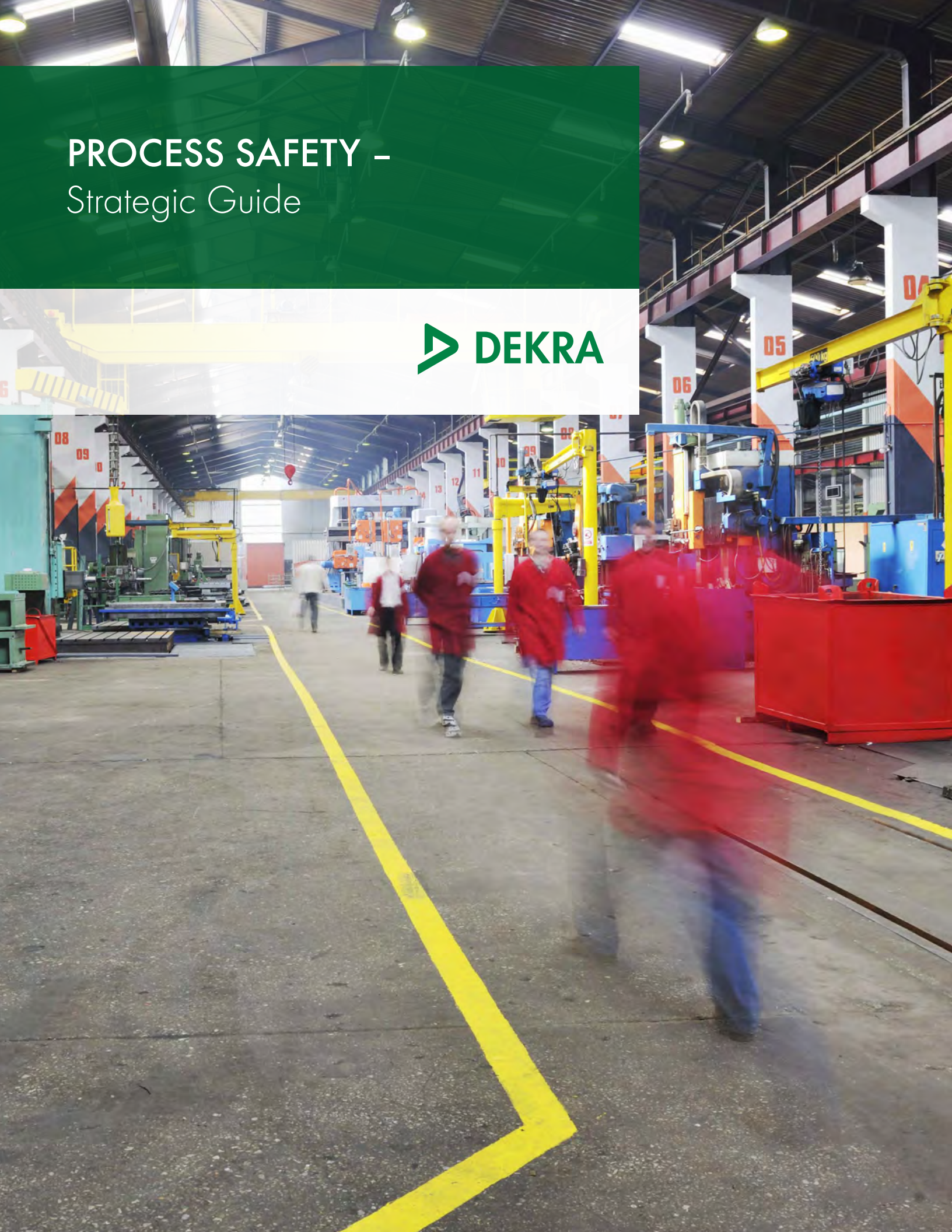
PROCESS SAFETY –
Strategic Guide

DEKRA



First published in the US in 2018 DEKRA Process Safety
113 Campus Drive, Princeton, NJ 08540, USA
Tel +1 609 799 4449 Fax +1 609 799 5559
Email: process-safety-usa@dekra.com Website: www.dekra-process-safety.com

Designed and typeset by DEKRA Process Safety

Content

1. A Guide to Process Safety

What is Process Safety and is your company approaching it in the same manner as personal or occupational safety?

Process safety needs to be considered separately from personal or occupational safety. The latter considers such issues as slips, trips and falls along with equipment safety such as machine guards or extract systems to minimize exposure to dangerous products. Accidents involving personal safety tend to occur frequently but often have little consequence. Conversely process safety incidents tend to happen infrequently but can often have catastrophic results when things go wrong. Typical examples of process safety incidents include rapid overpressure events in process plant arizing from dust, gas or vapor explosions, detonation or deflagration of highly energetic materials, rapid decomposition of thermally unstable substances or mixtures and runaway exothermic chemical processes. The result of any of these events going out of control range from insignificant to catastrophic and they can result in death or serious injury, loss of manufacturing plant, unwelcome media attention and large financial losses.

Much of the assessment of hazard and risk associated with process safety and the safe operation of process plant is the responsibility of the employer following guidelines, legislation and best practice. It is therefore critical that informed decisions are made, often involving advice from an expert in process safety and using the best tools available.

Process safety includes the identification of a suitable Basis of Safety to prevent or mitigate process safety hazards and is therefore a prerequisite for safe operation. However realizing and implementing the proposed Basis of Safety involves an in-depth knowledge of the materials in use, the process operations, equipment specifications and the facilities that house the processes. Having the ability to thoroughly understand all of the hazards is critical in developing a suitable and robust Basis of Safety.

The various phases of the assessment procedures, used to define the most appropriate Basis of Safety, are explored herein.

The most common approach to process safety involves identification of the hazard, determination of the level of risk and implementation of the necessary safeguards that form the Basis of Safety. Depending upon the process, it may be necessary to employ prevention or protection solutions some of which may require the specification and design of a functional safety system. The overall success of the functional safety system(s) relies on each stage being well executed – deficiencies in any phase of the safety lifecycle will directly impact on the end result.

Why Bother?

There are numerous reasons to pay attention to process safety risks. The threat of legal action for non-compliance is a very real inducement, but the threat of serious injury or fatalities to staff, loss of production and income, damage to a company's reputation, the potential for increased insurance premiums and the loss of valuable production assets are equally good reasons even though they may not involve the law directly.

2. Process Safety Legislation

At the time of publication, and especially within the EU, there are several directives that have been implemented into national legislation to ensure that personnel working within the process industries are satisfactorily protected. The most commonly encountered are:

Health and Safety at Work

All countries within the EU have some form of Health and Safety at Work legislation. In the UK this is the Health and Safety at Work Act 1974 (HSWA 1974). The legislation states;

The employer must consult you or your safety representative on matters relating to your health and safety at work, including:

- Any change which may substantially affect your health and safety at work, e.g. in procedures, equipment or other ways of working;
- The employers arrangements for getting competent people to help him/her satisfy health and safety laws;
- The information you have to be given on the likely risks and dangers arizing from your work, measures to reduce or remove these risks and what you should do if you have to deal with a risk or danger;
- The planning of health and safety consequences if introducing new technology.

In particular, the employer must:

- Assess the risks to health and safety
- Make arrangements for implementing the health and safety measures identified as being necessary by the assessment;
- If there are five or more employees, record the significant findings of the risk assessment and the arrangements for health and safety measures;
- Appoint someone competent to assist with health and safety responsibilities, and consult you or your safety representative about this appointment;
- Take precautions against danger from flammable or explosive hazards, electrical equipment, noize and radiation.

Most countries, and especially those within the EU and USA, follow a similar approach to Health & Safety.

CONTROL of MAJOR HAZARDS (COMAH or Seveso II), EU Council Directive 96/82/EC

Control of Major Accident Hazards involving Dangerous Substances is the UK implementation of the Seveso II directive. These Regulations were amended in 2003 by directive 2003/105/EC and consider potential incidents with off-site effects.

- Member States shall require the operator to draw-up a document setting-out his/her Major Accident Prevention Policy (MAPP) and to ensure that it is properly implemented. The Major Accident Prevention Policy established by the operator shall be designed to guarantee a high level of protection for persons and the environment by appropriate means, structures and management systems.
- For upper tier sites, a safety report has to be completed that takes into consideration consequences of incidents, both on and off site. Detailed hazard and risk assessments, along with how the safety of processes is controlled, form part of this document.

Lower and upper-tier sites are classified by the quantity of hazardous materials that are kept on-site. For instance, consider 'very toxic' substances stored on-site, the lower-tier value is 5 tons and once the quantities reach 20 tons, upper-tier classification would come into force. For materials classified 'flammable' the lower-tier level would be 5000 tons and upper-tier 50,000 tons.

EU Machinery Directive 2006/42/EC

Fire

Machinery must be designed and constructed in such a way as to avoid any risk of fire or overheating posed by the machinery itself or by gases, liquids, dust, vapors or other substances produced or used by the machinery.

Explosion

Machinery must be designed and constructed to avoid any risk of explosion posed by the machinery itself or by gases, liquids, dust, vapors or other substances produced or used by the machinery.

To that end, the manufacturer must take steps to:

- Avoid a dangerous concentration of products
- Prevent combustion of a potentially explosive atmoshpere
- Minimize any explosion which may occur so that it does not endanger the surroundings
- The same precautions must be taken if the manufacturer foresees the use of the machinery in a potentially explosive atmosphere
- Electrical equipment forming part of the machinery must conform, as far as the risk from explosion is concerned, to the provision of the specific Directives in force.

Safety Devices, for example

- Valves with additional means for failure detection intended for the control of dangerous movements on machinery
- Emergency stop devices
- Discharging systems to prevent the build-up of potentially dangerous electrostatic hazards

Emissions of hazardous materials and substances

- Machinery must be designed and constructed in such a way that risks of inhalation, ingestion, contact with skin, eyes and mucous membranes and penetration through the skin of hazardous materials and substances it produces can be avoided.
- Where a hazard cannot be eliminated, the machinery must be so equipped that hazardous materials and substances can be contained, evacuated, precipitated by water spraying, filtered or treated by another equally effective method.
- Where the process is not totally enclosed during normal operation of the machinery, the devices for containment and/or evacuation must be situated in such a way as to have the maximum effect.

The directive also makes reference to IEC 61508/61511 (see section 12 on Safety Instrumented Systems) as best practice.

CHEMICAL AGENTS DIRECTIVE "CAD" (EU Directive 98/24/EC)

"On the protection of the safety and health of workers from the risks related to chemical agents at work."

Fires, explosions and chemically unstable (mixtures of) substances are included (article 6.6)

- Refers to ATEX 95 for equipment group categorization
- Overlaps with ATEX 137 for explosions

Measures shall be taken, in order of priority:

- To prevent hazardous concentrations or quantities
- To avoid ignition sources or adverse conditions for chemically unstable substances
- To mitigate the detrimental effects of fires/explosions and harmful physical effects from unstable substances

ATEX 95(EU Directive 94/9/EC) (The Equipment and Protective Systems (Amendment) Regulations 2001 (SI 2001/3766) - UK)

- Applies to equipment and protective systems intended for use in potentially explosive atmospheres
- Safety devices, controlling devices and regulating devices outside explosive atmospheres can be covered as well
- Any equipment conforming to ATEX 95 must be allowed on the market in the EU.

ATEX 95 requires that account must be taken of the intended use of the equipment and that the manufacturer must establish the operational parameters for the functioning of the equipment. The directive covers both the electrical and mechanical components and must take into consideration the propensity to generate electrostatic discharges

ATEX 137 (EU Directive 1999/92/EC)

"On minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres".

The employer shall assess the specific risks from explosive atmospheres, taking account at least of:

- The likelihood that explosive atmospheres will occur and their persistence
- The likelihood that ignition sources, including electrostatic discharges, will be present and become active and effective
- The installations, substances used, processes and their possible interactions
- The scale of the anticipated effects
- The overall assessment of the explosion risks
- The directive also states that an Explosion Protection Document (ATEX 137, article 8) must be produced and that is mandatory, to demonstrate explosion risks have been DETERMINED & ASSESSED
- Adequate measures have been taken to attain aims of the Directive
- Hazardous areas are classified into zones
- Places where minimum requirements of the Directive apply (signs displayed)
- Workplace & work equipment is designed, operated & maintained with due regard for safety
- Arrangements are made for safe use of equipment

One of the most important aspects of this regulation is to ensure that all actions are completed by a person 'competent' in the field of fire and explosions.

Dangerous Substances and Explosive Atmospheres Regulations (DSEAR,2002)

The UK implementation of ATEX 137 differs from most other European national legislation in that it includes the section on fires and explosions and chemical runaway reactions from the Chemical Agents Directive, but does not specify a separate Explosion Protection Document.

The Pressure Systems Regulations 1999

These Regulations apply to pressure equipment and assemblies with a maximum allowable pressure PS greater than 0.5 bar. The following are pressure equipment -

(a) Vessels, except those referred to in sub-paragraph (b), for -

- Gases, liquefied gases, gases dissolved under pressure, vapors and also those liquids whose vapor pressure at the maximum allowable temperature is greater than 0.5 bar above normal atmospheric pressure (1 013 mbar) within the following limits -
  - (i) For fluids in Group 1, with a volume greater than 1L and a product of PS and V greater than 25 bar-L, or with a pressure PS greater than 200 bar;
  - (ii) For fluids in Group 2, with a volume greater than 1L and a product of PS and V greater than 50 bar-L, or with a pressure PS greater than 1000 bar, and all portable extinguishers and bottles for breathing apparatus;
- Liquids having a vapor pressure at the maximum allowable temperature of not more than 0.5 bar above normal atmospheric pressure (1 013 mbar) within the following limits -
  - (i) For fluids in Group 1, with a volume greater than 1L and a product of PS & V greater than 200 bar-L, or with a pressure PS greater than 500 bar;
  - (ii) For fluids in Group 2, with a pressure PS greater than 10 bar and a product of PS and V greater than 10 000 bar-L, or with a pressure PS greater than 1000 bar;

(b) Fired or otherwize heated pressure equipment with the risk of overheating intended for generation of steam or super-heated water at temperatures higher than 110°C and having a volume greater than 2L, and all pressure cookers;

(c) Piping intended for -

- gases, liquefied gases, gases dissolved under pressure, vapors and those liquids whose vapor pressure at the maximum allowable temperature is greater than 0.5 bar above normal atmospheric pressure (1 013 mbar) within the following limits
  - (i) For fluids in Group 1, with a DN greater than 25;
  - (ii) For fluids in Group 2, with a DN greater than 32 and a product of PS and DN greater than 1 000 bar;
- liquids having a vapor pressure at the maximum allowable temperature of not more than 0.5 bar above normal atmospheric pressure (1 013 mbar), within the following limits:
  - (i) For fluids in Group 1, with a DN greater than 25 and a product of PS and DN greater than 2 000 bar;
  - (ii) For fluids in Group 2, with a PS greater than 10 bar, a DN greater than 200 and a product of PS and DN greater than 5 000 bar;

(d) Safety and pressure accessories intended for equipment covered by sub-paragraphs

(a), (b) and (c), including where such equipment is incorporated into an assembly.

