Confidential to Members of EPSC Report Number 33

Safety Critical Measures

Safety Critical Measures

Author

Dirk Roosendans

Review

Richard Gowland
Charles Butcher

Any enquiries about this report, or other EPSC matters, should be addressed to Mr Lee Allford, Manager – EPSC Operations

Objectives of the European Process Safety Centre

1. Information
To provide advice on how to access safety information and whom to consult, what process safety databases exist and what information on current acceptable practices is available.

2. Research and Development
To collect European research and development needs and activities in the safety and loss prevention field, to inform members accordingly, to act as a catalyst in stimulating the required R&D and to provide independent advice to funding agencies priorities. "R&D" here includes experimental research and the development and review of models, techniques and software.

3. Legislation and Regulations
To provide technical and scientific background information in connection with European safety legislation and regulations, eg to legislative bodies and competent authorities.

4. Know How Exchange
To provide a platform for development of process safety knowledge for its members and to act as a focal point for dissemination of that knowledge to the European process safety community. Involvement in the Centre's groups gives organisations and individuals the opportunity to meet safety professionals from other companies to discuss areas of common interest and to share knowledge and experience, thus enabling informed comparisons of safety management systems and practice.

Benefits of Membership

- Improved cross-European co-ordination on safety standards
- Identification of areas where manuals and guidelines could be produced
- Improved co-ordination of safety R&D and handling of complex technical research programmes
- Stimulation of R&D in areas where there are gaps in knowledge
- Transfer of knowledge from elsewhere to Europe and between European countries
- Technical input to legislators and standard makers to ensure more realistic legislation
- Sharing and dissemination of information on safety technology and accident prevention
- Access to information from a single source

Contents

1. Introduction

A work group on Safety Critical Measures was created by the European Process Safety Centre in 2008. This document mirrors the discussions and reflections of this work group. The terms of reference of the work group can be found in Appendix I: Terms of Reference.

2. Background

Many major accidents in the process industries could have been avoided if prevention, mitigation and protection barriers had been properly designed and kept in good order. These barriers are often required because a full inherently safe process design is difficult to achieve, for both technical and economic reasons.

In the context of the control of major accidents (including multiple fatalities onsite or offsite), some of these barriers are called *Safety Critical Measures*.

Generally, a Safety Critical Measure can be defined as a measure with a beneficial effect on the scenario under consideration, such that if the measure was not present the scenario could present an unacceptable risk.

Safety Critical Measures are also characterised as (preventive, mitigating or protective) safety measures for which the integrity, availability, reliability and efficiency need to be guaranteed at all times because they have a key function in the control of major accidents.

Safety Critical Measures can be mechanical, instrumental or procedural. Safety Critical Measures can be either active or passive:

- **Active** systems need energy sources – which may be external or internal to the system - to perform their function. Without these energy sources, the active system will not function. Examples of external energy sources include electric power, pneumatic power, hydraulic power, manpower, and system pressure

- **Passive** systems do not rely on energy sources to perform their function. As a result they are generally more reliable than active systems.

