four risk levels ranging from ‘A’ representing a high risk level to ‘D’ a low risk level.

Risk Evaluation

At this stage of the procedure a table listing all possible hazards which may arise together with a ranking of the risk level for each hazard will be available. This enables a decision to be made as to whether further action is required to reduce the risk to an acceptable level (see Section 5.4). Where the risk estimation results in a risk level of A, the risk is so high as to be intolerable and additional risk reduction

measures are required. Similarly a risk level of D can be considered to be acceptable and no further risk reduction is required. Risk levels B and C are intermediate levels and will normally require some form of risk reduction measures to make the risk acceptable. However, the degree of these measures will be smaller and in the case of a risk level C, organisational risk reduction measures will often be sufficient.

Risk Reduction Option Analysis

Once the risk has been estimated and evaluated the risk reduction option analysis leads to the final decision as to whether or not the solution found reduces the risk to an acceptable level. It is necessary to deal with residual risks after all measures have been taken to reduce the probability and consequence of a specific hazardous event. The residual risks are those against which risk reduction by design and safeguarding techniques are not, or not totally, effective. Residual risks must be documented and included in the instructions for use of the equipment. If all the risks are classified as acceptable then no Risk Reduction is required and the Risk Assessment is complete.

Iteration of the risk assessment procedure

When the risk reduction option analysis shows that risks remain which are unacceptable then the risk assessment must be repeated. This should be carried out in an iterative manner after amending the safety concept or the definition of intended use until all risks have been reduced to an acceptable level.

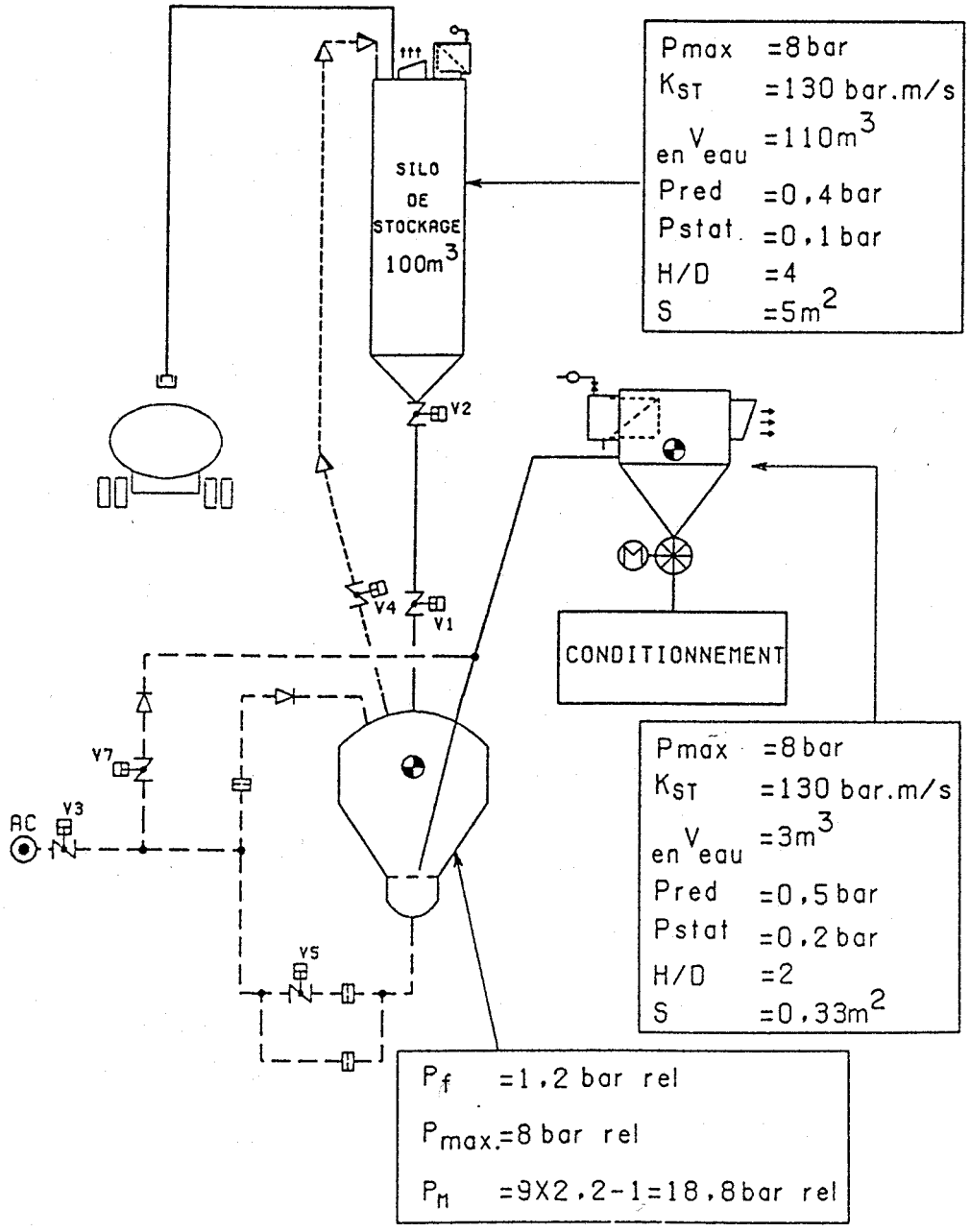
A pneumatic powder transfer system

Determination of intended use

The aim of the system is unloading, pneumatic conveying (PC) under air pressure and storing of granular combustible or uncombustible materials for further use.

Description of the system

The installation for the pneumatic unloading of crystallised sugar from a lorry to a silo is shown in the figure.



Schematic diagram of the installation

Equipment characteristics

The installation consists of different equipment :

- a 30 m3 lorry (out of the scope of the risk assessment) is able to withstand 2 bar overpressure. A compressor is generally installed on the lorry and coupled to the engine,
- pipes and couplings (length : 30 m, diameter : 100 mm) are able to withstand 30 bar,
- the storage silo has a volume of 110 m3, a height/diameter ratio of 4 and is fitted with a vent on the top which has been designed to open at 0.1 barg (Pstat) resulting in a residual pressure in the case of an explosion of 0.4 barg (Pred),
- a blow tank has an operating pressure of 1.2 barg (Pf). As the maximum pressure during an explosion of the product is 8 barg (Pmax), the mechanical resistance of this blow tank is 18,8 barg (Pm). It is fitted with a level control,
- a pneumatic conveying line (length : 100 m, diameter : 100 mm),
- a hopper has a volume of 3 m3, a height/diameter ratio of 2 and is fitted with an explosion vent which has been designed to open at 0.2 barg (Pstat) resulting a reduced explosion pressure in the case of an explosion of 0.5 barg (Pred). The hopper is fitted with a filter and a level control and has a rotary valve in the outlet.

Equipment is made of metallic parts and normally grounded.

Product characteristics

The installation has been designed for use with crystallised sugar with a grain size about 600 µm. However it is known that during operation appreciable amounts of sugar powder can be formed with a particle size of 20 µm. The following explosibility characteristics for the 20 µm dust formed have been measured :

- Kst : 130 bar.m.s-1,
- Pmax : 8 bar,
- Minimum Ignition Energy : 20 mJ.

Functional / State Analysis

A functional state analysis of the system is shown in the figure:

Physical state of the substance		Unit operations		Energies/operating state
		Lorry		
		↓		
crystallised sugar (particle size : 600 to 20 µm)	←	Lorry unloading pneumatic conveying	←	Moist air Maximal pressure = 2 bar Maximum air temperature = 60°C
		↓		
dusty	←	Storage in silo gravity feed		
dusty	←	Filling of the blow tank gravity feed	←	Operation of valves V1 and V2
		↓		
dusty	←	Filling of the hopper gravity feed	←	Operation of valves V3, V5 and V7 No temperature increase Pressure : 1.2 barg
		↓		
dusty	←	Unloading of the hopper		

Functional state analysis of the pneumatic unloading system

Hazard Identification

Potential ignition sources:

Ignition Sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface	No	
Flames and hot gases (including hot particles)	No	
Mechanically generated sparks	Yes	Yes
Electrical apparatus	Yes	Yes
Stray electric currents, cathodic corrosion protection	No	
Static electricity:	Yes	
Corona discharges	Yes	No - MIE dust cloud 20 mJ
Brush discharges	Yes	No - MIE dust cloud 20 mJ
Propagating brush discharges	Yes	Yes
Cone discharges	Yes	No - Size of the equipments too small, granulometry of the product too small, MIE dust cloud 20 mJ
Spark discharges	Yes	Yes
Lightning	Study to be undertaken by the user	
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz	No	
Electromagnetic waves from 3 x 10^{11} Hz to 3 x 10^{15} Hz	No	
Ionizing radiation	No	
Ultrasonics	No	
Adiabatic compression and shock waves	No	
Exothermic reactions, including self-ignition of dusts	No	

Table of Ignition sources

When «'no'» is mentioned in the second column, it means that the specified equipment can not generate this type of ignition source.