DN means nominal size of pipework.

3. First Steps in Process Safety

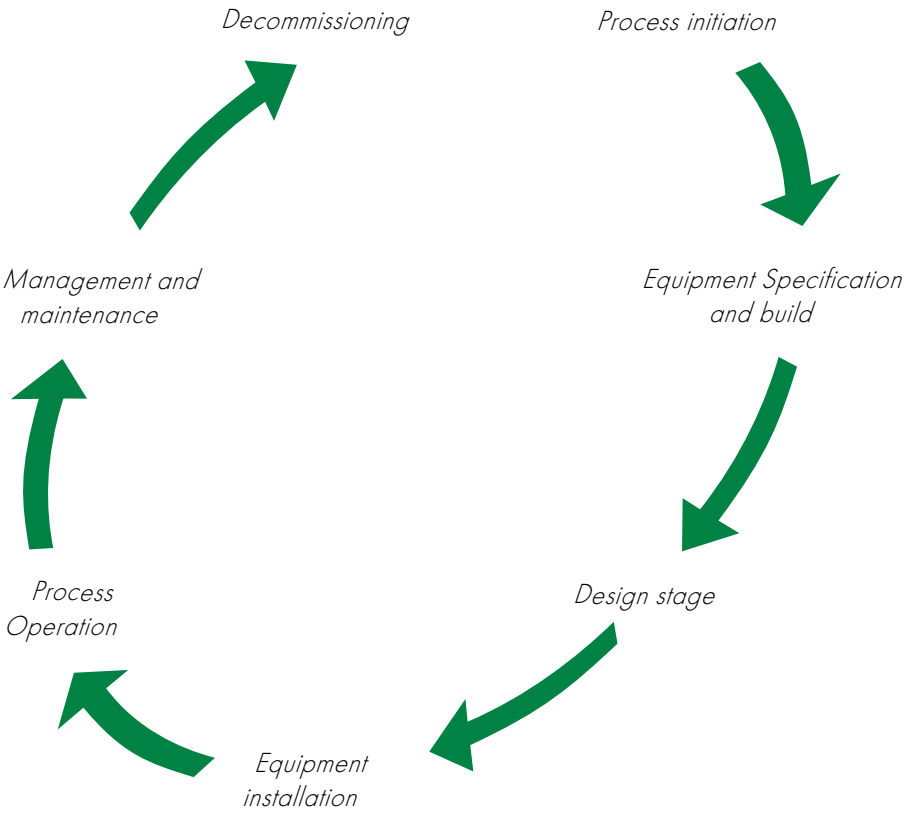
Process safety begins at the inception of an idea and continues through the various stages of development, use and finally removal of the equipment from the manufacturing process. This is called the Process Safety Lifecycle and is illustrated above with Figure 1 and dealt with in more detail in Section 14 of this Guide to Process Safety.

The same approach applies to new processes that have not even been designed, to those that are, and have been, in use for some time. In order to become aware that you have a process safety problem, it is first necessary to identify the hazard. For this Guide to Process Safety, it could either be;

- Flammability - fire or explosion associated with flammable gases, vapors or dusts
- Exothermic runaway or gas generating reactions (see Section 11)
- Release of toxic or harmful materials
- Over pressurization of vessels

Each of these items will be dealt with separately within the document, but on the majority of plants, there will be the necessity to manage and control dangerous substances. Therefore always remember that, along with the physical approach to handling hazardous materials, there should be in place some form of system of communication and documentation to ensure continued control for the safety of any operation. This in turn leads us to the implementation of process safety management systems (see Section 17) and the management approach. Detailed PSM systems are normally associated with what is termed Control of Major Accident Hazard sites (COMAH or SEVESO II), however a failure to apply a systematic approach for any industrial process handling hazardous materials, is 'foolhardy' whereby "complacency can ultimately lead to the mother of all accidents."

Although it is important to regard each of the above hazards as being equally important, it becomes difficult and complicated to cover every aspect of each hazard in a single document. Therefore this Guide to Process Safety tends to focus on two of the more prevalent hazards that DEKRA Process Safety Global has to work with, namely that of flammability and/ or explosion from gases, vapors or dusts and chemical reaction hazards. Note that it is also important to consider both normal and abnormal operating conditions when deciding on whether a potentially flammable atmosphere could exist. It is also important to realize that, at this stage of assessment, there is no requirement to appreciate the level of risk involved in any operation, but purely to establish whether a hazard exists.



4. Hazardous Area Classification (HAC)

"'Hazardous' means that special precautions are needed to protect the health and safety of workers".

Once it is realized that there is a potential to generate a flammable atmosphere, and this could occur within a vessel or in proximity to equipment, it will now be necessary to establish the frequency that the atmosphere is present and to then designate a zone number, in other words classify the area of release. Hazardous Area Classification was originally created as a means of optimizing electrical equipment selection located in areas where flammable gases and/or vapors were present and was initially called "electrical area classification". Over time this process was developed further and finally, with the introduction of more stringent, European legislation such as ATEX 137, dusts were included into the EU classification procedure along with the need to consider the potential for ignition from electrostatic charge generation or mechanical movement.

In hazardous areas special equipment must be used and hazardous areas must be clearly marked. Area classification assesses the probability of potentially explosive atmospheres occurring and once the probability is established, ignition sources can be controlled to match the level of risk associated with the designated area. Hazardous Area Classification does not specify the equipment and does not take account of consequences. These issues are covered as part of the general safety considerations.

European Union (EU)

ATEX 137, or DSEAR in the UK, requires that places where potentially explosive atmospheres may occur, or not occur, are classified into hazardous and non-hazardous areas respectively. There are separate hazardous area codings for gases/vapors and dusts and these are also broken down into 3 levels of frequency.

North America

Hazardous areas are placed into divisions which are decided by the probability of the presence of a hazardous material. The differences between the EU and the USA/Canada methodologies are shown in Table 1.

Examples of Zoning Levels Are:;

In the EU Zone 0/20 or in N. America Division 1 - inside gas/vapor and dust handling equipment

In the EU Zone 1/21 or in N. America Division 1 - inside some equipment or typically up to 1 m from the source

In the EU Zone 2/22 or in N. America Division 2 - typically up to 1 - 3 m from the source or wherever dust layers occur or around a non-confined Zone 21 due to formation of dust layers

Although standards give practical guidance on zoning sizes, practical considerations can make it necessary to classify a whole area such as when the boundaries of a room provide a more realistic border for a zone.

In order to establish correct zoning for any process it is necessary to;

- Identify sources of release
- Identify the duration, that is determine the grade of release (continuous, primary or secondary)
- Consider ventilation and housekeeping
- Assign zone numbers
- Estimate zone size

Area Classification

	Hazard	Hazard continuously present (> 1000 hours per year)	Hazard present under normal operation (10-1000 hours per year)	Hazard only present, under abnormal conditions (< 10 hours per year)
	Gases	Zone 0	Zone 1	Zone 2
European Union (EU)	Dusts	Zone 20	Zone 21	Zone 22
North America	Gases & Dusts	Division 1		Division 2

This is illustrated more simply by Figure 2, below;
All of the hazardous area information has to be collated into a detailed report that accompanies the zone drawings. These drawings are normally presented in plan form but sometimes it is necessary to also provide side elevations of process plant, especially where equipment covers several floors, or in the case of gases and vapors that may rize or fall.

A final mention on the application of hazardous areas is to consider the pros and cons of using 'blanket' zoning as against 'bubble' zoning. In principle the blanket zone approach can be acceptable especially where boundaries are governed, such as by the walls of a room. However, the advantages of bubble zoning are that these areas can be identified as being the places where hazardous materials are being handled and that only equipment located within these zones needs to comply with stricter regulations, thereby reducing purchasing costs and additional problems with maintenance and replacement.

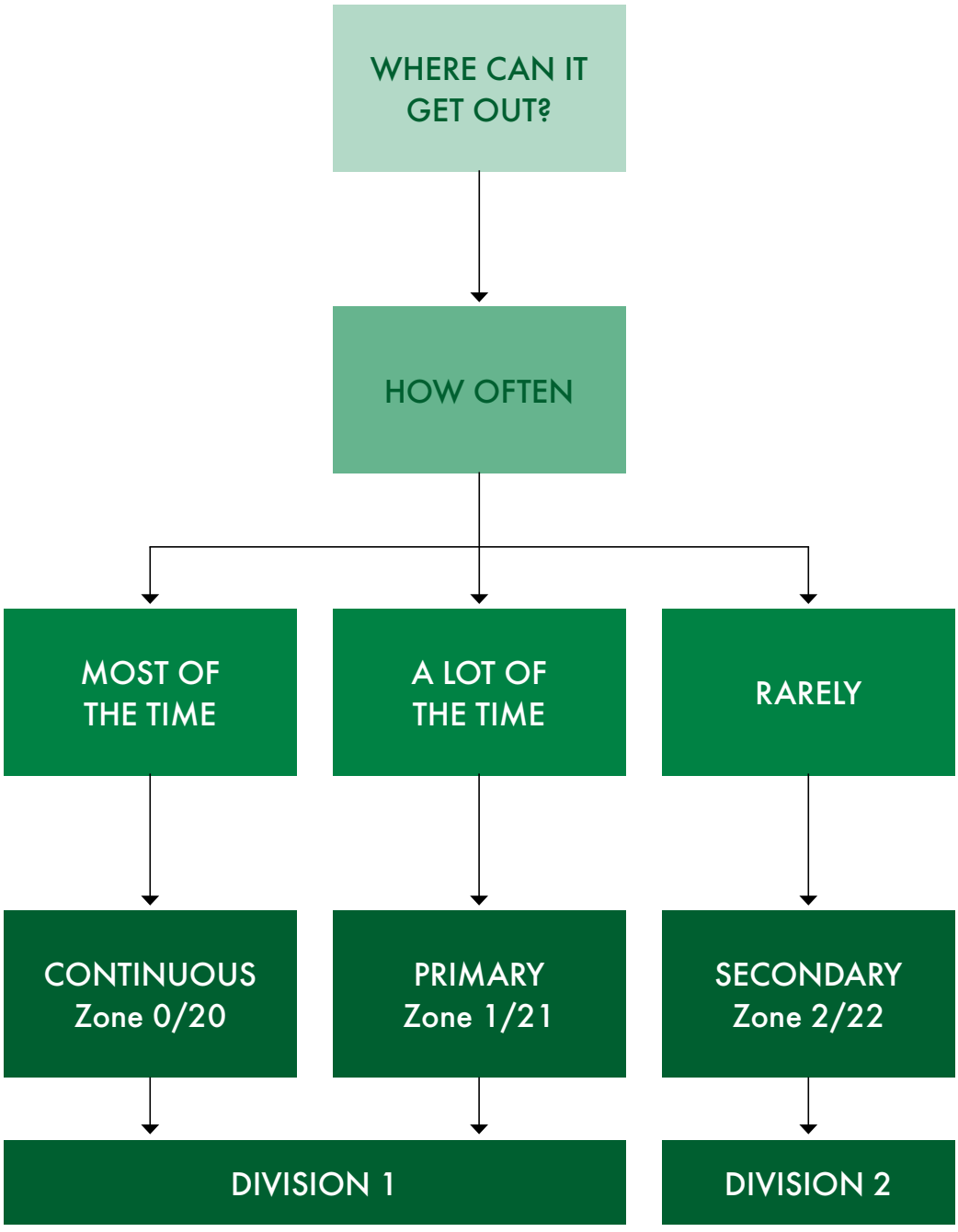


Figure 2. Schematic of Hazardous Area Classification

5. Hazard and Risk Assessment

"A hazard is anything that has the potential to cause harm. A risk is the chance of that harm occurring".

Once it has been established that a hazard exists and the area that may be affected has been defined, it is now necessary to look at the level of risk involved in processing the hazardous material.

All of the legislation noted before requires that the employer shall identify every potential hazard involved in a manufacturing process and to then determine the level of risk involved with each of the hazardous operations. The risk assessment procedure is an organized and systematic look at these processes with a view to determining if a process has the potential to cause harm and the likelihood of it doing so. Process Safety Culture (Ref. Section 16) and Process Safety Management (PSM, Ref. Section 17) all use some form of risk assessment to analyze and control the risks associated with their operations.

PSM is not just focused on high risk, COMAH sites but can also apply to any hazardous manufacturing operation. There are numerous techniques available for hazard and risk assessment including, but not limited to;

Hazard and Operability Studies (HAZOP)

A structured technique involving a review team of knowledgeable professionals guided by a study leader. A series of guide words are used to examine potential deviations that could occur for each part of the plant or process. For example, when considering a reactor, deviations might include higher temperature, increased catalyst, inhibitor contamination, failed agitation, inadequate cooling, etc. The consequence (including knock-on effects) of each deviation judged to have a credible cause is considered by the team, the acceptability of safeguards assessed, and potentially hazardous situations are retained for more detailed further investigation (consequence analysis).

What-If or Checklist Analysis

A technique in which a checklist of potential failure situations determined from past experience is reviewed in combination with the plant and process details. An example may be, 'What if the high level switch fails to operate?' The responses could vary from a fairly insignificant action to catastrophic failure.

Failure Modes and Effects Analysis (FMEA)

FMEA is based on identifying the possible failure modes of each component of a system and predicting the consequences of the failure. This method is especially useful for the analysis of systems containing many critical components but few process steps (e.g. instrumentation loops)

Fault Tree Analysis (FTA) and Event Tree Analysis (ETA)

FTA is based on working from a "top event" such as "explosion in reactor" and then considers all combinations of failures and conditions which could cause the event to occur. This technique is widely used as a precursor to Quantitative Risk Assessment (QRA).

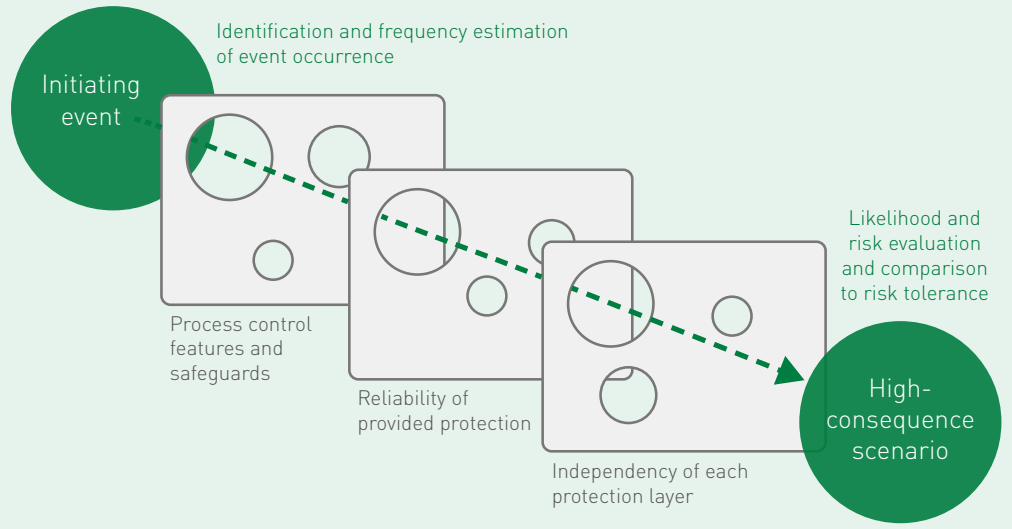
Event Tree Analysis (ETA) works in reverse, by identifying an "initiating event" and then working forward to "top events".