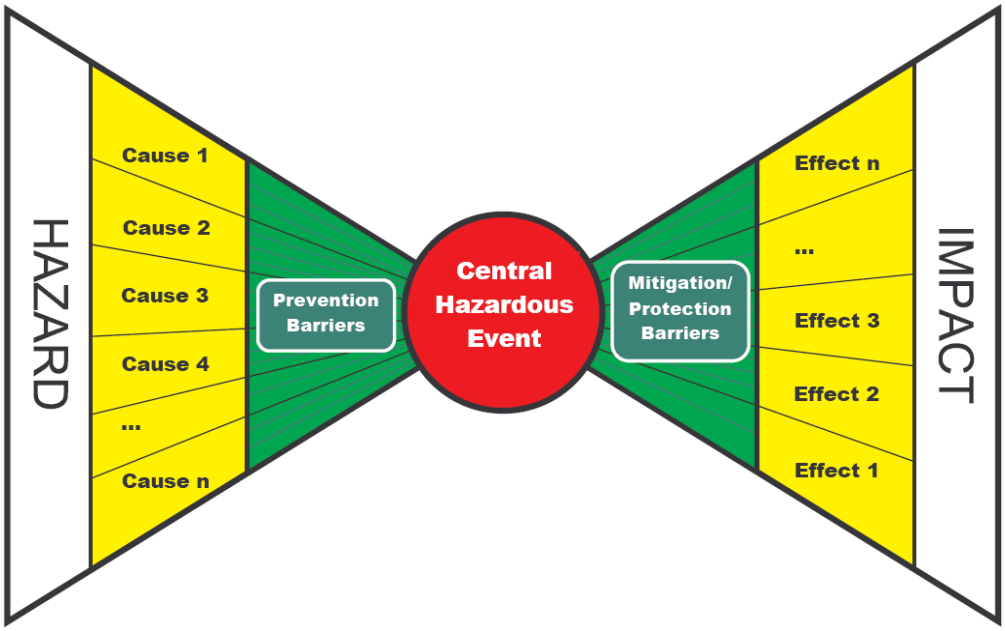
3. Context of Safety Critical Measures

3.1 Process Accident Scenario

The focus of this document is on major accident scenarios in processing and storage facilities. There is little emphasis on occupational accidents, even if many of the conclusions in this document may be equally relevant for the latter type of accidents.

A popular way to visualise process accident scenarios is the "bow tie" diagram (see Figure 1). In a bow tie, the initiating events or "causes" of many process accident scenarios converge to a "Central Hazardous Event" which can propagate to a number of different unwanted consequences. In this context a consequence is defined as the occurrence of physical effects resulting in damage to people or environment.

Figure 1: A bow tie diagram shows how a Central Hazardous Event typically has several causes (left) and several consequences (right)



For a given system (process system, utility system, storage system), initiating events include all possible deviations from a normal mode of operation. Initiating events include equipment failures, instrument failures and operating errors. For every Central Hazardous Event there may be several initiating events. Initiating events will propagate to a hazardous event if they are not stopped by preventive barriers.

The Central Hazardous Event is generally a release of a flammable or toxic substance or the release of energy. The Central Hazardous Event can propagate to several possible outcomes.

To avoid these possible undesired outcomes or render them less serious, safety barriers are installed to prevent the occurrence of the hazardous event, mitigate its effects, or protect the vulnerable environment (people, environment or assets):

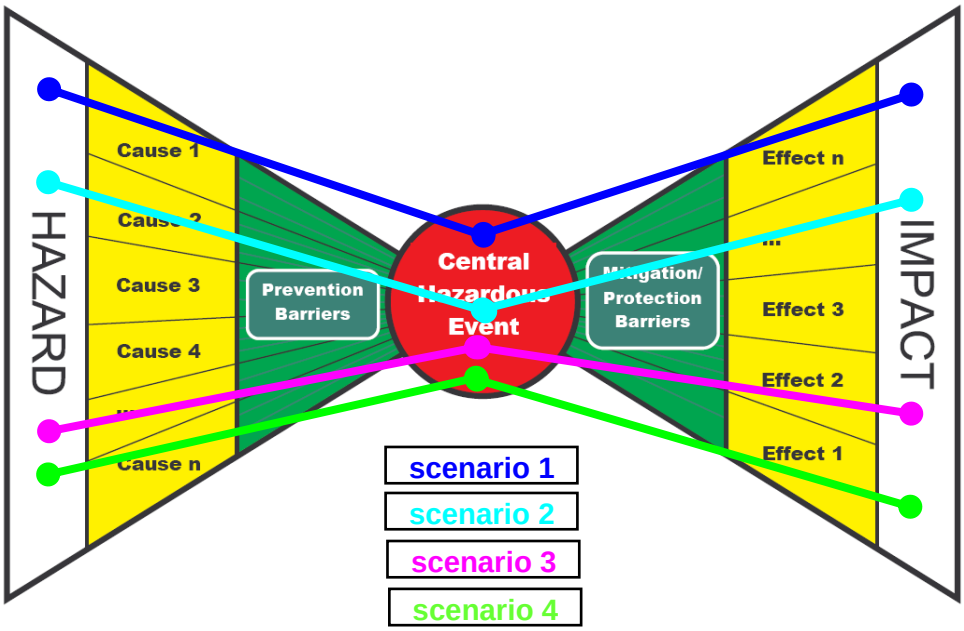
- Prevention barriers interrupt the propagation of initiating events towards the Central Hazardous Event
- Mitigation barriers reduce the extent or limit the effects of the Central Hazardous Event
- Protection barriers interrupt the propagation of physical effects capable of causing damage to people, environment or assets