	Explosive Atmosphere			Ignition Source			
Ref.	**Type**	**Frequency of occurrence or release**	**Location**	**Type**	**Cause**	**Likelihood**	**Effective-ness of ignition sources**
1	Cloud of explosible sugar dust	Present at the end of loading	Inside the pneumatic pipe	Static electricity sparks	No earthing	During malfunction	High as energy > MIE
2	Cloud of explosible sugar dust	Present at the end of loading	Inside the pneumatic pipe	Mechanical sparks or heating	Introduction of foreign bodies	During rare malfunction	Low as grid at the PC inlet
3	Cloud of explosible sugar dust	Present during filling	Inside the silo	Static electricity sparks	No earthing	During malfunction	High as energy > MIE
4	Cloud of explosible sugar dust	Present during filling	Inside the silo	Mechanical sparks or heating	Introduction of foreign bodies	During rare malfunction	Low as grid at the PC inlet present
5	Cloud of explosible sugar dust	Present during filling	Inside the blow tank	Static electricity sparks	No earthing	During malfunction	High as energy > MIE
6	Cloud of explosible sugar dust	Present during filling	Inside the blow tank	Mechanical sparks or heating	Introduction of foreign bodies	During rare malfunction	High as valves present
7	Cloud of explosible sugar dust	Present during filling	Inside the blow tank	Electric sparks	Level control	During malfunction	High as energy > MIE
8	Cloud of explosible sugar dust	Present during filling	Inside the hopper	Static electricity sparks	No earthing	During malfunction	High as energy > MIE
9	Cloud of explosible sugar dust	Present during filling	Inside the hopper	Mechanical sparks or heating	Introduction of foreign bodies	During rare malfunction	Low as pneumatic conveying
10	Cloud of explosible sugar dust	Present during filling	Inside the hopper	Electric sparks	Level control	During malfunction	High as energy > MIE

Table recording hazards identified

Risk Estimation / Risk evaluation

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5 in the methodology

This first risk estimation does not take into account the preventive and protective measures.

Reference	Frequency	Severity	Risk Level
1	probable	major	A
2	probable	major	A
3	probable	major	A
4	remote	major	B
5	probable	major	A
6	probable	major	A
7	probable	major	A
8	probable	major	A
9	remote	major	B
10	probable	major	A

Table of frequency and severity of events and resulting risk level

Risk Reduction Option Analysis

Preventive and protective measures have to be applied, to reduce the frequency and/or the severity. The following measures are proposed:

procedure of earthing,

grid at the PC inlet,

magnetic detector,

explosion pressure resistant vessel for the pipes and coupling,

vent on the silo,

explosion pressure resistant vessel for the blow tank,

level control for use in dusts explosive atmospheres,

vent on the hopper taking into account the ignition of a jet flame, or a vent with an explosion decoupling system.

Iteration of the risk assessment procedure

After the application of all these preventive and protective measures, a new risk estimation and risk evaluation have been made.

Reference	Frequency	Severity	Risk Level
1	Remote	minor	C
2	Occasional	minor	B
3	Remote	minor	C
4	Remote	minor	C
5	Remote	minor	C
6	Occasional	minor	B
7	Occasional	minor	B
8	Remote	minor	C
9	Remote	minor	C
10	Occasional	minor	B

Table of frequency and severity of events and resulting risk levels after Risk reduction measures

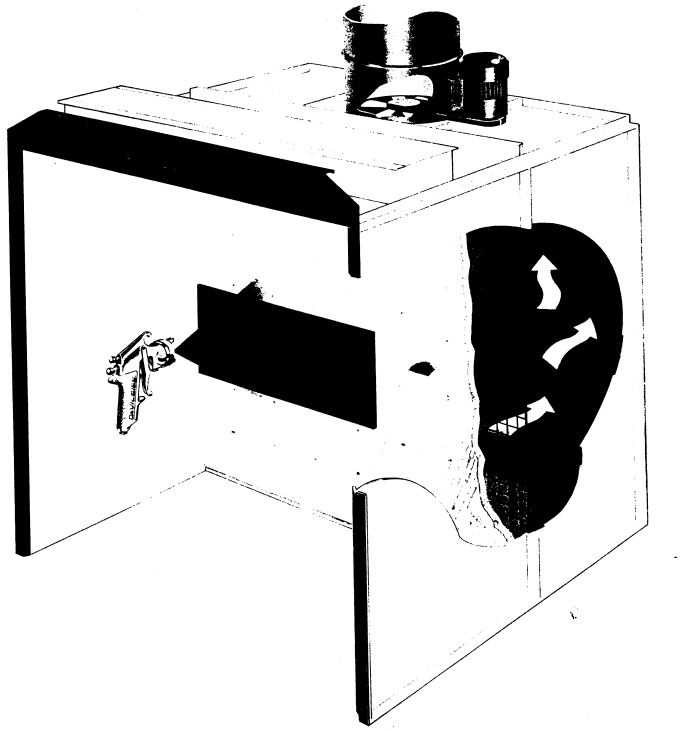
A paint spray booth

Determination of intended use

The application of paints, varnishes, lacquers and other coatings to models and test pieces manufactured in a workshop. The paint-spray booth is used occasionally by one trained operator (or under his supervision). This person is also responsible for general housekeeping, cleaning, replacement of filters etc.

Description of the system

The manually operated paint spray booth is situated inside a busy workshop. It is enclosed on three sides and open fronted to allow easy access. Work pieces can be either hung from a bar or placed on a metal table. Paint contained within a storage can, forming part of the spray gun, is atomised by compressed air supplied by a high pressure flexible hose from a compressor, (outside the scope of the risk assessment), at 4 bar. The booth is ventilated from the rear in order to draw overspray away from the operator and keep the concentration of the volatiles below the lower explosive limit within the booth. The air flows are tested every six months to check that they are within design parameters. Glass fibre filter pads separate the spray area and the ventilation ducting to remove any entrained paint present in the air flow. These can be easily changed after set periods of use. Ducting removes the air out of the back of the booth to an area outside the workshop containing no ignition sources. The operator wears a breathing mask when spraying is performed to minimise occupational health risks associated with the material being sprayed. The most commonly used coating material are water based lacquers, and paints containing volatile flammable solvents are used only occasionally.



Schematic diagram of the installation

Equipment characteristics

The spray gun is manually operated, and is connected to an air line supplying air at 4 bar, and a container holding up to $1x10^{-3}m^3$ of paint. The ventilation with the

entrained overspray passes through a fire retardant glass fibre filter (which captures the overspray and is easily changeable). The air flow then passes through ducting connected to the back of the booth to an area outside the building. The fan is situated inside the ducting, and is belt fed by an electric motor, which is located outside the ducting. Illumination is provided by a light, which is sealed from the atmosphere in the booth behind a glass plate. The booth is constructed to withstand a fire for up to half an hour. The dimensions of the booth are a height of 2.1m, a width of 2.5m, and a depth of 2m of which 1m is in front of the filter, a volumetric air throughput of 3.55m^3/s is achieved by the booth.

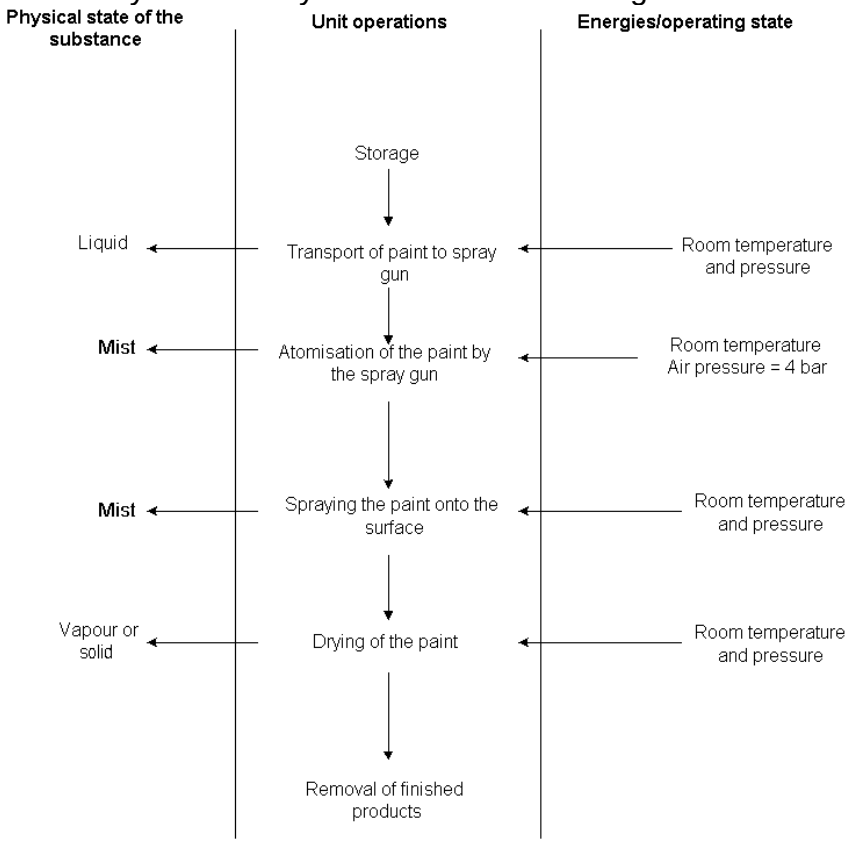
Product characteristics

The characteristics of the paint used in the assessment are:-

Boiling point	138°C
Flash point	35°C
Auto ignition temperature	490°C
Explosive limits	1-6.6% Vol
Volatile content	40%