FMEA, FTA and ETA are complex techniques and, because of this, their use in the process industries is often limited to the identification of hazard progression sequences before quantification is applied.

Layer of Protection Analysis (LOPA)

Layer of Protection Analysis (LOPA) is a methodology for hazard evaluation and risk assessment and fits between a qualitative risk assessment such as HAZOP and quantitative risk assessment techniques such as FTA/ETA. LOPA is a recognized technique for selecting the appropriate Safety Integrity Level (SIL) of a Safety Instrumented System (SIS) (Ref. Section 12).

As with any form of risk assessment, it is always wize to be aware that things can still go wrong and the Swiss Cheese example (Figure 3 over) highlights the alignment of unidentified faults that can result in an incident



Hazard & Risk Assessment

Simple hazard and risk assessment technique carried out by a competent person. This is often the most efficient approach when considering simple process safety issues.

The choice of the most appropriate hazard identification technique is a key step in being able to ensure and demonstrate the degree of safety of a plant. The detailed techniques are generally more applicable to highly hazardous processes (e.g. chemical processes using extremely hazardous substances) and often follow on from less rigorous screening studies. The HAZOP technique is probably the most widely used identification methodology in the process industries but its success is governed by the quality of the team. A team containing experienced practitioners and straddling a variety of disciplines is required to achieve a thorough and balanced view of the process hazard. Such a team will usually focus the HAZOP study in the appropriate direction – spending a proportionate amount of time on the higher risks while remaining rigorous across the whole process.

Whichever technique is chosen, the outcome should be a list of retained scenarios requiring consequence analysis, possibly their quantification, and will yield recommendations for steps to be taken for the specification, detailed design and implementation of appropriate safety measures. When any hazard and risk assessment is performed, it must take into consideration both normal and abnormal situations. This is particularly relevant when maintenance is being performed. These situations can sometimes only be realized due to experience in performing risk assessments on other similar pieces of equipment, or attending incidents where a particular failure mode has occurred. This amplifies the requirement under ATEX 137/ DSEAR that the person who performs the hazard and risk assessment must be 'competent' in the field of fire and explosion.

Risk Analysis

The consequence and risk of an undesirable event will dictate the level of expense and time allocated to addressing it. The consequence may be trivial (e.g. off-spec product) or catastrophic (e.g. reactor explosion resulting in fatalities, environmental contamination, and commercial loss). For gas, vapor or dust explosion hazards, the consequences of an event may be evaluated using explosion prediction software (such as PHAST, etc). Such software is well developed, readily available and provides a rapid overview of the impact of an event.

For thermal stability and reaction hazards, consequence analysis is harder to evaluate by modelling with software owing to the extensive nature of the required inputs (kinetic parameters, physical properties, prediction, etc). For batch and semi-batch reaction hazards, experimental techniques are usually employed to simulate the deviation scenario under thermal inertia (phi factor) and heat loss conditions which closely resemble the manufacturing environment. The techniques employed are usually based around adiabatic scenarios such as the ADC II (adiabatic pressure Dewar calorimeter). These methods provide a basis for simulating specific events and determining – in terms of pressure, temperature and time – the consequences of the deviation under assessment. Data from such tests is also indispensable for the specification of safety systems (e.g. required response time from corrective controls, data for emergency relief vent sizing, etc).

The magnitude of the consequences will govern the acceptability of the risk and therefore the extent of effort and cost applied to controlling the risk.

The principle of ALARP (As Low As Reasonably Practicable) is applied by UK and other regulators to such risks, and decisions taken during the assessments will be required to be fully supported by investigation. This involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which workplace risks should be controlled.

In the great majority of cases, ALARP can be decided by referring to existing 'good practice'. Good practice is usually a determination agreed with the Competent Authority (CA) which, in the UK, would be the Health and Safety Executive (HSE) and in the USA, the Occupational Safety and Health Administration (OSHA). Every country has its own CA such as Ireland which uses the Health and Safety Authority (HSA). Good or best practice may be based upon national or internationally accepted standards and/or guidelines.

For high hazards, complex or novel situations, good practice is supplemented using more formal decision making techniques, including cost-benefit analysis. The amount of effort expected for the ALARP analysis is directly proportional to the size of the risk.

In essence, making sure a risk has been reduced to ALARP is about weighing the risk against the sacrifice needed to further reduce it. The decision is weighted in favour of health and safety because the presumption is that the duty-holder should implement the risk reduction measure. To avoid having to make this sacrifice, the duty-holder must be able to show that it would be grossly disproportionate to the benefits of risk reduction that would be achieved. Thus, the process is not one of balancing the costs and benefits of measures but, rather, of adopting measures except where they are ruled out because they involve grossly disproportionate sacrifices. Extreme examples might be:

- To spend $1m to prevent five staff suffering bruized knees is obviously grossly disproportionate; but
- To spend $1m to prevent a major explosion capable of killing 150 people is obviously proportionate.

Of course, in reality many decisions about risk and the controls that achieve ALARP are not so obvious. Factors come into play such as ongoing costs set against remote chances of one-off events, or daily expense and supervision time required to ensure that, for example, employees wear ear defenders set against a chance of developing hearing loss at some time in the future. It requires judgment. There is no simple formula for computing what is ALARP.
ALARP does not mean that every measure that could possibly be taken (however theoretical) to reduce risk must be taken. It does not necessarily represent the highest standards of risk reduction, nor does it guarantee against loss.

Qualitative Risk Assessment (RA)

Qualitative Risk Assessment is useful because it allows one to quickly identify potential risks, as well as assets and resources which are vulnerable to these risks. A standard qualitative risk assessment would be HAZOP and it's aim in risk analysis is to gain a level of risk protection which is acceptable, and one which will increase awareness among people working with the hazard. This type of risk analysis will often make use of calculations which are fairly basic and uses values based on ranking such as high, medium or low; very important, important or not important. It is not necessary to put a value to the risk being identified.

Quantitative Risk Assessment (QRA)

Quantitative Risk Assessment (QRA) is a structured approach to identifying and understanding the risks associated with hazardous activities such as the operation of an industrial process. The assessment starts by taking inventory of potential hazards, their likelihood, and consequences. The quantified risks are then assessed by comparison against defined criteria.

Quantitative Risk Assessment provides valuable insights into the features of the process, highlighting those aspects where failures may result in harm to operators, members of the public, the environment and/or the asset itself. QRA provides a basis for decision making in the design and operation of the plant, and may also be required to legally show "fitness to operate".

Hazard & Risk Factors

One word of warning with only using QRA is that some critics have expressed concerns that QRA tends to be overly quantitative and reductive. For example, they argue that QRAs can ignore qualitative differences among risks. Some claim that quantitative approaches divert attention from precautionary or preventative measures. Others consider risk managers little more than „blind users" of statistical tools and methods.

6. Potential Ignition Sources

The risk assessment is based on the hazard of the material but also the 'potential' to ignite any **flammable** atmosphere. There are many potential ignition sources in the workplace and European standard EN1127-1 specifies the following as the main cause for concern;

Effective Ignition Sources from EN 1127-1

(a) Hot surfaces;
(b) Flames, included smoking and hot work activities;
(c) Mechanically generated (friction) sparks including thermite sparks;
(d) Electrical apparatus;
(e) Stray electric currents within installations;
(f) Static electricity;
(g) Lightning;
(h) Radio frequency electromagnetic radiation;
(j) Visible and similar high frequency electromagnetic radiation;
(k) Ionizing radiation;
(l) Ultrasonic sound waves;
(m) Adiabatic compression and shock waves and exothermic reactions, spontaneous combustion

Other potential ignition sources are thermal decomposition (Ref. Section 9), chemical runaway reaction (Ref. Section 11) etc.

Once a potential ignition source has been identified, then it may be necessary to continue with more detailed assessments. For instance where ignition from mechanical equipment may be an issue, such as in high speed mixers or mills, then a detailed Mechanical Equipment Ignition Risk Assessment (MEIRA) should be performed using the relevant standard and published guidelines. This is most apparent in the EU directive ATEX 137 where this is actually a legal requirement. Any new equipment being installed into a zoned area should be ATEX compliant.

For electrical equipment to be installed, maintained and repaired it is advisable for the electrical personnel to be adequately trained.

The CompEX Scheme within the UK is an example of a recognized certified training program.

Electrostatic assessments can be difficult and should only be performed by somebody with appropriate knowledge of the risks from electrostatic discharges. For more details please see the DEKRA Process Safety Guideline to Electrostatic Hazards.

Prohibition Notices for Ignition Sources

7. Developing the Basis of Safety

Once the potential for an explosive atmosphere to occur has been determined, then the next stage is to establish a suitable Basis of Safety for each part of the manufacturing process.

The selection of the most appropriate Basis of Safety will be governed by technical and financial issues. Whichever Basis of Safety is selected, it is critical that all phases of the hazard and risk assessment process are rigorously completed. Characterization of the process and / or material hazards is a critical phase in the process and one that can easily be omitted. The selected Basis of Safety must ultimately prevent personnel from injury and therefore must be based on a sound understanding of the hazards.

As stated before most of the information will come from the hazard and risk assessment and will involve taking into consideration the following manufacturing conditions, as shown in Figure 4.

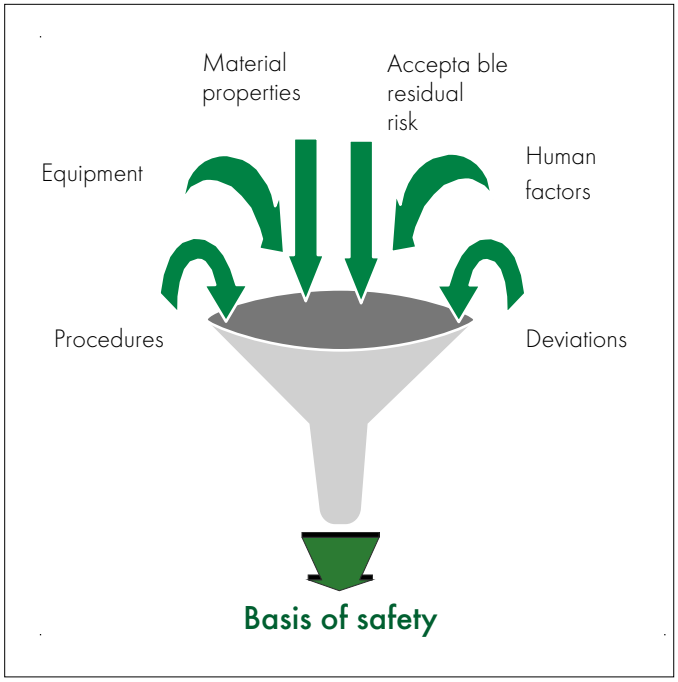


Figure 4. Basis of Safety Funnel

Procedures

It needs to be established that written operating procedures are provided by the company to ensure safe operation of the process, and that these procedures are communicated to personnel who are actively involved in working in hazardous areas.

Deviations

Is it possible to deviate from a given procedure, and has the risk assessment taken this into consideration? In many instances an incident has occurred because either an operator working on a process has inadvertently changed the way the operation is meant to have been performed, or maintenance has been involved which has resulted in an extraordinary situation being created.

Equipment

In some instances the way a piece of equipment operates may indicate the preferred Basis of Safety, for instance where a dust collector is supplied with explosion vent panels. Often equipment is upgraded during the working life of a process such as when a mill is replaced by a micronizing unit to produce finer powder. In an instance where a piece of equipment is replaced by a non-identical piece of equipment, then the risk assessment should be repeated.

Human Factors

The way that a human interacts with a process can be extremely diversified. In some instances a human can sense that equipment is not functioning correctly and stop it before a disaster occurs, or on the other hand a human can turn the wrong valve, add or fail to add the correct product, or change an operation to work outside its temperature or pressure limitations. It is therefore necessary to take both the positive and negative aspects and their consequences together when defining the Basis of Safety.

Material Properties

As stated previously a detailed hazard and risk assessment cannot be completed without an understanding of the materials properties. The ATEX/DSEAR regulations specifically refer to the requirement for material property information, in order to conduct a valid risk assessment. Therefore, fundamental to the provision of a sound Basis of Safety is a thorough understanding of the process and / or materials involved. For explosion hazards, characterization of the hazard is provided through an understanding of the parameters detailed in Table 2.

Data may be available from reliable literature sources for gases and vapors, but for dusts and powders this data is less dependable. Variable properties such as particle size or moisture content can significantly affect the flammability properties, meaning that testing is often the only solution. However testing can be limited to those tests needed to specify and confirm the acceptability of the Basis of Safety. Not all parameters may be essential for the ultimate Basis of Safety. Please note that in certain instances, thermal stability data may be required (reference Section 9.) For more information, see DEKRA Process Safety Strategic Guide to Handling Dust and Powders Safely.

Acceptable Level of Risk

No manufacturing operation is 'risk free' and it is therefore necessary to establish the acceptable level of risk involved with an operation. For instance for a silo that is located on a green field site, far from domestic housing, it may be acceptable to use explosion relief panels as the sole Basis of Safety. If the silo were close to other external locations such as a domestic housing estate or even another factory, then suppression systems or inert gas blanketing may be a preferred solution. The Basis of Safety normally fits into one of the following 3 groups:

Inherent Safety

This is where the system itself has been identified as being safe to use without modification. No system is technically, 'inherently' safe but there are normally four ways in which a process can be made safer:

- Minimize or reduce the quantities of hazardous materials present at any one time. For instance this could be achieved by using smaller vessels or putting in a day hopper instead of feeding off a main silo
- Substitute or replace one material with another of less hazard, e.g. cleaning with water and detergent rather than a flammable solvent, or using aqueous solutions rather than powder with solvent
- Moderate or reduce the hazardous effect of a material, e.g. using a solvent in a dilute form rather than concentrated form, or working below the Flashpoint of a flammable liquid.
- Simplify the process design rather than adding additional equipment or features to deal with a problem. Only fitting complex systems and using multifaceted procedures if they are really necessary.

An example of inherent safety for powder operating systems could be that the material has been proved to be non flammable with the Group A/B Classification test, or an inert powder is added to the flammable dust, therefore decreasing its sensitivity to ignition sufficiently to allow safe operation of the processes.

Explosion Prevention

In order to prevent an explosion occurring it is necessary to either remove the flammable material or to remove oxygen from the atmosphere.