Other factors which can influence the propagation of the Central Hazardous Event include conditional modifiers such as meteorological conditions, the presence of ignition sources and the presence of targets such as people.

Each of the paths in a bow tie, from a specific initiating event (or cause) to the Central Hazardous Event and from the Central Hazardous Event to a specific outcome, represents an individual process accident scenario.

Figure **2** shows individual process accident scenarios in a bow tie structure.

Figure 2: Examples of process accident scenarios in a bow tie structure



3.2 Scope of Safety Critical Measures

Some process accidents have the potential to cause very severe consequences. This potential is usually controlled by applying engineering controls (design, hardware, instrumentation,…) and operating controls (operating procedures, maintenance, inspection,…). The need for these controls or safety measures is usually identified during systematic and structured brainstorming sessions by a multidisciplinary team.

A basic principle applicable to all kinds of safety measures (including procedures, instrumentation and equipment) is that they need to be properly designed and regularly maintained and tested.

On any industrial site, *numerous* safety measures can be identified, each of which can play a decisive role in avoiding loss. From those numerous safety measures, *many* are necessary to avoid single-fatality accidents. From those many safety measures, only *some* will play a role in preventing major accidents.

Error-free management (including periodic testing and maintenance) of thousands of safety measures is difficult to achieve in a highly complex industrial environment. There is therefore a need to focus efforts and identify priority safety elements.

As a result, we can define two categories of safety measures:

Safety Measures: Any measure taken or required because of a safety concern.

Safety <u>Critical</u> Measures: A subset of safety measures that are required to avoid or control the impact of major accident scenarios

For a given Central Hazardous Event, we must assess all possible consequences before deciding whether Safety Critical Measures need to be identified. Various tools are available for consequence assessment, including sophisticated consequence modelling software.