Functional / State Analysis

A functional state analysis of the system is shown in the figure:



Functional state analysis of the paint spray booth

Hazard Identification

Ignition Sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface	Yes	Yes – though will depend on the temperature and size of the surface
Flames and hot gases (including hot particles)	Yes	Yes – can provide sufficient energy
Mechanically generated sparks	Yes	Yes – can provide sufficient energy
Electrical apparatus	Yes	Yes – can provide sufficient energy
Stray electric currents, cathodic corrosion protection	No	
Static electricity:		
Corona discharges	Yes	No – insufficient energy
Brush discharges	Yes	Yes –will only provide sufficient energy for a vapour explosion
Propagating brush discharges	No	
Cone discharges	No	
Spark discharges	Yes	Yes – can provide sufficient energy
Lightning	No	
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz	No	
Electromagnetic waves from 3 x 10^{11} Hz to 3 x 10^{15} Hz	No	
Ionizing radiation	No	
Ultrasonics	No	
Adiabatic compression and shock waves	No	
Exothermic reactions, including self-ignition of dusts	No	

Table of Ignition sources

	Explosive Atmosphere			Ignition Source			
Ref.	**Type**	**Frequency of occurrence or release**	**Location**	**Type**	**Cause**	**Likelihood**	**Effective-ness of ignition sources**
1	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Static electricity	Static producing clothing	Likely to occur during malfunction	High
2	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Mechanical sparks	Additional work being performed in the booth	Likely to occur during rare malfunction	High
3	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Mechanical sparks	The fan striking the ducting	Likely to occur during malfunction	High
4	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Electrical sparks	Additional work being performed in the booth	Likely to occur during rare malfunction	High
5	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Hot surface	Additional work being performed in the booth	Likely to occur during rare malfunction	High
6	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Hot surface	Glass breaks allowing access to the light	Likely to occur during rare malfunction	Medium
7	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Inside the spray booth	Naked flame	Smoking in the booth	Likely to occur during rare malfunction	High
8	Volatile vapour	Malfunction (during spillage or drying, and insufficient ventilation)	Outside the spray booth	Various	Ignition sources outside the booth	Various	Various
9	Volatile mist	During normal operation	Inside the spray gun	Static electricity	No earthing	Likely to occur during malfunction	Low
10	Volatile mist	During normal operation (only near the nozzle of the spray gun)	Inside the spray booth	Static electricity	Electrostatic charging of the paint spray	Likely to occur during malfunction	Low
11	Volatile mist	During normal operation (only near the nozzle of the spray gun)	Inside the spray booth	Mechanical sparks	Additional work being performed in the booth	Likely to occur during rare malfunction	High
12	Volatile mist	During normal operation (only near the nozzle of	Inside the spray booth	Electrical sparks	Additional work being performed in	Likely to occur during rare	High

		the spray gun)			the booth	malfunction	
13	Volatile mist	During normal operation (only near the nozzle of the spray gun)	Inside the spray booth	Hot surface	Additional work being performed in the booth	Likely to occur during rare malfunction	High
14	Volatile mist	During normal operation (only near the nozzle of the spray gun)	Inside the spray booth	Naked flame	Smoking in the booth	Likely to occur during rare malfunction	High

Table recording hazards identified

Risk Estimation / Risk evaluation

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5, in the methodology

This first risk estimation does not take into account the preventive and protective measures.

Reference	Frequency	Severity	Risk Level
1	Occasional	Minor	B
2	Remote	Minor	C
3	Remote	Minor	C
4	Remote	Minor	C
5	Remote	Minor	C
6	Remote	Minor	C
7	Remote	Minor	C
8	To be considered by user		?
9	Remote	Minor	C
10	Remote	Minor	C
11	Remote	Minor	C
12	Remote	Minor	C
13	Remote	Minor	C
14	Remote	Minor	C

Table of frequency and severity of events and resulting risk level

Risk Reduction Option Analysis

Preventive and protective measures have to be applied, to reduce the frequency and/or the severity. The following measures are proposed:

Grounding of all equipment.

Good house keeping:-

Allow no naked flames in or near the spray booth.

Minimise the build-up of paint layering, due to over spray, by regular cleaning.

Maintain all equipment in good condition.

Use equipment that will not produce sparks when performing maintenance.

Check for any leaks in the extraction ducting.

Continuous measurement of the concentration of volatiles in the air.

Design the ventilation system to keep the concentration of the volatiles in the air well below the lower explosion limit.

If the air flow stops, or the concentration of volatiles in the air becomes too high, then a warning should be given, or the spray gun could be automatically cut off.

Construct the booth from non-flammable material.

Provide easy exit points for operators.

Wear clothing that will not produce static electricity.

Provide lighting that cannot be an ignition source.

Only permit paint spraying in the booth, no additional work.

Install sprinklers.

Install the booth as far from external ignition sources as possible.

Use water based paints and lacquers where applicable.

Provide material able to absorb any spillages.

Iteration of the risk assessment procedure

After the application of these preventive and protective measures, a new risk estimation and risk evaluation have been made.

Reference	Frequency	Severity	Risk Level
1	Ignition source has been eliminated		
2	Ignition source has been eliminated		
3	Improbable	Minor	C
4	Ignition source has been eliminated		
5	Ignition source has been eliminated		
6	Improbable	Minor	C
7	Ignition source has been eliminated		
8	To be considered by user		?
9	Improbable	Minor	C
10	Improbable	Minor	C
11	Ignition source has been eliminated		
12	Ignition source has been eliminated		
13	Ignition source has been eliminated		
14	Ignition source has been eliminated		

Table of frequency and severity of events and resulting risk levels after Risk reduction measures

Oil seed extraction unit

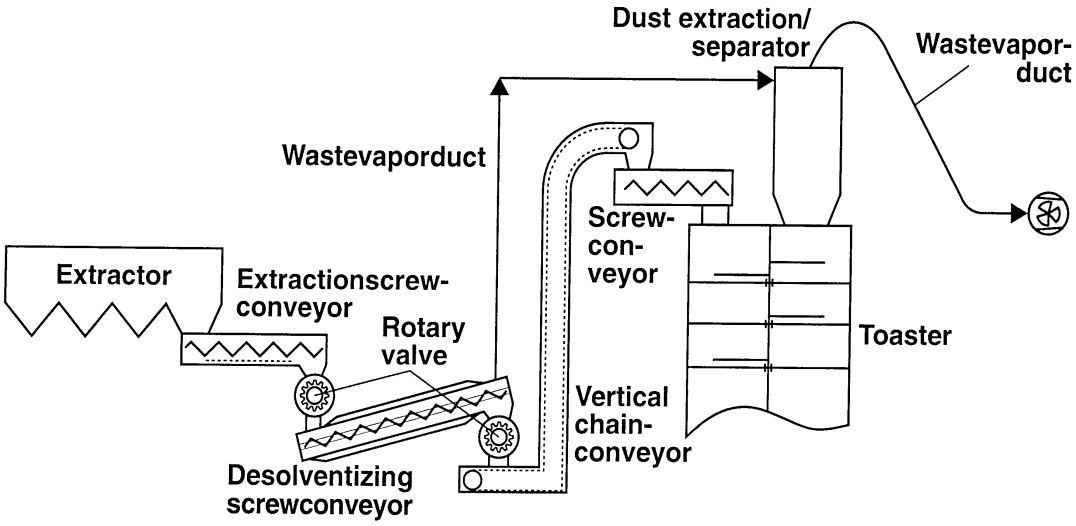
Determination of intended use

Extraction is the widely used industrial process to gain special oil products of high quality (crude oils, lecithin etc.).
There are several processing steps before starting the extraction process itself to prepare the seed, for example, storage, cleaning, dehulling, heating, crushing, pressing. To obtain good extraction results, the preceding preparation of the seeds and the conditions used are important.
The extraction process is operated by using hexane as a solvent. Due to its characteristics hexane is known as a flammable substance which can form explosive hexane/air mixtures taking into account miscella as well. Using hexane as a solvent is recognized as both an economic way of extracting and also hazardous from the point of view of explosive atmospheres occurring.
This application example deals with oil seed extraction unit using hexane covering the process steps on extracting, desolventizing and toasting.