Parameter Group	Dusts/ Powders	Gases/ Vapors
Ignition Sensitivity	> Minimum Ignition Energy (MIE) > Minimum Ignition > Temperature (MIT) > Layer Ignition Temperature (LIT)	> Minimum Ignition Energy (MIE) > Autoignition Temperature (AIT)
Explosion Severity	> Maximum explosion pressure (P_{max}) > Explosion severity constant (K_{st})	> Maximum explosion pressure(P_{max}) > Explosion severity constant (K_g)
Flammable Range	> Minimum Explosible Concentration (MEC) > Limiting Oxygen Concentration for combustion (LOC)	> Upper and Lower Explosive Limits (UEL and LEL) > Minimum Oxygen for Combustion (MOC) > Flash point

Remove the Flammable Material

For dusts, this is difficult to achieve in the majority of cases, as dust tends to move from one place to another, forming layers which can then be regenerated into a dust cloud. Sometimes the **Minimum Explosible Concentration (MEC)** can be determined that shows that low concentrations of powder are not flammable and this can indicate, especially in the case of dust extract systems, that there is minimum risk of a dust cloud occurring. However, except for very extraneous cases, the MEC should not be used as the sole Basis of Safety as dust clouds are never totally homogeneous and can form slugs of powder that can create dust clouds within the flammable range. For gases and vapors it is possible to remove the flammable atmosphere by using local exhaust ventilation (LEV) to stay below the Lower Explosion Limit (LEL). As always it is necessary to ensure that the extract system operates efficiently and effectively at all times.

Remove the Oxygen from the Atmosphere

This is quite a common way of ensuring that a flammable atmosphere does not exist and is particularly useful in industries where not only other Bases of Safety are difficult to achieve, but also toxic materials may be present such as in the production of pharmaceuticals. As with all systems that use a specified value to ensure process safety, it is necessary to measure and monitor the oxygen levels within the process. It is also necessary to obtain the Limiting Oxygen Concentration (LOC) of the material being processed. The most common systems for ensuring an inert atmosphere is to use pressure-swing-inerting or flow-through-inerting. Some industries also use a vacuum as a technique to reduce oxygen levels. If Safety Instrumented Systems (SIS) are used to control the oxygen levels, from a safety point of view, it may be necessary to evaluate these systems. Please refer to Section 12 for more information on SIS.

Explosion Protection

This Basis of Safety assumes that there is a flammable atmosphere present and that there is a potential ignition source available to ignite the flammable atmosphere. The explosion is then handled in a safe manner using one of the following three methods: Pressure relief venting, flameless venting or supression systems.

Pressure Relief Venting

Where the explosion is released safely from the vessel using either prescribed, pressure relief panels or explosion relief doors, the relief venting normally has some form of ductwork attached to it, to ensure that the released explosion exits into an exclusion zone. It is also necessary to ensure that methods are employed to isolate the vessel if an explosion occurs. This type of protection has many advantages and disadvantages attached to it. On a positive side it is cheap to install and to maintain, working very effectively if properly designed and installed. On the negative side, many systems are badly designed resulting in equipment that is meant to be protected, having insufficient explosion strength to maintain its integrity after the explosion occurs. It also means that vented vessels need to be sited near an outside wall, and a considerable area has to be kept free from obstructions and personnel to prevent harm if the vent operates. If explosion doors are fitted, it is necessary to ensure that the doors do not fully close too quickly after the explosion or damage can occur due to a vacuum formed by the cooling gases. Explosion doors are often heavy and attached with hinges. This gives the door inertia which must be accounted for by increasing the vent area according to a certified efficiency. Under EU legislation all vent panels and explosion relief doors have to be type tested and certified suitable for use.

Flameless Venting

Is a by-product of venting whereby the system operates as a standard vent, but by extinguishing the flame and allowing the pressure to release. Special devices such as the “Q-Rohr” or “Flam-Quench” systems are attached to the explosion vent and can stop the propagation of flame, while still allowing venting of the pressure. However, efficiency is reduced compared to bursting discs, and they need to be type-tested as per the vents and doors specified above. This type of system, although being more expensive than standard relief panels, does give the option to position the vessel away from outside walls and technically allow venting into the room.

Suppression Systems

Can be installed where explosion relief venting is not an option. This can occur where a vessel is located away from an outside wall or where the process involves the use of toxic materials. The suppression system operates by using a pressure detector in the unit to identify a small but rapid increase in pressure as an explosion starts to build. An inert gas or powder is then injected into the vessel at high pressure and quenches the explosion before it has a chance to expand sufficiently to cause structural damage. The system can be set to ignore fluctuations in pressure created by process conditions. The advantages of suppression systems are that the equipment can be located anywhere within a facility and the system is particularly suited where toxic materials are produced. On the negative side, the suppression system must be designed and installed by a suitably qualified company and it can be expensive to maintain.

Containment of the Explosion

Is the final option where the actual vessel, and all ancillary pipework or ducting, is designed to be able to withstand the full effects of the explosion. At first sight this approach seems to be the best option, but it must be realized that the system has to be designed so that all parts of the process can withstand the maximum explosion pressure. The equipment also has to be suitably maintained so as to ensure the integrity of the equipment over its complete life cycle. In all of the above approaches to explosion protection, it is necessary to ensure that the vessel to be protected is isolated from the rest of the plant when the explosion occurs. In this way propagation of the fire or explosion, and the devastating effects of a secondary explosion, can be avoided. The advantages of containment systems are that there is no restriction on vessel location. The disadvantages are that they are often expensive, need isolation and expert maintenance.

8. Equipment Selection and Operation

All manufacturing processes require either a single piece of equipment or multiple pieces of equipment to complete the manufacture of a product. Equipment can constitute something as simple as an FIBC or day hopper, up to complicated chemical reactors. Within the EU, as stated previously, equipment being utilized in hazardous areas has to fulfill the requirements of both the ATEX directives, and in particular ATEX 95 which specifies clearly how each piece of equipment has to comply. This approach holds for both equipment manufactured within the EU, as well as equipment brought into the EU from such countries as Japan or America. Although the equipment may be certified as being acceptable for use, it is also necessary to ensure that it is installed correctly by suitably trained personnel.

Outside EU legislation, or within the EU, where equipment has been installed prior to the ATEX regulations coming into force, then equipment can be determined as being suitable for use by performing a detailed risk assessment. This risk assessment should consider the risk of generating sufficient ignition energy from mechanical, electrical and electrostatic sources to ignite the material being processed.

Along with the detailed risk assessment to determine the suitability of equipment for use, it is also necessary to ensure that the equipment is maintained in such a manner as to ensure that failure frequency of the process is kept to a minimum, and that the equipment continues to work as per the original manufacturer's instructions. Planned maintenance will help to ensure that, for example, leaks of flammable material do not occur, that ignition sources such as tramp metal or worn bearings do not occur, or that oil contamination which could affect the thermal characteristics of the material is prevented by regular, planned inspections of the equipment. Care must be taken when performing a maintenance operation as it may be necessary to shut down a particular piece of equipment within a process that may have a knock-on effect on other equipment that is located up or down stream of the equipment being repaired. Therefore, before any maintenance activity is started, it will be necessary to carry-out a hazard and risk assessment suitable for the maintenance activity being performed which should ideally be recorded. Maintenance should also be covered by operating procedures and a good level of training for technicians, supervisors and managers.

9. Thermal Instability

The majority of processes operate under normal temperature and pressure but sometimes it is necessary for a process to operate at high temperature, and in the case of some chemical reactions, this may include the necessity to keep a vessel under pressure.

Working at Elevated Temperature

The most common process working at elevated temperature is a drying operation that uses the higher temperature to remove solvent from the material being dried. This creates its own hazards and these hazards have to be considered carefully before commencement of any drying operation

Obviously the greatest hazard would be the potential for the material to self ignite due to thermal decomposition, or oxidation where burning embers or fire could be carried forward into down-stream equipment, which could result in a larger fire or even an explosion. Thermal decompositions can also generate permanent gas, and in some instances this could over pressurize the dryer if it is not vented adequately. Most thermal hazards associated with powders are due to oxidization which will be considered in this section, although chemical decomposition can also occur

To evaluate thermal stability, it is first necessary to identify the type of dryer being used. Typical dryers are not restricted to, but mostly fall into, the following categories:

- Spray dryers
- Fluid Bed dryers
- Tray dryers
- Vacuum dryers
- Flash dryers
- Rotating, drum dryers
- Filter Dryers
- Belt Dryers

It is probable that, for many dryers, there will be the potential to create an explosive atmosphere during normal operation, which would mean a classification of at least Zone 21 for dusts and a Zone 1 for any flammable gas or solvent vapor. In some circumstances even a Zone 20 or Zone 0 may be considered. Thermal decomposition can often generate intense heat or flame which could then provide an ignition source for the flammable atmosphere, but this will depend upon how the dryer is operated.

In order to determine whether there is the propensity for thermal activity to occur, it will be necessary to establish the thermal decomposition or oxidation onset temperature. This requires specific test data which should consider the type of dryer, the potential volume of powder deposits and air availability. Suitable safety factors need to be applied to the test results and these are dependent upon the type of test being performed. Testing requirements are provided in more detail in the 'DEKRA Process Safety Strategic Guide to Handling Dusts and Powders Safely.'

Thermal decomposition or oxidation can create burning embers, or even a full scale fire situation, that could then provide a potential source of ignition for dust or vapor clouds present within the dryer or downstream equipment. In addition, it is also necessary to have an understanding of how elevated temperature can affect ignition characteristics. For instance if the material being processed has a Minimum Ignition Energy (MIE) of 100 mJ at ambient temperature (21°C), then at 100°C this value can drop to below 10 mJ.

Along with the main dryer, there are often associated ancillaries such as cyclones, extract systems, dust filters, big bag filling stations or silos. In these situations the atmosphere may still be at an elevated temperature albeit at a lower temperature than the dryer itself. For equipment that has a high volume of product present, such as the dust filter or hoppers, big bags and silos, it will also be necessary to ensure safe storage temperatures and, if possible, safe residence times for any material being processed.

The accepted and most scalable experimental technique for determination of these properties is 'Basket' testing. This technique is again described in more detail in the 'DEKRA Process Safety Strategic Guide to Handling Dusts and Powders Safely'. An example of the extrapolation graph provided by this method of testing is illustrated in Figure 5 below.

As can be seen from Figure 5, as the size of the vessel increases, so the onset temperature decreases. This approach can be used for vessels of any volume, as long as suitable vessel dimensions (shape & size) are available to calculate surface area and volume.

Highly Energetic Materials

Some materials may undergo exothermic decomposition at a very high rate, often generating gas as a by-product. In extreme cases, the decomposition may be so rapid that the material (or mixture) is classified as explosive. In such cases, the sensitivity of the material to ignition should be assessed and understood such that these conditions can be avoided by organizational or technical measures. Explosives, as well as being initiated by elevated temperatures, can also be initiated by mechanical energy from friction or impact and the sensitivity to these potential ignition sources should be understood. Molecular examination of a compound or mixture can be sufficient to identify the potential for energetic decomposition.

For example, a compound containing a nitro functional group (-NO2) would be expected to show energetic decomposition potential – although the conditions required to initiate the activity can rarely be predicted.

If highly energetic materials are processed, safety would be normally based on prevention rather than protection. It is thus critical that the conditions required to initiate the activity are well understood, and that the process is assessed to ensure that such initiating mechanisms are identified and eliminated.

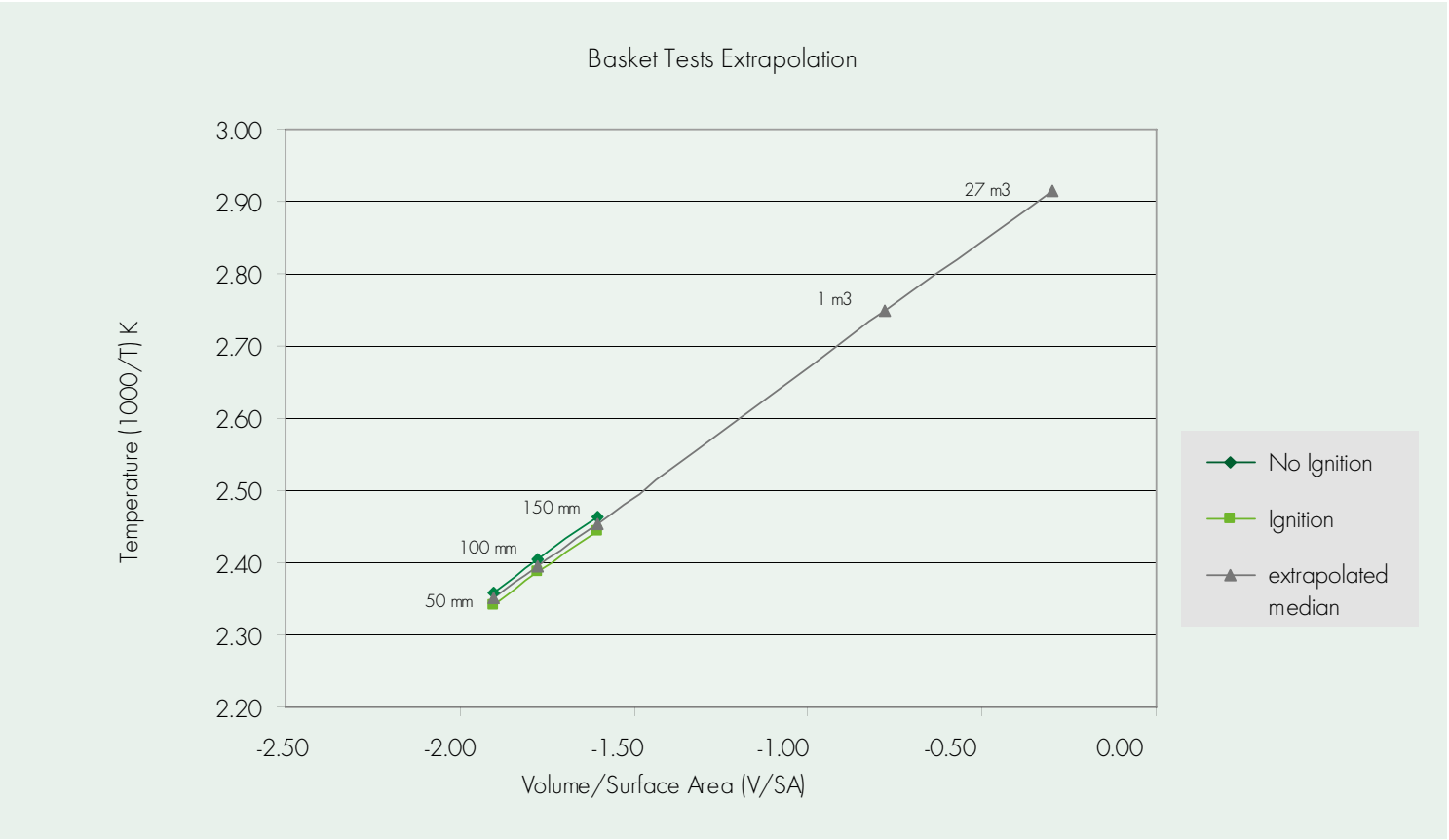


Figure 5. Estimated Onset Temperatures

10. Process Safety Worked Example

In Figure 6 illustrated below, a dust filter in a manufacturing operation handling combustible powders is reviewed using a simple hazard identification and risk assessment technique. The collector is part of a process that includes a high speed, hammer mill. The hazard is the flammable dust being collected from various inputs around the factory including areas where high energy equipment is located such as the hammer mill.