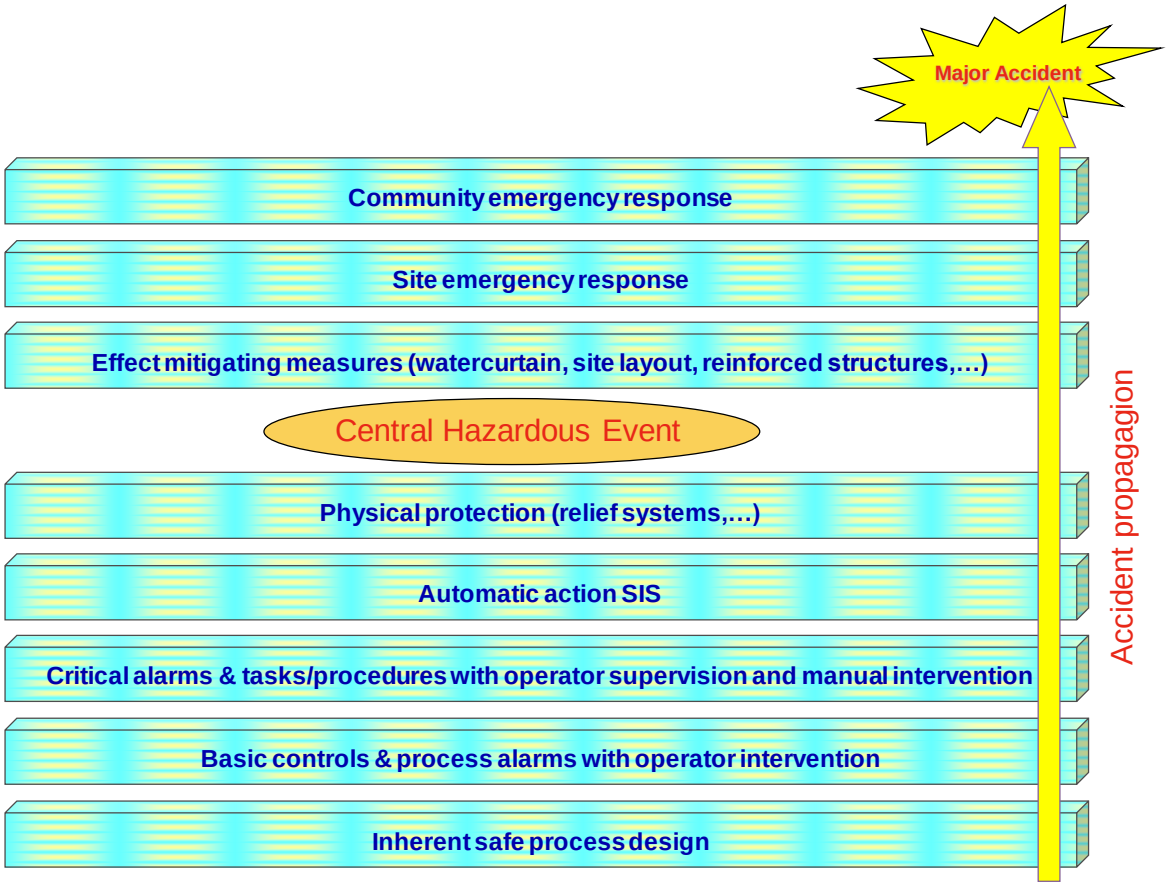
3.3 Protection Barriers

A process accident scenario – as illustrated in Figure 2 - can be defined as a sequence of events leading to the uncontrolled release of the hazard contained within a system, with unwanted consequences to people, the environment, or assets.

Hazards are usually controlled by applying engineering controls (design, hardware, instrumentation,…) and operating controls (operating procedures, maintenance, inspection,…).

Figure 3 shows some protection barriers that are frequently used to stop an initiating event propagating to unwanted consequences.

Figure 3 : Protection Barriers



The failure (or absence) of all of the above protection barriers means that the initiating event will be able to propagate to a major accident. Successful operation of one of the protective barriers will generally stop the accident sequence.