Description of the system

Extraction is the key operating step in the process considered. Natural products (oilseed) are processed and thus involve continually changing compositions.
Larger oilseed extraction units normally process 2500 t/d. For that they need as energy about 250 kg steam, 12 kWh electrical energy, 18m^3 cooling energy between 5 and 10°C and 1,5 kg solvent per 1000 kg oil seed. However, these amounts of energy depend on the natural composition of oil seed being processed and vary from case by case.
In normal operation the atmosphere is not explosive. The oxygen concentration that is occurs in the gas phase of an extractor in normal operation iis insufficient to form an explosive atmosphere, provided that there is an equilibrium-vapor pressure and a homogenous gas-concentration distribution. This means that the so-called critical oxygen concentration is not attained in normal operation.

Schematic diagram of the installation



After seed preparation the extraction is performed in a continuous process. The meal is carried by chambers or boxes inside the closed extractor. The chambers are moved with sieves percolated by hexane heated up to 60° C in opposite directions. Having percolated though the meal, the hexane is collected again and pumped into a next chamber. The meal and the miscella leavie the extractor in different ways.
The miscella then is treated to gain the oil, whereas the meal needs to be desolventized from hexane. Meal conveyors connect the extractor with the toaster and thus allow ingress of air, propagation of explosive atmospheres, ignition sources transmission and the spread of fires and explosions. The desolventizing is mainly performed in the toaster which consists of different levels to treat the meal with the energy required at the different stages.

Equipment characteristics	
Extractor	• consists of separated chambers or boxes; • as a rule, temperatures range from 45 to 63° C in normal operation; • designed to be gas – and liquid proof;
meal conveyor	• mechanical system where many ignition sources may occur; • chain-conveyor/screw conveyor in connection with rotary valve; • conducts meal, liquid miscella and hexane/air mixtures in normal operation; • provides pre-desolventizing;
toaster	• meal is treated on different levels; • on the upper level steam is injected directly, the other levels are operating powered steam to get meal on approximately 100° C; • considered to be the most critical equipment in the extraction process;

Product characteristics Combustion Properties / Explosion Characteristics of hexane / miscella
• both fluids are easily flammable; • they can form explosive hexane/air mixtures starting at –26° C • hexane/air mixtures are heavier than air and accumulate in holes, canals, shafts and other deepenings; • fatty hexane/air mixtures thin out in air through convection and diffusion and become explosive mixtures; • the minimum ignition energy of 2.16 mJ of an optimum explosive hexane/air mixture is very low; • also the ignition temperature is very low at 223° C; • hexane cannot be mixed with water and its density is less than that of water. Thus hexane fires cannot be extinguished with water; • there exists related risks due to the combustibility of oilseed, flakes, white oil used for hexane absorption, oil-drenched isolation material and others.

Functional / State Analysis

A functional state analysis of the system is shown in the figure:

Physical state of the substance	Unit operations	Energies/operating state
	prepared seed ↓	
solid meal ←	moving of meal by extractor boxes ←	mechanical energy
	↓	
liquid miscella and moist meal ←	percolating of meal with hexane ←	temperature 60 °C negative pressure
	↓	
hexane moist meal, liquid miscella and hexane air mixtures ←	conveying of hexane treated meal ←	room temperature cooling energy
	↓	
solid meal and hexane in the form of vapor ←	desolventizing the meal from hexane ←	injected steam approximately 100 °C
	↓	
	desolventized meal	

Functional state analysis of the oil seed extraction system

Hazard Identification

The main risk originates from hexane and the miscella due to their combustion properties and explosion characteristics. The risk of fire is very high according to the wide range of potential ignition sources, and these might be also capable of igniting explosive atmospheres.

The relevant ignition sources and their significance to trigger fires and/or explosions at air impact are summarized in the following table.

Miscella, liquid hexane and hexane vapors can escape into working areas, if the following conditions are provided in normal operation, incidents or repair works:

- the extractor and input devices are overloaded where tightness or exhaustion is insufficient at the same time;
- the extractor is opened or de-flanged above the miscella level;
- leakage above the miscella level and failure of the operational negative pressure;
- opening of the emptied extractor without any internal exhaust;
- when discharging residual quantities of moisted meal from the open extractor;
- miscella is relieved into open receiving containers;
- circulation pumps are leaking;
- a sampling valve is opened and not properly tightened;
- glassy miscella or hexane pipes, sight glasses or glass panes break;
- a flange connection in a miscella or hexane pipe is leaking.
- Explosions and/or open fire which have developed in an oil seed extraction unit can spread within aggregates as much as an explosive atmosphere can develop

from air impact as long as the spread is not limited by a protective system. To that end a risky situation could be shifted from one to another unit part and endager the system.

Furthermore, explosion and / or open fires which have developed or spread into working areas will most likely cause further events that are uncontrollable and will affect the entire plant.

Ignition Sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface	Yes	Yes-due to hot walls and frictions
Flames and hot gases (including hot particles)	Yes	Yes-can provide sufficient energy
Mechanically generated sparks	Yes	Yes-because of transport means
Electrical apparatus	Yes	Yes-in case of incidents etc.
Stray electric currents, cathodic corrosion protection	No	
Static electricity:		
Corona discharges	Yes	No- insufficient energy
Brush discharges	Yes	No- insufficient energy
Propagating brush discharges	No	
Cone discharges	No	
Spark discharges	Yes	Yes-can provide sufficient energy
Lightning	No	
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz	No	
Electromagnetic waves from 3 x 10^{11} Hz to 3 x 10^{15} Hz	No	
Ionizing radiation	No	
Ultrasonics	No	
Adiabatic compression and shock waves	No	
Exothermic reactions, including self-ignition of dusts	Yes	Yes-can provide sufficient energy

Table of ignition sources

	Explosive Atmosphere			Ignition Source			
Ref.	**Type**	**Frequency of occurrence or release**	**Location**	**Type**	**Cause**	**Likelihood**	**Effectiveness**
1	Explosive hexane/air mixtures	not likely to occur in normal operation but in cases where air is sucked in (filling, discharge)	extractor input	mechanically generated sparks	Extractor is overloaded	Not likely to occur in normal operation, but during malfunction, blockages etc.	high due to energy level involved
2	Explosive hexane/air mixtures	not likely to occur in normal operation but in cases where air is sucked in (filling, discharge)	inside extractor	static electricity	insulated metal parts	not likely to occur in normal operation	high or low depending on the way of discharging
3	Explosive hexane/air mixtures	not likely to occur in normal operation but in cases where air is sucked in (filling, discharge)	inside extractor	hot surface	overheating of extractor walls	not likely to occur in normal operation but in case of incidence	high relating to self-ignition processes
4	Explosive hexane/air mixtures	not likely to occur in normal operation but due to air impact	inside meal conveyor	hot particles	smouldering products	not likely to occur in normal operation but during transmission	high depending on energy level involved
5	Explosive hexane/air mixtures	not likely to occur in normal operation	inside meal conveyor	mechanically generated sparks	rubbing of driving elements on housing	not likely to occur in normal operation but during malfunction	low due to slow conveyor speed
6	Hexane in the form of vapor	not likely to occur in normal operation due to low oxygen – concentration	inside toaster	hot surface	overheated toaster walls	not likely to occur in normal operation ; temperature monitoring not properly working	high, as surface temperature > ignition temperature

Table recording hazards identified

Risk assessment technique	Factors/relationships which could influence the risk
Hazard and Operability Study (HAZOP) applicable to complex items of process plant / What – If? Analysis	Explosive hexane / air mixtures develop: during cooling, recovery and opening of the unit during the filling of the empty extractor with hexane / especially distinct and long-term if the hexane is cold in case of incidents within the unit, if air can get into unit because of leaks, breakdown or maloperation in case of drip-leakage during sampling
Task Analysis / Maintenance Analysis	Explosive hexane / air mixtures develop: if hexane and/or miscella is drained into open receivers, i. e. not into a closed stop-system from the extractor, nor drained from destillation apparatus, condensators and hexane / water separators if meal which is still hexane-moisted is discharged from the desolventizer hexane-, miscella– or meal-conducting apparatus is opened and emptied
Check List for Ignition Sources	Relevant ignition sources for fire and explosion in working areas and product-conducting unit parts: self-ignition fires in oil-drenched isolations of hot-product-pipelines; rubbing friction; overheated bearings; electrostatic discharges; defect electrical apparatus

Application of risk assessment techniques

Risk Estimation / Risk Evaluation

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5 of the methodology.