As the powder is stated as being 'flammable', then the first step is to identify the flammable characteristics of the powder, and to ascertain as to whether there are solvent vapors present. In this instance there are no flammable vapors being used and therefore it is just the flammable dust to consider.

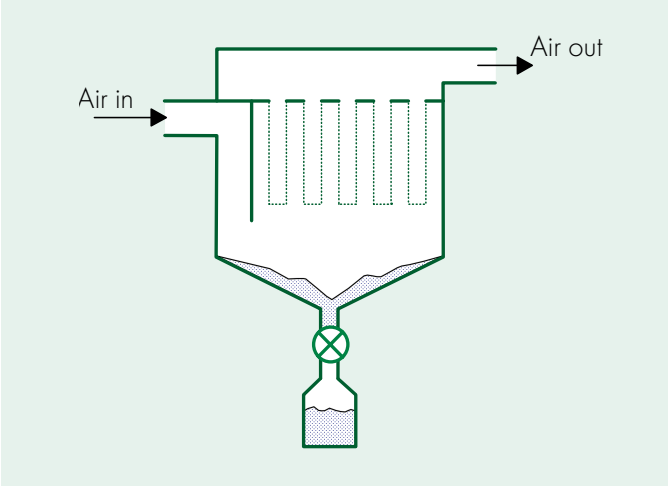


Figure 6. Schematic of Filter

Material Data

For the example given above there is actual, flammability data available (please see Table 2 below).

Please note that in the UK some HSE guidance state that the best place to find this information is on the Safety Data Sheet (SDS) supplied with the raw material. However, it is not a legal requirement to put this information on a SDS, and therefore it is not unusual to find it missing especially for dusts. There is also published literature on powders which gives generic values for many materials, but this data is often extremely old, may have been determined using out-of-date test techniques, and may not have the same physical characteristics as your material, e.g. particle size distribution. Therefore obtaining test data may be the only suitable and safe option.

As previously stated, to find out how to select the most suitable test, please refer to the 'DEKRA Process Safety Strategic Guide to Handling Dusts and Powders Safely'.

For gases and vapors, published data is perfectly acceptable as these figures have been proven to be correct over the years and are independent of changes in physical characteristics such as particle size. Greater care is needed with mixtures where expert advice is recommended.

We now know that the material is flammable and we have proven test data. The next step is to establish where a potentially flammable atmosphere could exist.

Flammable Locations

The dirty volume of the unit itself will contain a flammable atmosphere for most of the time that the system is running. This becomes even more apparent when reverse jet cleaning is in operation. Over time, very small particles might build up on the bag

Maximum Explosion Pressure, P_{max}	8.7 bar g
Dust Explosion Constant, K_{St}	185 bar m s^{-1}
Dust Explosion Class	St 1
Minimum Explosible Concentration, MEC	60 g m^{-3}
Minimum Ignition Energy, MIE	5 - 7 mJ
Layer IgnitionTemperature, LIT (5 mm)	180 °C
Minimum Ignition Temperature (Dust Cloud), MIT	390 °C
Burning Behavior, BZ (Combustibility Class, CC)	5

Table 2. Important Parameters for Characterizing Flammability Hazards

plate on the clean side. A leaking filter bag would cause a more drastic build-up of material on the clean side. If the extraction system is misused, eg. for "vacuuming" up dust, denser clouds of dust could then enter the system and cause local flammable atmospheres.

In the case of the dust filter, the main unit on the 'dirty side' has the potential to create an explosive atmosphere all of the time and is normally designated Zone 20. The collection bin is emptied regularly and always at the end of the batch process. This would therefore dictate a Zone 21 area as the potential for an explosive atmosphere to occur is only found during normal operation. The same applies to the input ducting. On the clean side of the filter there is the propensity for dust clouds to exist if a dust filter breaks or due to dust accumulation of fine particles. Therefore, Zone 22 may apply for this example in the exhaust ducting, which would extend through to the fan.

It is now established that there is a flammable atmosphere but how could it be ignited?

Potential Ignition Sources

Defining potential ignition sources is sometimes the most difficult step of a simple hazard and risk assessment, but is critical to establishing the correct Basis of Safety. In the case of the dust collector shown above, there may be a possibility of smouldering powder particles passing into the filter unit because of the nature of the upstream processes, in particular milling, finishing etc. In addition, there may be electrically powered sensors (e.g. pressure switches) installed in the ducts. The fan on the clean side would be a potential ignition source (in case of malfunction) and in the event of a filter bag failure.

The material is very sensitive to ignition by static electricity, and therefore isolated conductors could cause 'spark' discharges that may have the energy to ignite the dust cloud. Corona discharges or brush discharges from insulating materials could not ignite the dust cloud, but most other potential discharges could. Therefore electrostatic ignition sources cannot be ruled out.

To find out more about electrostatic hazards then please refer to 'DEKRA Process Safety Strategic Guide to Electrostatic Hazards and Applications'.

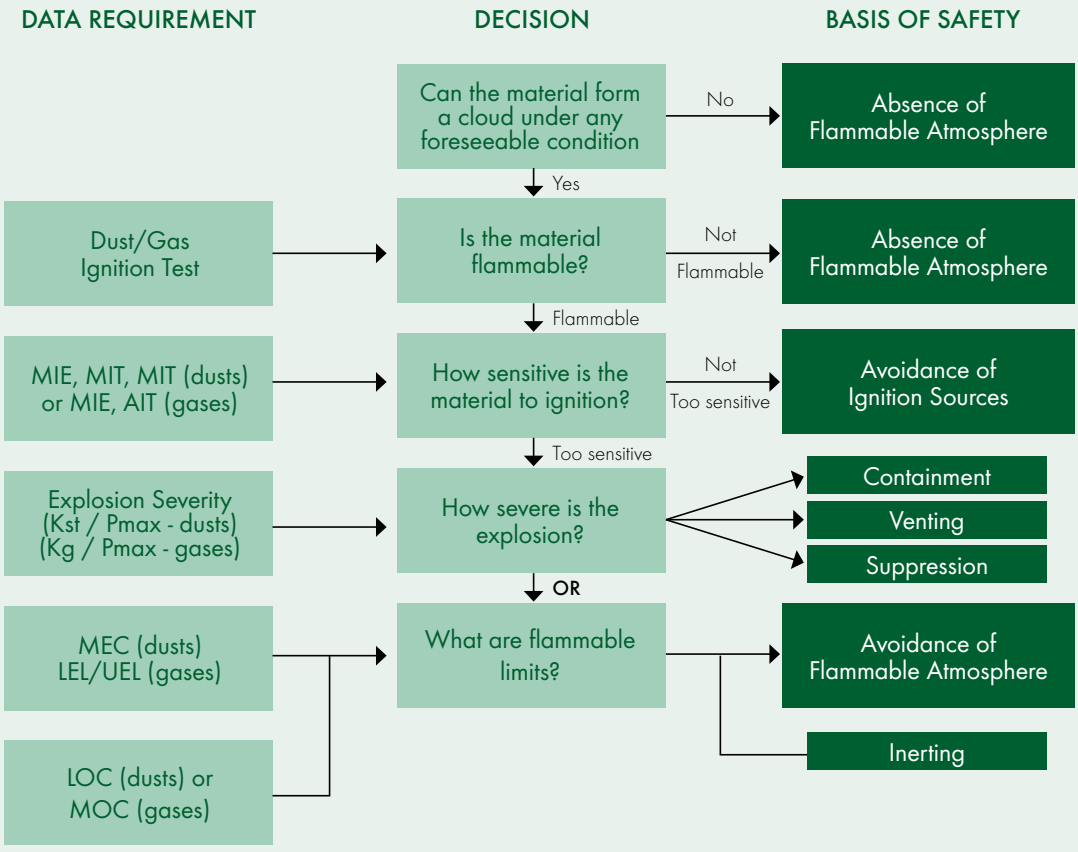


Figure 7. Basis of Safety

The flammability characteristics of the powder have been ascertained, the location of the flammable atmospheres has been established, and potential ignition sources have been determined. The final stage of the assessment is now to define a suitable Basis of Safety for the dust collector.

Basis of Safety

The final step in the assessment is to propose a suitable Basis of Safety for the Dust Collector and to determine whether further testing may be necessary.

By using the following methodology as illustrated in Figure 7 opposite, it is possible to determine the correct Basis of Safety from the available flammability data. If this data is not available, it is also possible to propose a suitable Basis of Safety and to then obtain suitable data to confirm it.

Please note that, although not necessary for this worked example, Figure 7 also includes the methodology for gases/vapor as well as dusts.

Therefore, for the example given above, most of the ignition sources can be effectively controlled. Company regulations and procedures should control hot work and naked flames on site. A detailed Hazardous Area Classification (HAC) has been carried out and appropriate equipment installed in and around the extraction system. Where electrical equipment installed within the filter unit complies with the appropriate electrical standards (probably Zone 20 which uses Group II, Cat. 1D equipment), it is not considered to be a source of ignition.

Elements such as the filter support cages are often fitted in such a way that they are not automatically earthed. This electrostatic hazard must be eliminated by the earthing and bonding of all conducting parts of the plant to eliminate the possibility of spark discharges from isolated conductors. The low value of the MIE makes it imperative that any earthing failure, even of relatively small items, must be avoided.

Ignition sources introduced into the extraction system from the extracted plant (e.g. smouldering material from the mill), are very difficult to prevent. In some cases it may be possible to fit a spark detection and extinguishing system. Whether this is an effective solution depends on the powder properties and the system layout. The high Burning Rate (BZ or CC) number means that any deposit that ignites will burn rapidly and spread to connecting equipment. A spark extinguishing system may not be able to handle this situation if there are deposits in the inlet ducting.

As the system is used for extraction and high volumes of air are handled, use of nitrogen inerting would be impractical. Dilution of the incoming gas would be occurring most of the time meaning that uneconomically large volumes of nitrogen would be consumed. As there is a small, but not negligible risk of an ignition, the Basis of Safety must include explosion protection.

As the filter unit is only built to withstand a pressure (Pdesign) of 0.4 bar g, containment would not be sufficient. In any case, if a stronger vessel were available, the isolation equipment required to protect upstream and downstream equipment would also have to take the maximum explosion pressure, and would be correspondingly more expensive.

Explosion venting of the dust handling unit would be possible provided the flame and products of combustion can be vented to a safe area. Upstream equipment would have to be protected against flame propagation and pressure effects by isolation devices. Downstream, the unit exhausts through the fan, and if damage to the fan can be tolerated, no isolation would be required here.

Suppression is generally possible on such systems, but a supplier of suppression equipment would have to be consulted on the suitability of this method. Again, isolation would also have to be considered. Suppression is often considered quite expensive in comparison with venting, and as venting of the explosion is a practical proposition, suppression would probably not be chosen. However, it is important to make any financial decision on the basis of the cost of the overall systems, including isolation measures and ongoing maintenance costs. If venting is selected,. then the explosion relief system would need to be designed correctly and vented to a safe area. Any ducting necessary to exhaust the explosion, would also have to be considered in any calculations. All of the Hazardous Area Classification information, hazard and risk assessments and the Basis of Safety have to be recorded in a detailed report.

11. Chemical Reaction Hazards

For runaway **chemical reaction hazards**, characterization of the hazard is provided through an understanding of the parameters detailed in Figure 8 (below).

The most common hazards associated with chemical reactions are those which cause elevated pressures inside reaction vessels (or other inadequately vented vessels). Exothermic reactions generate heat and, in the presence of a volatile liquid (e.g. solvent) can generate very high pressures associated with the volatile liquid. This normally happens when the reaction temperature rizes above the atmospheric boiling point of the solvent. It is wize to note that a reaction may be exothermic even if you have to heat the reaction mass initially to get the reaction started. As the temperature of a reaction increases so this can lead to a thermal runaway created by a linear loss of temperature (due to accepted heat loss conditions) but an exponential production of temperature due to the exothermic reaction. This is a situation where control of the vessel is lost and there is little time for correcting the situation. Therefore, the reaction vessel may be at risk from over-pressurization due to violent boiling or rapid gas generation. The elevated temperatures may initiate secondary, more hazardous runaways or decompositions. If either of these scenarios generates sufficient pressure and the vessel relief systems are inadequately sized to contend with the rapidity of the pressure rize, there is a risk of vessel rupture or uncontrolled release of flammable or toxic gas. Some of the largest incidents have been caused by runaway chemical reactions such as Seveso in Italy and Bhopal in India. An analysis of thermal runaways in the UK has indicated that most incidents occur because of:

- Inadequate understanding of the process chemistry and thermochemistry;
- Inadequate design for heat removal;
- Inadequate control systems and safety systems; and
- Inadequate operational procedures, including training.

Parameter Group	Thermal Instability / Runaway Reaction Hazards
Thermodynamics	Magnitude of heat release "Onset" temperature of activity
Kinetics	Rate of heat release and rate of change with temperature Catalytic impact of possible contaminants – including autocatalytic behavior
Pressure effects	Identification of gas generation (quantity and rate) and / or Identification of vapor pressure effects of principal components and secondary decomposition products

4. Important Parameters for Characterizing Runaway Reaction Hazards

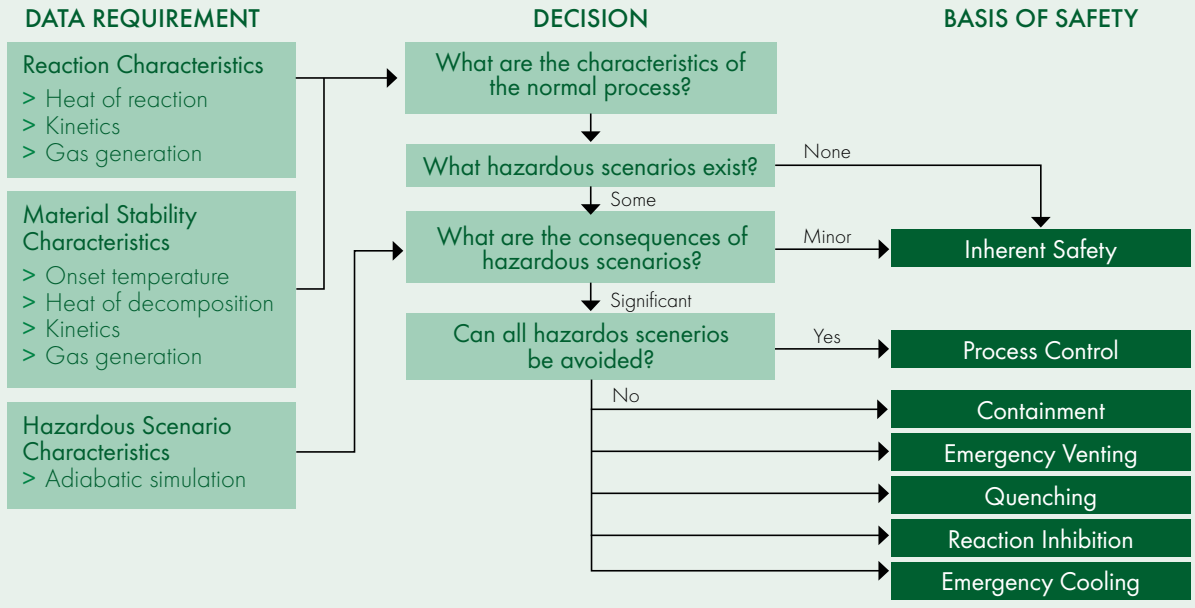


Figure 8. Decision Tree for Chemical Reaction Hazards

Type of Safety System	Specific Safety Measure
Passive - Prevention	Inherent safety
Passive - Protection	Venting Containment
Instrumented - Prevention	Process control
Instrumented - Protection	> Emergency (secondary) cooling > Quenching > Reaction inhibition

Table 5. Types of Safety System

This decision tree is shown in Figure 8 (opposite). and as per the fire and explosion assessments given previously, the Basis of Safety can only be properly formulated if sufficient test data is made available.