This first risk estimation does not take into account the preventive and protective measures.

Reference	Frequency	Severity	Risk Level
1	occasional	major	B
2	remote	major	B
3	remote	major	B
4	occasional	major	B
5	occasional	major	B
6	remote	major	B

Table of frequency and severity of events and resulting risk levels

Risk Reduction Option Analysis

Contributions to reduce the risk should consider the following measures:
design measures for the entire oil seed extraction unit, e. g.

- the unit consists of inflammable materials or those which are hardly flammable;
- is equipped with an emergency-power supply,
- especially the MSR-plant, cooling and ventilation system;
- is gas – and liquid proof;
- is equipped with pressure switches to control the permissible pressure range and deviations;
- provides valves or means to plug in blank-off flanges between hexane-conducting unit parts

technical measures for individual unit parts, e. g.

- The extractor posses an automatic overpressure compensation as well as warning devices. Meal discharge is controlled by a level measuring device. Gas-shuttle pipes are supplied with explosion barriers. Valves or taps can only be opened with special tools. The impact of air together with the flake steam can be limited through a stuffing screw or gas-proof rotary valve.
- The meal conveyor has a speed less than 1,0 m/s. The driving force is limited and controlled by hardware. There may further be a redundant control to keep temperature (60° C) in the screw conveyors.
  Before the apparatus is opened to remove adhesions or cloggings it must be separated gas-proof from the plant directly at the product entry and discharge so that hexane can not reach working at the same time.
- The toaster is equipped with an automatic safety device to control temperature, pressure and liquid levels.
- The apparatus is regularly controlled, especially prior to being opened so that any long-term meal adhesions are detected in time.
- The toaster is to be equipped with appropriate fire extinguishing devices.

In general, the above-mentioned risk reduction options have to be applied all of them to achieve acceptable risk levels.

In addition, further safety measures have to be taken for special operational conditions like start-up, shut-down, opening, discharging, repairs including appropriate instructions thereof.

Iteration of the risk assessment procedure

After the application of these preventive and protective measures, a new risk estimation and risk evaluation have been made.

Reference	Frequency	Severity	Risk Level
1	remote	minor	C
2	improbable	minor	C
3	remote	minor	C
4	remote	minor	C
5	remote	minor	C
6	remote	minor	C

Table of frequency and severity of events and resulting risk levels after Risk reduction measures

Spray Dryer for Milk

Determination of intended use

Spray Drying is the widely used industrial process involving particle formation and drying. It is suited for the continuous production of dry solids in either powder, granulate or agglomerate form from liquid feedstocks such as emulsions and suspension.
Spray Drying involves the atomization of the liquid feedstock into a spray of droplets and contacting the droplets with hot air in a drying chamber.
The sprays are produced by either rotary or nozzle atomizers. All systems can be provided with post-treatment equipment, for example: fluid bed dryer/cooler, agglomerator, de-duster and conveyor.

Description of the system

Atomization plays a central role in the process. The formation of sprays having the required droplet size distribution is vital to both the operation and the explosive atmospheres in the form of a cloud of combustible dust occurring.

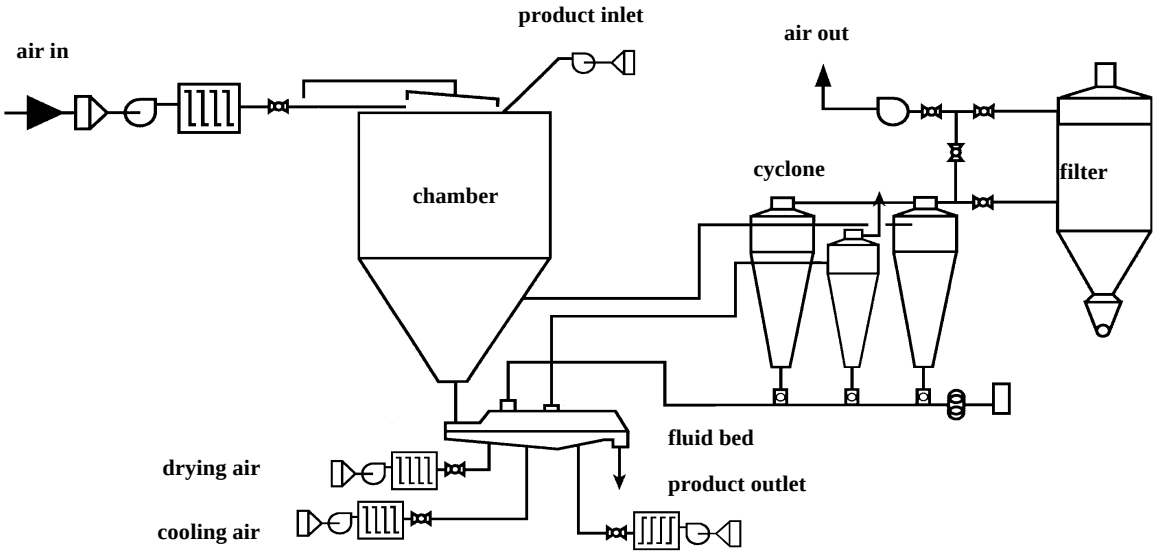
The selection of rotary atomizer or nozzle type depends on the feed properties and powder specification. The contact between spray droplets and drying air controls the evaporation rate and product temperatures in the dryer. There are three basic modes of contact:

- Co-current:
  Drying air and particles move through the drying chamber in the same direction. Product temperatures on discharge from the dryer are lower than the exhaust air temperature.
- Counter-current:
  Drying air and particles move through the drying chamber in opposite directions. The temperature of the powder leaving the dryer is usually higher than the exhaust air temperature.
- Mixed-flow:
  Particle movement through the drying chamber experiences both co-current and counter-current phases.

In Milk Powder Spray Dryers a co-current airflow pattern is almost exclusively used. The other modes are used mainly with products having high heat stability.
Exhaust air is subject to a cleaning process in cyclones, bag filters, and occasionally wet scrubbers.

The remaining part of this application example deals with a specific Milk Powder Spray Dryer. All equipment and its components have stainless steel housing or are mounted in a stainless steel casing.

Schematic diagram of the installation



The spray dryer transforms the feed, which is milk concentrate into a powder in one continuous operation.

The feed is pumped to the rotary atomizer machine located in the ceiling air disperser at the centre of the chamber roof. The atomizer produces a spray of droplets by passing the feed through a vaned wheel rotating at high speed. The spray of droplets produced by the atomizer is immediately contacted by and mixed with hot drying air entering the drying chamber in a flow pattern created by the ceiling air disperser.

Each droplet in the spray is turned into a solid particle by drying while suspended in the drying air. A high rate of collisions between particles produces agglomerates that form the powder product. Product separation from the drying air takes mainly place at the base of the drying chamber.

The powder is discharged continuously from the drying chamber. The powder passes into a fluid bed where final drying and cooling of the powder takes place. Small amounts of fines pass with the exhaust air from the drying chamber and the fluid bed to be collected in cyclones. A bag filter completes the cleaning of the exhaust air leaving the spray dryer.

The fine fraction of the powder collected by the cyclones is recycled to the drying system to participate in the agglomeration process. The re-entry point is in the drying section of the fluid bed. The fine powder is conveyed in a pneumatic conveying system.

Equipment characteristics

The feed pump is an eccentric helical pump of rotatory type working according to the positive displacement principle.
The rotary atomizer is a Niro proprietary design rated at 24 kW.
The heating system is indirect steam, 5000 kW, automatic control, max 220° C.
The air blower of the pneumatic conveying system is of the Rootes type.
The drying chamber has the following geometry:
Diameter 7.0 m

Cylindrical height 6.3 m
Total height 15.0 m
Cone 60°
Pneumatic hammer system
The milk spray dryer is designed to operate at the following temperature levels:
Inlet air temperature 200° C
Outlet air temperature 90° C
Feed Temperature 40° C
The exhaust system comprise the following components:
Main Cyclones 2 off Diameter 2.0 m
FB cyclone 1 off Diameter 1.4 m
Bag filter
Exhaust fan

Product characteristics

Combustion Properties and Explosion Characteristics of milk powder	
Particle size (median)	80-100 μm
Explosibility (modified Hartmann apparatus < 63 μm)	Yes
Max explosion overpressure (p_{max})	6 to 7 bar
max rate of pressure rise (K_{ST}-value)	80-130 bar · m · s^{-1}
Minimum ignition energy (MIE)	> 50 mJ
Minimum ignition temperature of a dust cloud	450 to 600° C
Lower explosion limit (LEL)	60 to 125 g · m^{-3}
Glowing (layer ignition temperature)	320 to 350° C

Note: This table contains approximate values. Properties may vary from product to product due to the amount of fat, glucose etc.