For thermal instability hazards, literature data may be available for common materials, whereas experimental testing will be required for proprietary materials or mixtures. For thermally unstable substances or mixtures, the conditions required to initiate the instability should be characterized. This may initially take the form of small scale screening tests such as Differential Scanning Calorimetry (DSC) or the Carius Tube test. These rapid and relatively crude tests provide a preliminary indication of onset conditions and the magnitude of the decomposition. If instability occurs at close to the plant's operating conditions, then more sensitive techniques may be required for detailed characterization (e.g. Accelerating Rate Calorimetry, ARC). Interpretation of the data from such tests requires a good understanding of the test sensitivity so that appropriate safety margins can be applied.

For exothermic chemical reaction processes, which have the potential to runaway, a good understanding of the thermodynamics, kinetics and gas generation / vapor pressure of the process provides a sound basis for evaluating the consequences of deviation from the specified process conditions.

Calorimetric techniques (typically employed for such measurements are often based on heat flow measurements under controlled laboratory conditions (for example, using the Mettler Toledo, RC1 system). Results from these investigations are used in combination with any thermal stability data to allow an understanding of the behavioral limits during foreseen deviations in the normal process.

There are a variety of safety measures that can be applied to runaway reaction hazards to prevent them occurring, or alternatively, protect against them, such as suitable control systems for material additions or monitoring systems for temperature and pressure. The safety systems need to be able to cope with the intended reaction and any foreseeable deviations. These measures can be passive (i.e. not instrumented and not requiring pneumatic or electrical activation) or instrumented (i.e. requiring pneumatic or electrical activation). If the latter approach is taken then, it may be necessary to look at the Safety Instrumented Systems (SIS) employed to ensure safe operation of the process. For more information on SIS please see Section 12.

Some of the more typical measures are summarized in Table 5, above.

Passive Systems

Looking at Passive Protection, one of the most common methods for handling runaway chemical reactions is to contain them by ensuring that the reactor is strong enough to withstand the maximum temperature and pressure that is evolved during the reaction. In order for containment to be effective, it is necessary to ensure that the vessel is completely isolated from any connecting pipework or ancillary vessels while the reaction is in progress. In order to ensure that the system remains effective throughout the life of the vessel, it is necessary to ensure that maintenance personnel have a thorough understanding of pressure containment systems as well as knowledge on the hazards of any materials being processed, their interactions and formation of waste products. It is also essential to ensure that procedures are in place that ensure equipment is maintained to it's original condition.

The other option for Passive Protection is to install a vent or more commonly called an Emergency Relief System (ERS). The purpose of the ERS is to release the pressure evolved from the runaway chemical reaction more rapidly than the pressure can build. Unlike dust explosion pressure relief systems, the ERS may not be allowed to vent to atmosphere as it may carry with it hazardous chemical waste, flammable or toxic gases.

Therefore, not only does the system have to cope with the release of pressure it also has to collect the waste products and handle the hazardous gases in such a way as to keep the system and surrounding areas safe.

The design of an ERS is a very specialized job and not only entails a good deal of knowledge concerning chemical reactions, but also an in depth understanding of the equipment and process conditions. It is widely accepted that the recognized approach to the design of the ERS is to use the Design Institute for Emergency Relief Systems (DIERS) methodology.

As stated above, an in depth understanding of the chemicals and process conditions must be available in order to apply DIERS, and this information can only be made available by using accepted test techniques.

Instrumented Systems

The second way forward is to use an instrumented approach. This would involve positioning various sensors such as temperature or pressure monitoring units at strategic locations in the process. When an inadvertent rize in temperature or pressure is monitored, then this would result in a stoppage of the system and a pre-planned cycle of actions to prevent the reaction running away. As stated before, it is extremely important to ensure that any SIS is properly designed and installed.

If instrumented prevention is not an option or forms only part of the safety approach then it may also be necessary to use instrumentation to protect the reaction. This could be in the form of emergency (secondary) cooling where circulation of a secondary working fluid through inner and/or jacket coils, or circulation of coolants such as liquid nitrogen through inner and/or jacket coils, are used to rapidly cool the overrunning reaction and so prevent it from reaching a runaway state.

Along with forced cooling, is the possibility to quench a reaction. This can be similar to a firefighter quenching a flame by dousing it with vast amounts of water. For chemical reactions this may equate to a reaction that includes an acid being quenched by the addition of a measured excess of an alkali to neutralize the acid.

One technique that is not so common, but can be applied, is to look at using a reaction inhibitor. This is a substance that decreases the rate of, or prevents, a chemical reaction occurring. This can be most effective when used in a catalysed reaction where the inhibitor can be added, which can be similar to (one of) the reactants.

However, the inhibitor is unable to undergo the reaction that the catalyst can facilitate, and when it is introduced into the vessel, the catalyst can no longer perform its job.

Finally, a point to remember is that each type of safety system has been covered as an independent method of prevention or protection. However, in practice it is not unusual to use different types of system to ensure the safety of a chemical reaction process.

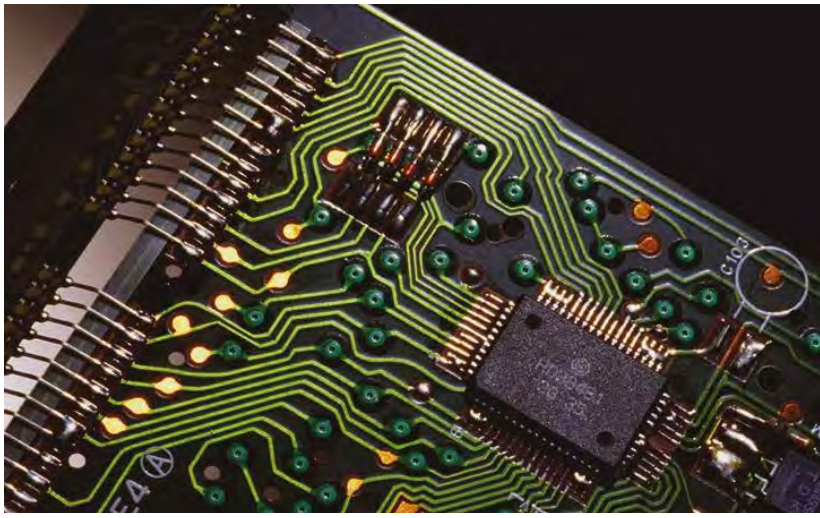
Although safety measures have been selected with care and installed correctly, they may not function as designed due to the ineffectiveness of the operators who may not have been instructed on how to react when an emergency situation occurs. Therefore, properly implemented management systems are paramount to the safe operation of any chemical reaction. Safe operating and emergency procedures, coupled with consultation with employees, is a necessary part in ensuring systems operate safely. It is also a requirement to train operators and supervisors to ensure that equipment is maintained correctly, and take control of any operational or equipment modifications. The subject of Process Safety Management (PSM) is dealt with in more detail under Section 17 of this guide.

For more detail on Chemical Reaction Hazards, refer to the 'DEKRA Process Safety Strategic Guide to Reaction Hazard Assessment'.

12. Safety Instrumented Systems (SIS)

Inherent safety is the ideal goal in process design, but this is difficult to achieve and is rarely given as the sole Basis of Safety for a manufacturing operation. Passive protection systems such as explosion relief venting, or pressure relief venting are often considered favorably against instrumented safety systems which are often complex, require evaluation and maintenance in operation. However, in many applications, and especially when considering complicated chemical reactions, there may be a requirement to use computer controlled, Safety Instrumented Systems (SIS) to ensure that the operation can be monitored and safely controlled to avoid catastrophic failure. For example when considering runaway reactions, it is common to use process control systems backed up with passive emergency venting systems, to safely relieve over-pressure. On the surface, this is a straightforward safety solution. However, such relief systems require detailed design, using best practice techniques (e.g. DIERS methodology) to account for multiphase flow, and almost always require provision of an adequate catch-tank or other environmental protection systems to contain the material ultimately relieved. The additional costs of such systems (in space as well as cost) can therefore impact on the desirability of this Basis of Safety. It must also be realized that some reactions are too violent for passive protection systems alone and must be prevented by using safety instrumented control systems for example.

As has been stated, the allocation of protection measures is a choice by the designer bearing in mind the characteristics of the hazard, the desirability and efficacy of the various options, the consequence of failure and the costs to install and maintain the systems. Where Safety Instrumented Systems are employed to control safety critical parameters, it is best practice to follow the principles laid down in IEC 61508 and IEC 61511, the latter being specific to the process industries. These international standards provide both a framework for assessing the required level to which a Safety Instrumented System (SIS) should be specified, and provide the instrument engineer with the methodology to build, operate and maintain an appropriate system – thus the standards encompass process safety and are not just instrumentation standards. The standards cover the entire lifecycle of safety instrumentation from assessment of the process risk through design, installation, commissioning, validation, operation, maintenance and decommissioning.
The first step in the application of IEC 61511 would typically follow on from HAZOP analysis and consequence studies and in many cases



use Layers of Protection Analysis (LOPA). This approach has recently found prominence in extending the hazard identification and risk assessment process, to demonstrate that a systematic assessment of multiple independent safety features achieves an acceptable level of safety.

If a specific safeguard is effective in preventing a hazardous scenario from reaching its consequence, and it is independent of the initiating event and other layers of protection, then it is considered to be an Independent Protection Layer (IPL). A combination of IPLs, general design features, procedural and other such layers are assessed to yield an overall credit or Layers of Protection.

A SIS performs specified functions to achieve or maintain a safe state of the process when unacceptable or dangerous process conditions are detected. Safety Instrumented Systems are often separate and independent from regular control systems but are composed of similar elements, including sensors, logic solvers etc.

The specified functions, or Safety Instrumented Functions (SIF) are implemented as part of an overall risk reduction strategy which is intended to reduce the likelihood of identified hazardous events. The outcome of any SIF is to ensure a 'safe state' for any process operation where the hazardous event cannot occur. The safe state should be achieved within one-half of the Process Safety Time. The Process Safety Time (PST) is comparable to the fault-tolerant time of a process, prior to it becoming a dangerous condition. Therefore, if a

dangerous condition exists for longer than the PST, the process enters a dangerous state. In order to maintain a 'safe state' it is necessary to detect any dangerous internal faults and correct them within the PST, or consequently the system should be considered unsuitable for safety applications on that process. Most SIFs are focused on preventing catastrophic incidents

In order to decide the acceptability of an identified risk it is necessary to consider the frequency of the initiating event, the assessed Risk Reduction or Probability of Failure on Demand (PFD), and the severity of the undesired consequence and to compare these against tolerable safety, environmental and commercial criteria. By analyzing the efficacy of the combined layers of protection against the risk acceptability criteria it can be decided whether there is a necessity to add additional layers.

Using either Risk Graphs or LOPA (discussed above), the magnitude and likelihood of the unprotected hazard would be assessed by a review team – only hazards deemed significant by the earlier studies would be taken into this analysis. Credit will then be assigned for traditional protective measures, possibility of avoidance or escape, and proportion of time exposed to the risk. By using these techniques it is possible to calibrate the identified risks against tolerable risk criteria for safety (e.g. Reducing Risks and Protecting People), environmental and commercial risk. The required integrity of the protection systems can then be determined which is principally the Safety Integrity Level (SIL) of the proposed Safety Instrumented System (SIS).

A Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).

Four SILs are defined, with SIL4 being the most dependable and SIL1 being the least dependable. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

By analyzing the efficacy of the combined layers of protection against the risk acceptability criteria it can be decided whether there is a necessity to add additional layers.

Using either Risk Graphs or LOPA (discussed above), the magnitude and likelihood of the unprotected hazard would be assessed by a review team – only hazards deemed significant by the earlier studies would be taken into this analysis. Credit will then be assigned for traditional protective measures, possibility of avoidance or escape, and proportion of time exposed to the risk. By using these techniques it is possible to calibrate the identified risks against tolerable risk criteria for safety (e.g. Reducing Risks and Protecting People), environmental and commercial risk. The required integrity of the protection systems can then be determined which is principally the Safety Integrity Level (SIL) of the proposed Safety Instrumented System (SIS).

A Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety function. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).

Four SILs are defined, with SIL4 being the most dependable and SIL1 being the least dependable. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

Safety Integrity Level (SIL)	Required Risk Reduction	Average Probability of Failure on Demand
1	10 to 100	0.01<PFDavg <0.1
2	100 to 1000	0.001<PFDavg <0.01
3	1000 to 10.000	0.0001<PFDavg <0.001
4	10.000 to 100.000	0.00001<PFDavg <0.0001

4. Important Parameters for Characterizing Runaway Reaction Hazards

13. Maintenance & Management

The majority of process safety focuses on the 'normal' operation of a plant. However, when any abnormal operation is performed and maintenance comes under this banner, as it is not part of normal process conditions, then a detailed risk assessment should be performed, specific to the maintenance operation. For many abnormal operations a risk assessment is required, such as;

- Before maintenance, repair, modification, extension, restructuring, demolition or cleaning where dangerous substances are being used
- Where equipment has contained dangerous substance and residue may remain
- When using any dangerous substance

The risk assessment must identify any fire or explosion hazards or chemical reaction hazard arizing from the proposed work. It is also necessary to ensure that control and mitigation measures are in place and take into consideration any appropriate system of work to ensure that measures are properly understood and implemented. Toxic releases or damage to the environment should also be covered but are not included in this guide.

Factors to consider when performing the risk assessment are the materials that are being used or may have been used (and still may be present in the equipment). These materials may also contain 'waste' products which need to be identified for hazardous properties. This assessment will identify any conditions where the materials may become dangerous through work. Consideration should also be given for any potential heat that may be generated or ignition sources that may occur and how and where explosive atmospheres can arize.

Always consider the consequences of fire or explosion or chemical runaway reactions during maintenance work and what is the proposed Basis of Safety during the maintenance operation. All personnel involved in the maintenance activity should have undergone training and show a suitable level of competence. It is probable that additional protective and emergency equipment will be required and that certain permits may be required such as for confined spaces or hot work etc.

14. Process Safety Lifecycle

Process safety should not just be considered when a hazardous situation has been realized or even worse when an incident has occurred. In order to ensure that Process Safety becomes an intricate part of any manufacturing operation it is necessary to consider it in all aspects of the Process Safety Lifecycles shown in Figure 9 below.

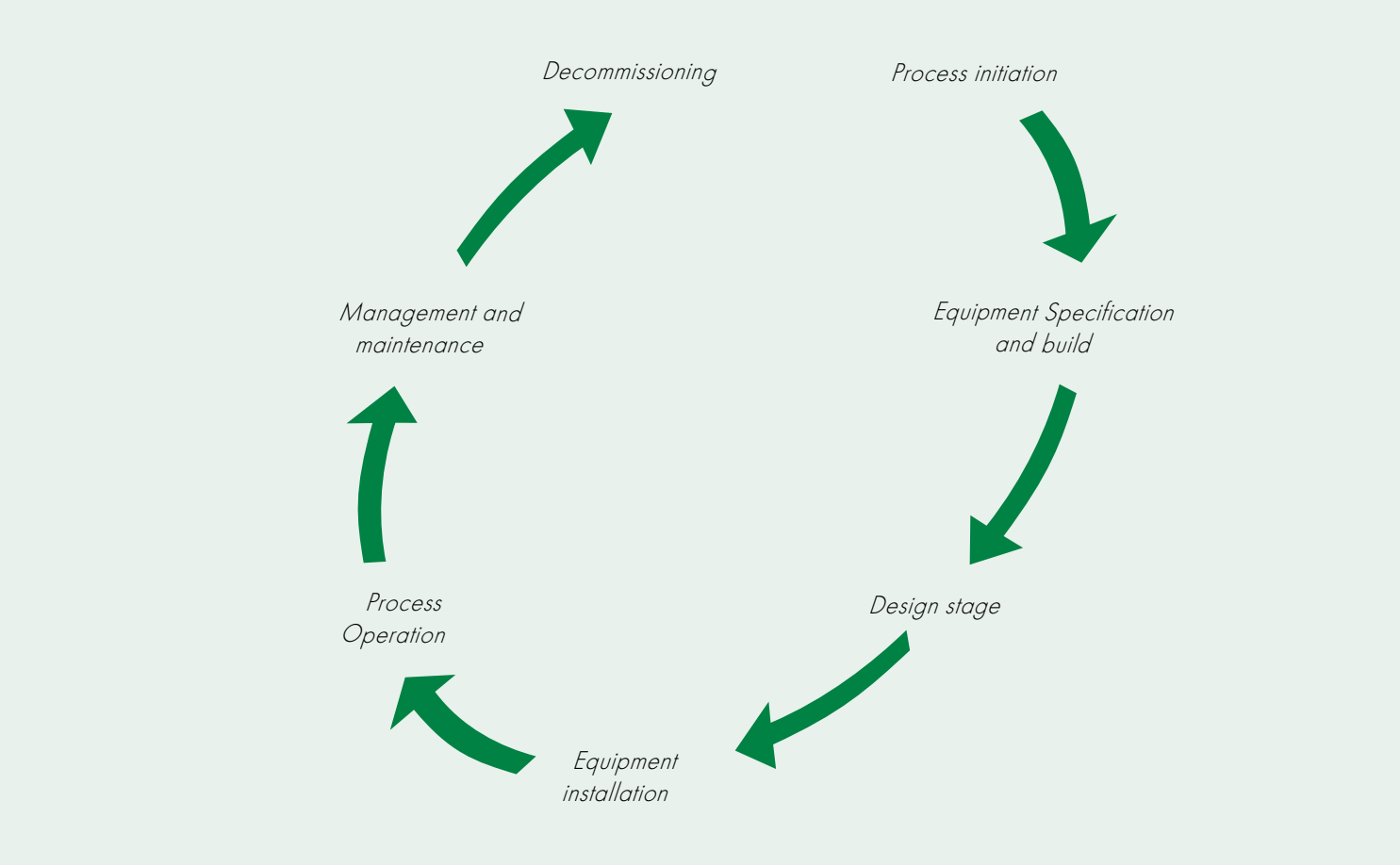


Figure 9. Process Safety Lifecycle

Project Initiation

When it has been decided that a new process has to be installed or new equipment purchased, then along with all the other accepted issues up for discussion, such as what type of equipment will be required, where it is to be installed and obviously the cost of purchasing and commissioning, process safety should come high on the agenda.

Initial Design

At this stage of the project there must be an understanding of how the materials are to be processed and a proposed Basis of Safety has to be put forward. Hazards and potential ignition sources should be considered and appropriate safety measures placed into the design. This may also include the necessity for Safety Instrumented Systems (SIS) to be considered. Where possible critical material data should be obtained to substantiate the proposed Basis of Safety.

Equipment Specification and Build

It is important to ensure that any Process Safety components are included within the equipment specification. For instance, explosion protection may have been entered into the initial design and it must now be incorporated into the build specification. If Explosion Prevention has been proposed by using inert gas to avoid the formation of a flammable atmosphere then this must be incorporated into the equipment specification. The same would apply for Safety Instrumented Systems.

Equipment Installation

Where the equipment is to be installed may also have a bearing on Process Safety aspects of the project. For instance, if explosion protection has been selected then the explosion relief panels will need to be fitted close to an outside wall or through a roof exit. Either way the ducting must ensure that all waste gases etc. are vented to a considered, safe area.

Process Operation

This is an integral part of Process Safety. The operating instructions should always incorporate the Process Safety functions of the equipment. For instance if Avoidance of Ignition Sources has been selected as the proposed Basis of Safety then it may be necessary to ensure that all plant and personnel are properly earthed at all times. The monitoring and control of inert gas blanketing may be paramount to the safe operation of a process. As well as written Safe Operating Procedures (SOPs) there may also be the necessity to provide training for personnel involved with the process so as to ensure a proper and detailed knowledge of how the process safety functions operate. Training may also need to incorporate knowledge of where the hazardous zones are located, why restrictive measures are in force and the need for specific PPE.

Personnel operating hazardous plant should also be trained in the correct action to take in an emergency.

Process Management

Once the equipment has been commissioned and is now in manufacturing mode, it will be necessary to manage and maintain the process. This will ensure that throughout the life cycle of the process it continues to operate safely and comply with the original Basis of Safety. During maintenance of the equipment it will also be necessary to ensure that risk assessments have been performed and that it is still possible to work safely with the equipment.

Decommissioning

Finally, when the equipment is deemed no longer suitable for production needs then it will need to be decommissioned. Throughout the decommissioning process it will be necessary to perform detailed risk assessments to ensure that no operation is performed that could be hazardous. This can also include the removal and disposal of waste material which in itself could be deemed as hazardous. As before, when the equipment was in the design stage, it may be prudent to obtain flammability data or chemical reaction hazard information on the waste material before removal is started.

15. Undesirable Events and Effects

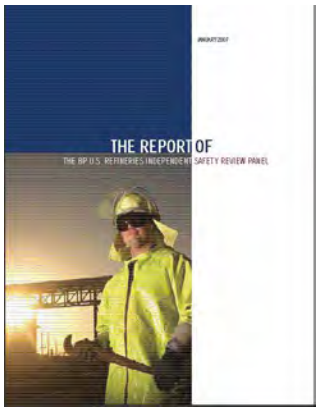
Even where no legislation exists such as that referenced in the first section of this Guide to Process Safety, it is always advisable to consider Process Safety. This may be incorporated into a company's own Health and Safety rules and regulations but as likely as not these will be focused more on personal and environmental aspects of safety.

However, if adequate process safety measures are not taken then an incident could occur. In some cases, the incident or undesirable event will not actually result in injury to personnel but it could result in severe property damage and impact business continuity. Consequently, the effect of the incident could be that major capital expenditure is necessary to restart the process. This expenditure may not only be due to the actual cost of the equipment and facilities that have been damaged but could also be caused by a long lead time for the equipment and therefore a long interruption in business production. Lost customers could ensue and this could ultimately lead to a decline in business over a sustained period of time.
More importantly than the material cost could be a total loss of image within the market sector or within the factory environment where a company has experienced a major incident and is now regarded as not being 'responsible'. This in turn could significantly damage the corporate reputation of a company as customers relate this failing to show responsibility with Process Safety with other responsibilities such as product quality or customer service.

Finally, when a major incident occurs then the effect is to draw the company to the attention of the regulatory authorities. This means that they, like the customers, will start to question whether this event is just the tip of the iceberg and further, deeper investigation may be more appropriate. Often the underlying result of any such investigation is that upper management of the company has not actually considered Process safety as part of it's responsibilities along with such items as production quotas and profit and loss analysis.

16. Process Safety Culture

As stated above an undesirable event may have significant effects on the operating success of a company after the event. In many cases an incident has occurred due to a lack of understanding of process safety or a poor Process Safety Culture (PSC) within an organization. How many times are signs situated at the entrances to factories stating the number of days without a lost time accident? This information can point to the fact that the focus is actually on personal or occupational safety and may not be considering the larger picture. The biggest hurdle that is often encountered is the infrequent happening of a Process Safety event unlike personal safety such as trips, slips and falls that may occur much more frequently but with generally low consequence of failure. This can result in a company having a false sense of security over the safety of their processes.



The Baker report

As stated by the Baker Panel report following on from the Texas City incident;

"the presence of an effective personal safety management system does not ensure the presence of an effective process safety management system." A good corporate process safety culture is demonstrated by the actual performance of the process safety management systems in the operating facilities, not by a filing cabinet full of standards and procedures, hazard studies, audit reports, and other documents. Systems and procedures are important and necessary, but they do not ensure effective process safety management."

The systems must be real and functioning, not just paper systems. Actions recommended by process safety reviews must be implemented, incident investigations must be used to improve the process rather than to assign blame, mechanical integrity inspections must be completed on time and corrective actions actually taken, training at all levels must be appropriate and up to date, operating procedures must be correct, up to date, and actually used.

Most importantly, management at all levels from the Board of Directors and CEO to the front line supervisor must demonstrate leadership for process safety at all times.

How do you recognize that PSC is taken seriously and what is the differences between Personal Safety and Process Safety?

Personal Safety

- Slips, Trips and Falls
- Often, low impact high frequency
- Does not require specialist knowledge to recognize, but does need training

Versus

Process Safety

- Reactivity hazards, overpressure, fire and explosion and toxicity
- Potentially catastrophic, low frequency
- Will require specialist knowledge and training

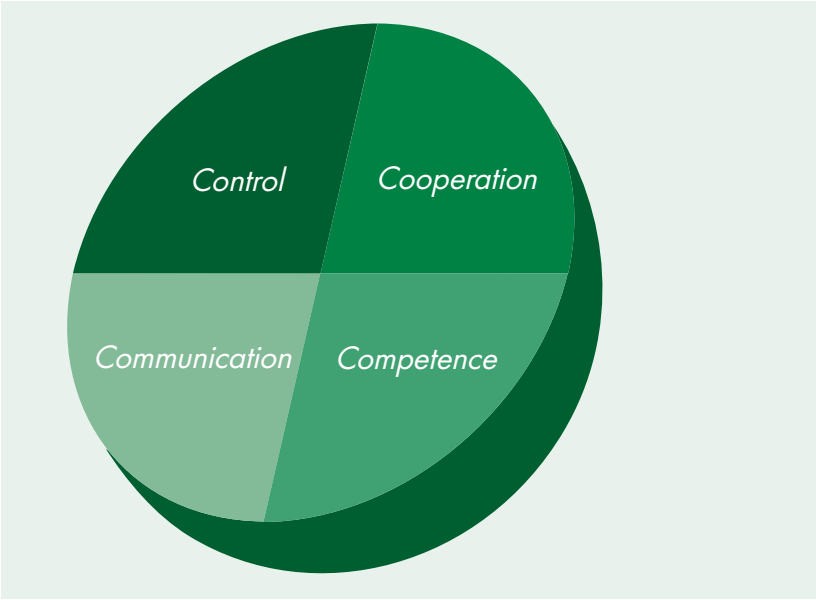


Figure 10. The Four Items for PSC

For PSC to operate effectively it is necessary to consider the 4 'C's; Therefore it is advisable to use the following systems and parameters

to achieve the PSC goal;
Engineering Design Practices and Standards

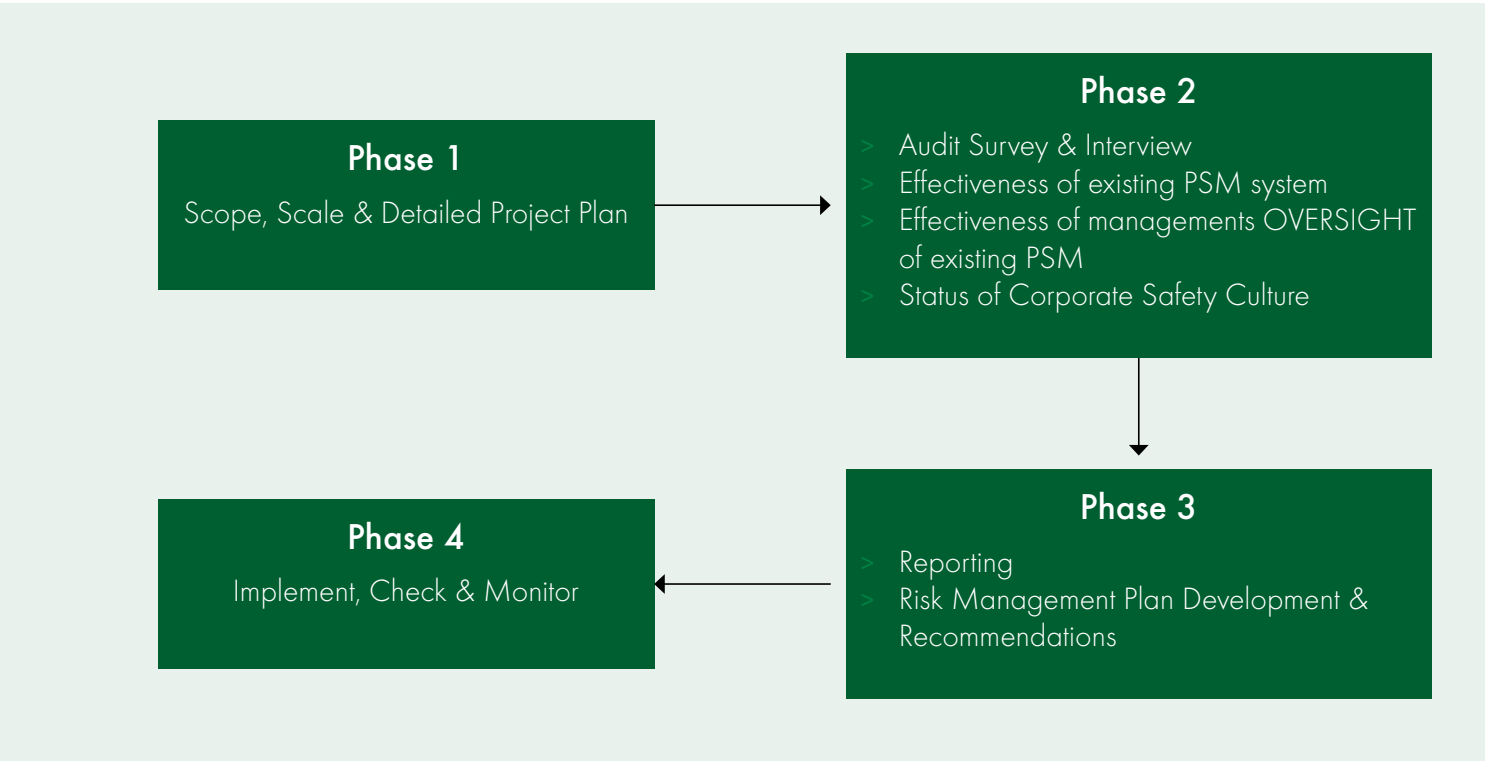
- What is done by Engineers
- Management Systems
- Procedures (R&D, Engineering, Design, Construction, Start-up, Operating conditions, Maintenance, Change, etc.)
- Safety Reviews
- Training / Awareness
- Equipment Inspections / Mechanical Integrity
- Contractor Process Safety Program
- Near Miss / Incident Investigations
- Performance Management / Measurement
- Audits / Site inspections
- Communication

It's how well an organization undertakes these systems and procedures that defines its PROCESS SAFETY CULTURE.