Functional / State Analysis

A functional state analysis of the milk spray drying system is shown in the figure:

Physical state of the substance	Unit operations	Energies/operating state
	Storage of liquid feed	
	↓	
Liquid ←	Pumping of liquid to atomizer ←	Temperature 40C Liquid pressure < 10 bar
	↓	
Cloud of droplets ←	Atomization of liquid by atomizer ←	Temperature ~ 40 C Atmospheric pressure
	↓	
Vapour and powder particles ←	Drying of droplets ←	Temperature < 90 C Atmospheric pressure
	↓	
Vapour and powder particles ←	Drying and cooling of Powder particles in fluid bed ←	Temperature < 90 C Atmospheric pressure
	↓	
Powder particles ←	Pneumatic conveying of powder particles ←	Temperature < 90 C Atmospheric pressure
	↓	
Powder ←	Discharge of powder ←	Temperature < 50 C Atmospheric pressure
	↓	
	Storage of powder	

Functional state analysis of the spray drying system

Hazard Identification

Taking into account both units and components considered safety-relevant as well as combustion properties and explosion characteristics of milk powder, the occurrence of an explosive atmosphere must be anticipated. Further, milk powder may under certain circumstances be capable of undergoing exothermic processes leading to self-ignition of fires.

An atmosphere in the form of a cloud of combustible milk powder in air is present continuously. The concentration of milk powder is, however, usually under the lower explosion limit (LEL). It is likely to occur occasionally in normal operation.

In case of dust, it is difficult to achieve the objective of avoiding explosive atmospheres by limiting the concentration since dust-air mixtures are usually inhomogeneous. Calculation of dust-concentration from the total amount of dust and the total equipment leads to erroneous results. Local dust concentrations can be present that differs greatly from the globally calculated ones.

Deposits of milk powder may under certain circumstances be compacted in layers of more than 60 mm thickness. When such layers are subject to temperatures over 80-90 °C for a period of more than 20 hours an exothermic reaction may cause smoldering. A smoldering lump can ignite a fire, which in turn can ignite an explosion
High temperatures on drying air inlet devices or atomizer systems without adequate cooling can also lead to the initiation of smouldering and / or burning.
Consequently the prevention of fire sources is getting highest priority. Of course, this includes the avoidance of any ignition sources that might be also capable of igniting explosive atmospheres.
Operational limits are determined by the combustion properties and explosion characteristics of milk powder in combination with a safety margin.
The ”Hazard Identification” is summarized in the following tables:
Table of Ignition sources
Table recording hazards identified

Ignition Sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface	Yes	Yes – can provide sufficient energy
Flames and hot gases (including hot particles)	No	
Mechanically generated sparks	Yes	Yes – can provide sufficient energy
Electrical apparatus	Yes	Yes – can provide sufficient energy
Stray electric currents, cathodic corrosion protection	No	
Static electricity:		
Corona discharges	Yes	No – insufficient energy
Brush discharges	Yes	No – insufficient energy
Propagating brush discharges	No	
Cone discharges	No	
Spark discharges	Yes	Yes – can provide sufficient energy
Lightning	No	
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz	No	
Electromagnetic waves from 3 x 10^{11} Hz to 3 x 10^{15} Hz	No	
Ionizing radiation	No	
Ultrasonics	No	
Adiabatic compression and shock waves	No	
Exothermic reactions, including self-ignition of dusts	Yes	Yes – can provide sufficient energy

Table of Ignition sources

	Explosive Atmosphere			Ignition Source			
Ref.	**Type**	**Frequency of occurrence or release**	**Location**	**Type**	**Cause**	**Likelihood**	**Effective-ness of ignition sources**
1	Cloud of Combust-ible dust	Present in normal operation	Inside chamber cone	Self-ignition	Deposits due to blockage problems	Not likely to occur in normal operation, but, if it does occur, will persist for a long period	High with respect to release of fire
2	Cloud of Combust-ible dust	Present in normal operation	Below chamber roof	Hot surfaces	Deposits due to overload of atomizer	Not likely to occur in normal operation	High due to enhance-ment of self-ignition process
3	Cloud of Combust-ible dust	Present in normal operation	Below chamber roof	Friction sparks	During malfunction of atomizer	Not likely to occur in normal operation	High with respect to release of fire
4	Cloud of Combust-ible dust	Present in normal operation	Inside chamber	Electrical apparatus	During malfunction or short-circuit of measuring and control equipment	Present continuously or for long periods. Frequently during malfunction or short-circuit of control equipment	High, depending on energy levels involved, i.e. lamps
5	Cloud of Combust-ible dust	Present in normal operation	Connecting parts between units and components considered safety relevant	Electro-static discharge	Insulated metal parts due to wearing out or bad maintenance	Not likely to occur in normal operation, but, if it does occur, will persist for a long period	High or low, depending on way of discharging
6	Cloud of Combust-ible dust	Present in normal operation	Fluid bed, filter	Self-ignition	Layers, deposits or heaps of combustible dust	Not likely to occur in normal operation	High with respect to release of fire
7	Cloud of Combust-ible dust	Present in normal operation	Pneumatic conveying system	Self-ignition	Layers, deposits of combustible dust	Not likely to occur in normal operation	High with respect to release of fire

Table recording hazards identified

Risk Estimation / Risk evaluation

Referring to the ”Frequency-Severity Matrix relating to risk levels” in Section 5 of the methodology, risk in terms of explosion safety is made up of the following elements, provided, that no preventive measures are applied:

- Severity is considered ”major”, because first and foremost the effectiveness of ignition sources are classified high in most of the cases on record and the complexity of plant given
- Frequency is considered ”occasional” mainly due to the fact, that the explosion event is likely to occur sometime in life of a spray drying system.

These classifications initially lead to risk level ”B” of the Matrix.

Risk assessment technique	**Factors/relationships which could influence the risk**
Hazard and Operability Study (HAZOP) applicable to complex items of process plant	• Dust concentration in the chamber is the quotient of dust amount (kg/h) and air current (m^3/h). • In the cone of the chamber dust concentration increases in the same measure as the volume thereof decreases. The discharge of powder reduces the relevant dust concentration up to 80 %.
Concept Safety Review / Concept Hazard Analysis	• Relationship between explosion protection measures and hygiene aspects: • Priority must be given to preventive measures rather than additional installations. The underpressure in the plant favours hygiene risks. • Basis of safety is to be achieved by the avoidance of ignition sources, because the occurrence of explosive atmospheres in the form of a cloud of combustible milk powder and its deposits cannot be eliminated. • It is critical for the atomizer from a safety point of view to be: • Non-dripping • Connected to a cooling system • Without vibrations.
Task Analysis / Human Reliability Analysis	• The chamber must be checked at regular intervals. The results must be subject to documentation. • The extent of explosive atmosphere zoning depends very much on the way, the system is operated, e. g. evaporative capacity. • Selection and training of qualified staff is required for the specific tasks. • Removal of dust deposits needs to be done at regular intervals.

Application of risk assessment techniques

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5 in the methodology

This first risk estimation does not take into account the preventive and protective measures.

Reference	Frequency	Severity	Risk Level
1	Occasional	Major	B
2	Remote	Minor	C
3	Remote	Minor	C
4	Remote	Minor	C
5	Remote	Minor	C
6	Occasional	Minor	C
7	Occasional	Minor	C

Table of frequency and severity of events and resulting risk level

Risk Evaluation

Risk level ”B” is an intermediate level and requires some form of risk reduction measures to make the risk acceptable. In the case of risk level ”B” organisational risk reduction measures will not be sufficient. Consequently the step of risk reduction option analysis giving priority to design measures has to be implemented for spray drying systems processing combustible milk powder.

Risk Reduction Option Analysis

Preventive and protective measures have to be applied, to reduce the frequency and/or the severity. The following measures are proposed:

The greatest contributions to reduce risk level ”B” down to risk level ”C” or ”D” are changes to the design concept to eliminate fire events as much as possible. Preventive fire protection measures serving at the same time explosion prevention are as follows

- Temperature monitoring
- Detection of carbon monoxide
- Sensor systems for spark detection (infra-red).
- Fire suppression system

These preventive measures should become part of the inherently safe design of the chamber but also be considered for the filters and the fluid beds. In addition, protective systems should be applied as a combination of options to approach to a low risk level, for example

- Pressure-relief systems or alternative
- Explosion suppression systems

The preventive and protective measures can be joined to an ”explosion safe package”, for example, detection of carbon monoxide triggering alarms and fire suppression systems and providing shut-down of the plant concerned in time.
Spray Drying Systems are often equipped with features to meet special design specifications, many of which provide an increase of safety at the same time. In this context, the following features can be mentioned:

- Pressure shock resistant drying chamber with venting or suppression for explosion protection

- Computerized control systems
- Weatherproof finish for outdoor installations

However, it should be recognized that the installation of such features requires a comprehensive approach taking into account the interactions between the equipment and the particular industrial process performed.

Iteration of the risk assessment procedure

After the application of preventive and protective measures, a new risk estimation and risk evaluation have been made.

Reference	Frequency	Severity	Risk Level
1	Occasional	Minor	C
2	Remote	Minor	C
3	Remote	Minor	C
4	Remote	Minor	C
5	Remote	Minor	C
6	Occasional	Minor	C
7	Occasional	Minor	C

Table of frequency and severity of events and resulting risk levels after Risk reduction measures

Protective system – An explosion venting door

Description of the system

An explosion venting door is an example of a protective system to protect a vessel against the consequences of an explosion. It is designed to open at a pre-determined pressure allowing the explosion inside the vessel to be vented. It consists of the following components:

- Door
- Frame
- Spring mechanism with defined opening pressure
- Baffle plate
- Vacuum breaker

Determination of intended use

The intended use of the explosion door is to open a defined area at a defined pressure without cracking the door The required vent area to protect a specific vessel is outside the scope of this assessment. The explosion door considered in this example is designed to vent an explosion of a dust/air mixture.

Equipment characteristics

All parts of the explosion venting door are constructed from steel. The relevant parameters that influence the intended use can be subdivided as follows:

Process:

Product, Vessel, Pressure, Temperature, Abrasion, Corrosion

Environment:

Maintenance, Specification, Configuration, Ageing, Operator, Weather conditions (Freezing, Snow, Wind, Corrosion)

Product characteristics

An explosible dust air atmosphere is present inside the vessel on which the door is fitted.

Hazard identification

An ignition source can be present inside the vessel and cause ignition of the dust / air atmosphere. However the door itself should not act as a source of ignition. Relevant sources of ignition that could arise from the door are electrostatic due to the impact of the dust / air mixture against the door and mechanical friction due to the door opening.

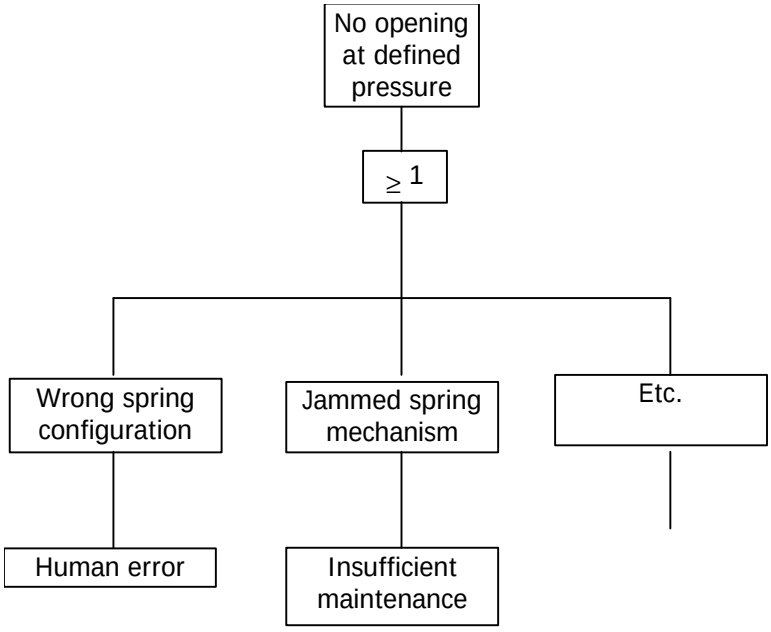
Analysis of possible operating faults

From the wide range of risk assessment techniques presented in the methodology two techniques are selected for hazard identification for this example: What-If-Analysis and Fault-Tree-Analysis.

The keywords for the use of the What-If-Analysis are shown below for one example:

What if...?	Related component	Effect/Hazard	Consequence
... the door do not open at defined overpressure	Door	Vessel cracking	Overpressure to high

The What-If-Questions are related to the identified relevant parameters and consider deviations from the normal operation values.
The following graph shows a part of the Fault-Tree-Analysis for the Top event ”No



The results of the analysis are shown in the following table:

Ref.	Deviation from intended operation	Possible reason	Consequence
1	No opening at defined pressure	Wrong spring mechanism configuration	Overpressure to high
2	No opening at defined pressure	Jammed spring mechanism	Overpressure to high
3	No opening at defined pressure	Insufficient design	Overpressure to high
4	No opening at defined pressure	Unconsidered weather conditions	Opening too early or too late
5	Turnover of the door	Insufficient baffle plate design	Fragmentation
6	Door cracking	Opening pressure to high	Fragmentation
7	Door cracking	Ageing	Fragmentation
8	Door cracking	Wrong door specification	Fragmentation

Risk estimation / evaluation

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5 in the methodology

Ref.	Frequency	Severity	Risk level
1	Remote	Minor	C
2	Occasional	Minor	B
3	Remote	Major	B
4	Remote	Minor	C
5	Remote	Major	B
6	Remote	Major	B
7	Occasional	Major	B
8	Remote	Major	B

Risk reduction methods

Several measures are available to ensure the intended function of the explosion door:

- Operating instructions for installation and use including earthing of the door to prevent electrostatic discharges.
- Use of design standards (existing, future)
- Maintain equipment in good condition
- Design according to environmental conditions (Protection against ice and snow)

Provided the specified measures have been implemented the risk assessment the risk will be reduced to an acceptable level.

Exhaust System of Gas Engines

Determination of intended use

Gas-fired engines are more and more common today mostly used for power generation purposes. The fuel is normally natural gas.
The main purpose of the exhaust system is to transport exhaust gases generated by the combustion in the gas engines, away from the engines to a safe place into the atmosphere. In many applications the waste heat is applied by including a boiler in the exhaust system.

Description of the system

Gas-fired engines can vary in capacity and application and the exhaust gas systems vary accordingly. It is common that several engines are operating simultaneously and their exhaust lines end up in a common stack.

In general the exhaust gas system of a single engine consists of four parts:

1. a pipeline between the engine and silencer or boiler and silencer
2. a silencer or boiler and silencer
3. a pipeline between the silencer or boiler and silencer and into the stack
4. stack (very often the pipelines just continue independently in the stack)

The first pipeline is often, but not always, relatively short. The exhaust gases emerge from the top of the engine and therefore the pipeline consists of an initial vertical pipe piece followed by a 90° bend and a horizontal pipe.

The boilers, which are installed as a part of the exhaust line, are varying in shape as well. Boilers are used especially when the engines are installed in power plants. Their main use is to apply waste heat in the exhaust gases. The casing of the boilers is generally considerably wider than the diameter of the inlet piping. The boilers act as heat exchangers and accordingly each boiler contains a number of pipes for heat transfer from the hot exhaust gases to the water flowing through these pipes.

Also the silencers are wider than the applied exhaust piping. The diameter varies typically up to 2.0 times the diameter of exhaust piping. The length-to-diameter ratio of silencers may vary up to 4. Silencers have internals to damp acoustics generated in the engines. These internals often consist of a set of plates positioned cross flow in the silencer.

The secondary pipeline is often very long (up to 25 time the diameter). The pipeline contains one or several bends varying in angle. In general this pipeline is orientated horizontally up to the stack where it turns vertically.

The entire exhaust gas system is typically designed to withstand pressures of up to 2 bar.

Characteristics of natural gas

The properties of natural gas vary with the composition. The main component of natural gas is methane (between 60-96 % v/v). Other components are higher alkanes (ethane, propane) (up to 30 % v/v) and inert gases (rest).

Based on the properties of methane and the other components of natural gas the properties can be estimated to be as follows:

Auto-ignition temperature	> 460 ºC
Minimum ignition energy	> 0.25 mJ
Explosion limits	LEL: 4 – 7 % v/v
	UEL 13 – 17 % v/v
Maximum explosion pressure	approx. 7 bar
K_G-value	approx. 60 bar.m/s

Functional / State Analysis

A functional state analysis of the exhaust system is shown in the figure below:

Physical state of the substance	Unit operations	Energies/operating state
	Start-up ↓	
Gaseous ←	Transport of gas into engine/ ignition ←	Room temperature/pressure in exhaust system, gas pressure 30 bar
	↓	
Gaseous ←	Normal operation with normal loading ←	385/ 500 ºC in exhaust system, pressure approx. 1 bar, gas pressure 1-3 bar
	↓	
Gaseous ←	Operation under off-loading conditions ←	385/ 500 ºC in exhaust system, pressure approx. 1 bar, gas pressure 1-3 bar
	↓	
	Out of operation	

Functional state analysis of the spray drying system

Remark: The unit operations really happen upstream of the exhaust system while operating the engine. The exhaust gas system is just taking the consequences of unit operations upstream.