Another widely used description of safety culture, developed by the Advisory Committee on the Safety of Nuclear Installations (ACSNI) describes safety culture as:

"The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management." "Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures. "

DEKRA Process Safety has developed a 4 phase approach to how a company implements PSC within its organization.



11. Process Safety Culture - Management - Oversight

17. Process Safety Management (PSM)

In simple terms;

"...Process Safety Culture is how the organization behaves when no one is watching..."

One of the main components of PSC is the need to manage a process safely. A good, well implemented **Process Safety Management (PSM)** system should anticipate risks then reduce or eliminate the risk thus avoiding the unwanted event (or near miss). Elements of Process Safety Management can be based on the HSE publication HSG 65 which is reflected in the OSHA PSM standard 1910.119. The Centre for Chemical Process Safety (CCPS) has also published guidelines for risk based process safety and this covers PSM in detail. In the EU there is no actual equivalent legislation and PSM tends to be covered by COMAH / Seveso legislation. Although, such standards have particular relevance to COMAH/Seveso sites, the principles of process safety management should be replicated for any industrial process that handles hazardous materials. This includes any site that has to control flammability and/or CRH hazards mentioned previously.

In addition to expressing the duty holder's commitment to safe design and operation, compliance with legal requirements and the responsibility of employees for safe operation etc. a good policy statement, or supporting documentation, would indicate the organization's approach to process safety management.

- Principles of inherent safety
- A coherent approach to risk assessment – risk assessment methodology must be proportionate to the risk. Ref. Section 5.
- Communication of the hazard management process
- Ensuring competence, and adequacy of resources
- Working within a defined safe operating envelope
- Careful control of changes that could impact on process safety
- Maintaining up to date documentation
- Maintenance and verification of safety critical systems
- Line management monitoring of safety critical systems and procedures
- Independent audits of management and technical arrangements
- Investigation and analysis of incidents to establish root causes
- Reviewing process safety performance on a regular (e.g. annual) basis
- Continuous improvement, with regularly updated improvement plans
- Principles of quality management e.g. ISO 9000

Senior management should endorse the policy, which should be adequately communicated and commitment to it should be visibly demonstrated.

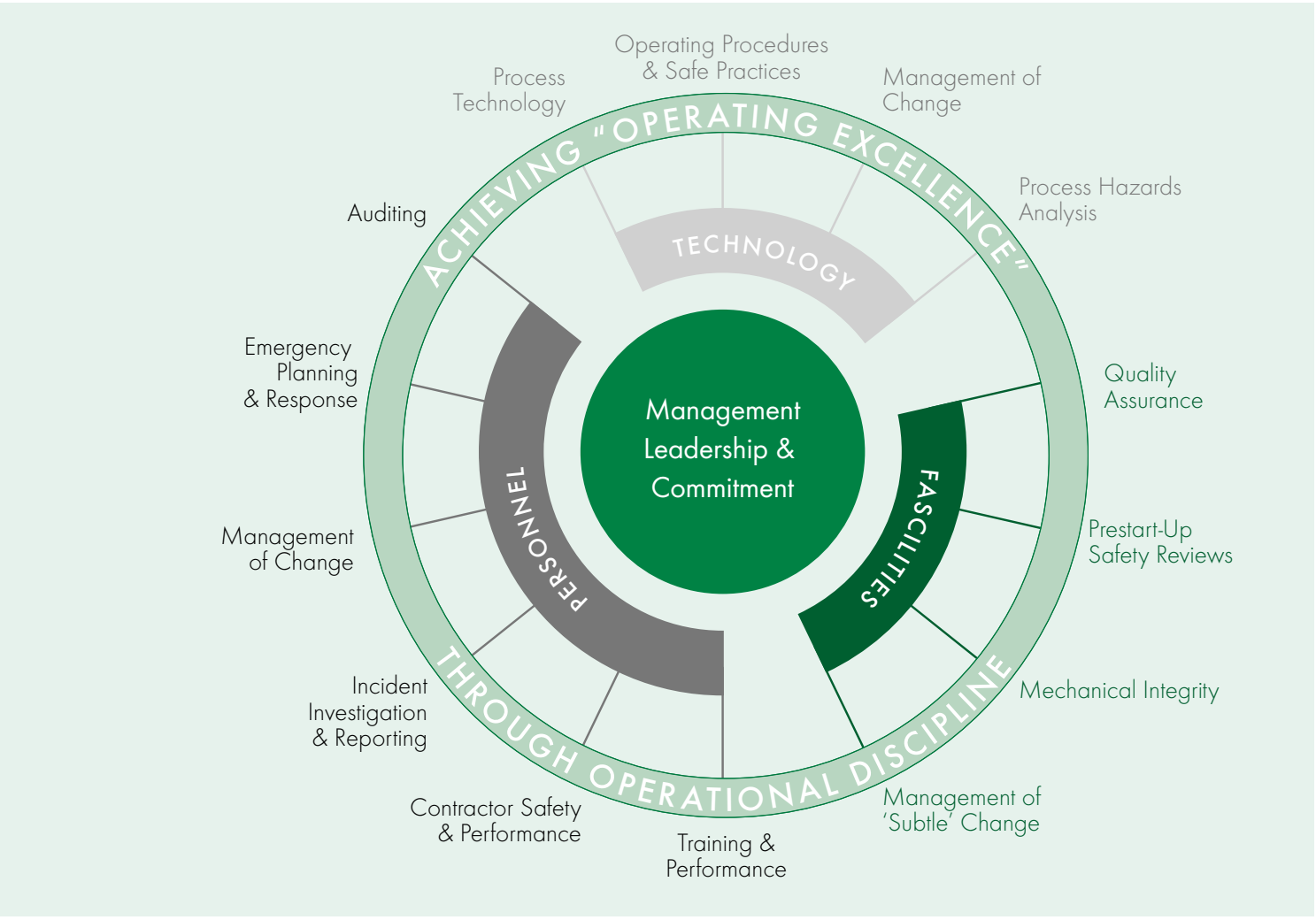


Figure 12. PSM

Successful PSM should cover all of the above areas of concern and the findings need to be documented. For detailed breakdown of the core ingredients to PSM/PSC please refer to DEKRA Process Safety Integrated approach to PSM Guide.

Auditing and Measuring Process Safety Management

It is almost impossible to measure the success of a program by "analyzing the events that never happened", however it is possible to assess the measures involved with the prevention of a catastrophic event. This leads us into the realm of assigning appropriate process safety performance indicators (PSPI) and also into the arena of PSM auditing. One of the important actions will be to identify the synergism between auditing and assigning PSPIs as an approach to effective control of a process safety management system.

The correct assignment of appropriate "Process Safety Performance Indicators" (PSPIs) can assist a company to identify when critical controls are not working effectively. However, in many cases, companies rely on auditing to solely highlight system faults. This results in a weakness in the auditing strategy where intervals between audits may be too long, thus allowing serious faults to develop in the interim or the focus of the audit may be to ensure that 'systems are in place', as opposed to reviewing the systems to determine if they are delivering the desired outcome.

Audits can be defined as 'the structured process of collecting independent information on the efficiency, effectiveness and reliability of the total process safety management system and drawing up plans for corrective action'. Audits are necessary to ensure that a companies' processes and procedures, as defined and carried out in practice, are consistent with the requirements of the Safety Management Systems and that they are seen to be effective.

All control systems tend to deteriorate over time or to become obsolete as a result of change. Therefore, audits should provide a check on the adequacy and effectiveness of the management procedures and risk control systems. Accordingly, audits need to be carried out by people who are sufficiently independent of operational management to ensure objectivity, yet technically competent to ensure the audit is focused in the correct areas. Moreover, it should be evident if the value of an auditing regime is limited by the technical competence of the Auditor/Auditing team. A simple example being a PSM audit which focuses on the management systems that are currently in place. An auditor may just look to determine if systems are in place and have been adopted. However, in order to determine the true 'Health Status' of the PSM there is a need to dig deeper than a system scan.

A competent Auditor should investigate further to determine the quality of the systems in place, to check if the correct technical criteria are implemented and determine if gaps are present using current best practice.

Benefits to Process Safety Performance Indicators – What is their real value?

Setting appropriate PSPIs can be beneficial by:

- Complementing Audits by providing more information on actual systems performance
- Reassuring that business risks are being controlled
- Providing early warning on critical control systems that have deteriorated, allowing for action before an incident occurs
- Helping identify reasons for process 'down time' which can improve business productivity and hence provide a monetary return
- Protecting the reputation of the company

PSPIs can be in a leading or lagging format.
Leading indicators involve active monitoring that provides focus on a few critical elements of a process safety management system to ensure its continued effectiveness. As such leading indicators are routine systematic checks, that 'key' actions or activities are undertaken as intended. Such process measurements should be related to process requirements which are essential to deliver a safe process outcome and as such are critical to ensuring process safety.

Lagging indicators are making use of reactive monitoring. Such indicators require the reporting and investigation of specific incidents and events to discover weaknesses in that system. The incidents do not have to result in major damage or injury or even to loss of containment providing that they represent a failure of a significant control system which guards against or limits the consequences of a major accident.

Performance management systems and indeed process safety management systems differ from organization to organization and as such the way Key Performance Indicators (KPIs) are used, similarly differs. However, it's important that new PSPIs are developed and integrated into the existing site arrangements for monitoring business performance.

As such PSM and the associated PSPIs must become an integral component whereby it is a seamless and critical part of business strategy.

Therefore, determination of the appropriate PSPIs is a very important component when establishing a proper PSM system as the choice of a few critical indicators can provide an overview of the risk control systems, thus providing a sufficient and representative overview of the sites performance. Also, avoiding KPI overload should be borne in mind, as it is not necessary to monitor every aspect/element of a process safety management system!

By utilizing a measuring and auditing approach as an integral component of a properly instigated PSM system it is possible to develop an effective process safety management system which results in fewer accidents, improved profitability, optimum reliability, decreased insurance costs and decreased expenses related to catastrophic incidents.

18. Summary

Process Safety is not just an action or legal requirement, but a way of life and an inbred culture. In order for it to work effectively, many actions have to be performed and incorporated into a manufacturing process from conception to decommission. Most importantly it is a live process whereby when any change occurs, no matter how small, the affected operation must be reassessed to ensure that the safety of the process is not compromized.

Identification of the hazard, understanding a material's hazardous properties, detailed risk assessments, the formation of a defined Basis of Safety and ensuring equipment is designed, selected and operated with process safety in mind, is paramount to its application.

The DEKRA Process Safety series of Process Safety Guides are useful tools in assisting anyone on their journey to achieve safer operating conditions for their staff and equipment. However always remember that a little bit of knowledge is a dangerous thing, and that these guides should always be combined with expert advice and assistance to ensure that people do not experience the unexpected.

'If there's anything worse than not doing something, it's doing something wrong and believing that it's right!'

DEKRA Process Safety

The breadth and depth of expertise in process safety makes us globally recognized specialists and trusted advisors. We help our clients to understand and evaluate their risks, and work together to develop pragmatic solutions. Our value-adding and practical approach integrates specialist process safety management, engineering and testing. We seek to educate and grow client competence to provide sustainable performance improvement. Partnering with our clients we combine technical expertise with a passion for life preservation, harm reduction and asset protection. As a part of the world's leading expert organization DEKRA, we are the global partner for a safe world.

Process Safety Management (PSM) Programs

- Design and creation of relevant PSM programs
- Support the implementation, monitoring, and sustainability of PSM programs
- Audit existing PSM programs, comparing with best practices around the world
- Correct and improve deficient programs

Process Safety Information/Data (Laboratory Testing)

- Flammability/combustibility properties of dusts, gases, vapors, mists, and hybrid atmospheres
- Chemical reaction hazards and chemical process optimization (reaction and adiabatic calorimetry RC1, ARC, VSP, Dewar)
- Thermal instability (DSC, DTA, and powder specific tests)
- Energetic materials, explosives, propellants, pyrotechnics to DOT, UN, etc. protocols
- Regulatory testing: REACH, UN, CLP, ADR, OSHA, DOT
- Electrostatic testing for powders, liquids, process equipment, liners, shoes, FIBCs

Specialist Consulting (Technical/Engineering)

- Dust, gas, and vapor flash fire and explosion hazards
- Electrostatic hazards, problems, and applications
- Reactive chemical, self-heating, and thermal instability hazards
- Hazardous area classification
- Mechanical equipment ignition risk assessment
- Transport & classification of dangerous goods

We have offices throughout North America, Europe, and Asia.
For more information, visit **www.dekra-process-safety.com**
To contact us: **process-safety-usa@dekra.com**

For assistance with interpretation and application of Process Safety issues, please feel free to contact us

Contact Us

DEKRA

DEKRA Process Safety
113 Campus Drive
Princeton, NJ 08540
USA

process-safety-usa@dekra.com
www.dekra-process-safety.com

Tel: +1 609 799 4449
Fax: +1 609 799 5559