Hazard Identification

Under normal conditions the gas in the exhaust gas system will consist of hot combustion gases and there will be no hazard but there are two conditions where unburned gas may reach the exhaust system:

During the start-up procedure of the engines: if ignition of the gas in the cylinder does not occur unburned mixture may enter the exhaust gas system during several strokes.
A second situation where unburned flammable gas-air mixtures may reach the exhaust system is during off-load running due to poor combustion in the engine.

These situations prevail for a relatively short time but can result in a considerable part of the exhaust system being filled with flammable gas-air. An important characteristic is the fact that the natural gas is mixed with air in the engine, which then is transported into the exhaust gas system. For environmental reasons the natural gas-air mixtures applied in the engines are lean.

Ignition sources in the exhaust gas system are only arising from the combustion in the engines. There are otherwise no ignition sources such as hot surfaces, electric equipment, electrostatic discharges etc. inside the pipes.

There are two types of ignition sources arising from the engines: hot gases and hot particles.

The hot combustion gases have a temperature varying from 385 °C to 500 °C depending on the capacity of the engine. The auto-ignition temperature for methane is 540 °C but for natural gas the auto-ignition temperature may be considerably lower: relatively small amounts of higher hydrocarbons (> 10 % v/v) may already lower the auto-ignition temperature by 60 °C. Hence for some engines and for some mixture compositions ignition cannot be excluded. On the other hand it should be mentioned that the auto-ignition temperature of a hydrocarbon fuel normally is measured for rich mixtures. For lean mixtures the auto-ignition temperature is considerably higher. The likelihood for ignition by exhaust gases is therefore considered to be very small.

The most likely ignition source of the gas mixture in the exhaust gas system is hot particles emerging from the engine. The temperature of hot particles can vary from a few hundred degrees up to 1000 °C.

The ”Hazard Identification” is summarised in the following tables:
Table of Ignition sources
Table recording hazards identified

Ignition Sources		
Possible	**Relevant (Yes/No)**	**Significant (include reason)**
Hot surface	No	
Flames and hot gases (including hot particles)	Yes	Yes – can provide sufficient energy
Mechanically generated sparks	No	
Electrical apparatus	No	
Stray electric currents, cathodic corrosion protection	No	
Static electricity:	No	
Lightning	No	
Radio frequency (RF) electromagnetic waves from 10^4 Hz to 3 x 10^{12} Hz	No	
Electromagnetic waves from 3 x 10^{11} Hz to 3 x 10^{15} Hz	No	
Ionizing radiation	No	
Ultrasonics	No	
Adiabatic compression and shock waves	No	
Exothermic reactions	No	

Table of Ignition sources

	Explosive Atmosphere			Ignition Source			
Ref.	**Type**	**Frequency of occurrence or release**	**Location**	**Type**	**Cause**	**Likelihood**	**Effective-ness of ignition sources**
1	Natural gas after ignition failure in engine	Only during start-up procedure (probable)	In exhaust close to engine	Combustion gases	Ignition of gas in engine after initial failures	May happen during start-up (low probability)	Low
2	Natural gas after ignition failure in engine	Only during start-up procedure (probable)	In exhaust close to engine	Hot particles	Ignition of gas in engine after initial failures	Happens every now and then during start-up	Medium
3	Incomplete burning in engine gives rise to flammable atmosphere in exhaust	Only during off-loading running (occasionally)	Entire exhaust	Combustion gases	During off-loading running conditions	May happen (low probability)	Low
4	Incomplete burning in engine gives rise to flammable atmosphere in exhaust	Only during off-loading running (occasionally)	Entire exhaust	Hot particles	During off-loading running conditions equipment	Does happen (medium probability)	Medium

Table recording hazards identified

Risk Estimation / Risk evaluation

Based on the hazard identification as presented above an estimation of the risk of these operations was carried out using the frequency-severity matrix given in the methodology.

To highlight the thoughts behind the severity of events the following:
Considering the severity of explosions in the exhaust gas system one should first of all consider the strength of the pipes, which is 2 bar at a maximum and the potential pressures generated by an explosion. The consequences of explosions in pipes are directly related to the mixture reactivity and to turbulence present in the mixture at the moment of ignition and the turbulence generated by the combustion itself. The latter could cause a positive feedback mechanism that will continue as long as there are walls for generation of turbulence and as long as there is a flammable atmosphere. In pipes this process may even lead to a transition to detonation. For normal hydrocarbons (ethane, propane, butane) a typical distance to obtain a transition to detonation is L/D=60 for straight pipes. For methane this distance is longer. Maximum flame speeds of approximately 150 m/s in a 30 m long, 400 mm pipe open

at one end (ignition at the closed end) have been reported. Pressures at such flame speeds are in the order of 0.5 bar. Similar results were found in a 1400 mm pipe for the same distance of flame propagation. The mixture in these tests was initially quiescent, i.e. not flowing. In case the pipe contains bends the distance for reaching pressures above 2 bar may be considerably shorter.

The positive feedback mechanism will be considerably stronger when obstructions are present inside the pipe. The turbulence generated ahead of the flame will be much more intense and as a result high pressures are generated at much shorter total propagation distance than in an empty pipe. The overpressure-distance relationship depends strongly on the obstacle density (number, size, degree of blockage) and obstacle layout (relative positions). This increase of the effectivity of the positive feedback mechanism will apply to the silencers and boilers included in the exhaust gas systems.

The consequences of explosions of natural gas-air mixtures are expected to be considerably more severe than those for mixtures arising in the exhaust system due to incomplete combustion.

The consequences of pipe failure would be associated with pressure waves causing damage to the building in which the exhaust system, the boiler and silencer are located, potential injuries to people due to these pressure waves and due to the flames emerging from the exhaust system. The exhaust system itself would be heavily damaged, leaving the engines out of operation over a long time.

Application of risk assessment techniques

For each hazardous event referred in the hazard identification, the frequency and severity of each risk has been estimated using criteria given in the methodology. The risk level has then been determined using the frequency-severity matrix in Section 5 in the methodology

This first risk estimation does not take into account the preventive and protective measures.

Reference	Frequency	Severity	Risk Level
1	Remote	Major	B
2	Occasional	Major	B
3	Improbable	Minor	C
4	Remote	Minor	C

Table of frequency and severity of events and resulting risk level

Risk Evaluation

The table shows that all events fall in the categories B or C, which are intermediate levels. Risk reduction measures are necessary to make the risk acceptable.

Risk Reduction Option Analysis

The risk reduction measures could be a combination of several measures often a combination of measures reducing the likelihood of ignition and of those limiting the consequences.

Due to the severity of the consequences of an explosion the reduction of likelihood of ignition will not always lead to changes in the categorisation as proposed by the methodology. The residual risk may still be too high. Nevertheless it is recommended to apply such measures as well to reduce the number of events.

The likelihood of ignition of a mixture of natural gas and air in the exhaust gas system can be reduced considerably by quenching hot particles emerging from the engine: the use of systems consisting of a detector and an extinguishing unit to quench sparks should be considered

There are several techniques to protect the exhaust gas system against the consequences of explosions , viz.:
explosion relief,
explosion proof construction
flame arresters or extinguishing barriers.

Considering explosion relief one should also consider the problems with respect to design of this type of protection. Choice of the size of the vent openings and the location of these is not straightforward. One should know the design pressure of the pipes and one should reckon with external effects: flames emerging from the vent openings and pressure build-up in the room into which the venting occurs. The use of additional vent ducts or flame arresters onto the vent openings should be considered.

Considering explosion proof construction one should be able to predict the maximum pressure in the exhaust system. Transition to detonation and the high associated pressures has to be considered as well.

Application of flame arresters would stop flames resulting from ignition upstream of the flame arrester. As hot particles may be an ignition source the location of these arresters should be considered with care. The flame arrester should be chosen according to the conditions prevailing in the engine: temperature and an optimal methane/air mixture. The arrester should be explosion resistant; i.e. it should be able to withstand the maximum explosion pressure generated in the part of the exhaust gas system upstream of the arrester and the drag due to the velocity through the arrester.
Special arrangements are available to clean flame arresters in case of pollution of the arrester by soot particles generated in the engine.

Another possibility is the use of an extinguishing barrier. As for the flame arrester location of the barrier should be chosen with care.

The proposed measures for limitation of the consequences of explosions would lead to reducing the severity to minor or even negligible depending on the solution chosen.