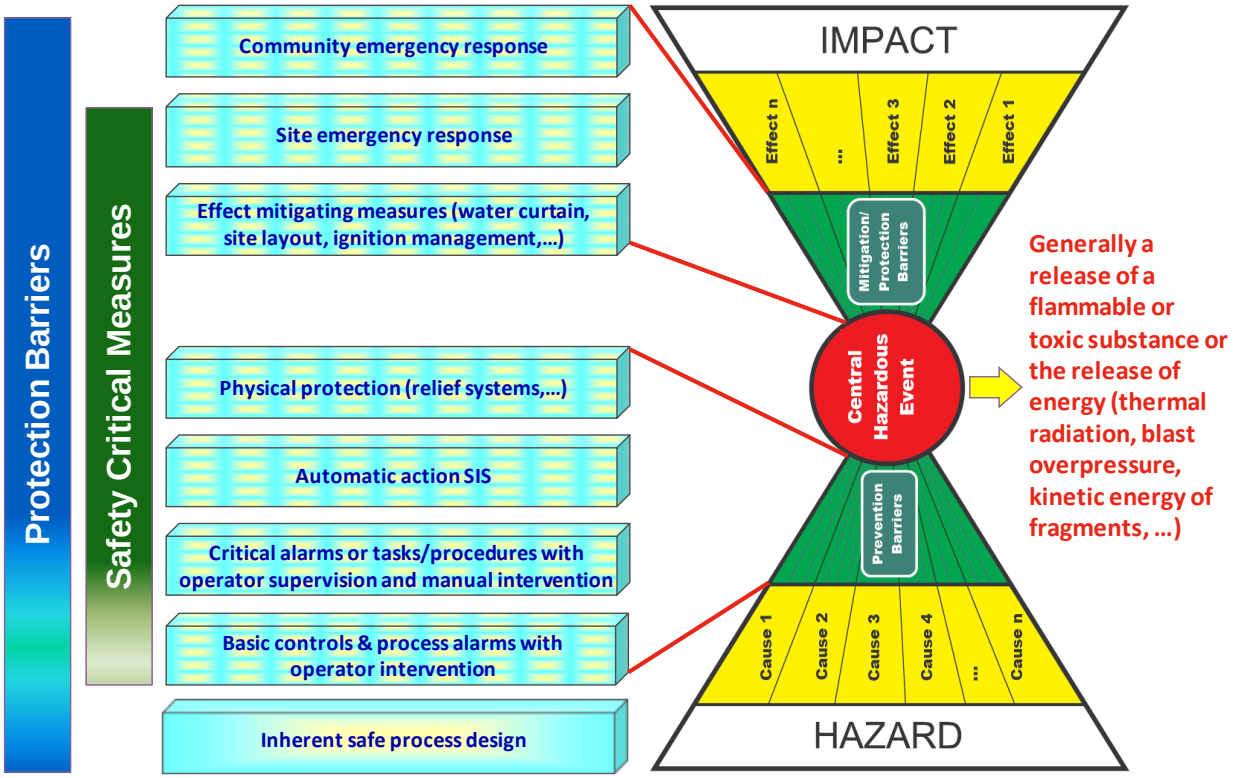
⚠ Not all of the above protection barriers are always present for every process accident scenario. Most scenarios include only some of these barriers.

3.4 Protection Barriers and Safety Critical Measures

Safety Critical Measures in general fall into the following types of protection barriers:

- Basic Process Control System (BPCS) trips and process alarms with operator intervention
- Critical alarms or tasks/procedures with operator supervision and manual intervention
- Automatic action by Safety Instrumented Systems (SIS)
- Physical protection systems such as pressure relief valves
- Mitigating measures (SIS, water curtain, site layout, ignition source management,…)
- Site emergency response

Figure 4 : Protection Barriers and the Bow Tie



Elements in the "Inherently safe process design" and "Community emergency response" categories are usually not known as Safety Critical Measures, although they are fundamental to the overall safety performance of a given process system. However, community emergency response may rely on Safety Critical Measures to function.

The effectiveness and efficiency of an emergency response plans depends on a large number of variables which are difficult to control (type of emergency, availability of

appropriate methods of response, location of emergency, escalation effects,…) and which are functions of the local environment and context.

Barriers requiring human intervention to become active may be disregarded as Safety Critical Measures because of the variability of human performance under stressful conditions. This does not mean that highly disciplined response to alarms is not required.

Procedures requiring human interaction can sometimes be considered Safety Critical Measures when there are *no other barriers* to avoid major accidents.

Often, more than one Safety Critical Measure is needed to reduce to acceptable levels the likelihood of a given accident scenario with major potential consequences. In this case, special attention should be given to possible *common mode failures* : we should verify that Safety Critical Measures are fully independent of other barriers and initiators. If this is not the case, estimates of risk reduction through multiple Safety Critical Measures may be too optimistic.

Some common mode aspects to consider are:

- Common operator
- Common power supply
- ESD signals handled by a single PLC without redundancy/diversity
- Common ageing
- Common maintenance
- Common fouling/blockage/dirt
- Common calibration of sensors
- Common factors at start-up or shut-down
- Multiple identical barriers (without diversity)
- Systematic failures (e.g. software, design)

More details on common mode failures can be found in the specialised literature (see references [12] to [16]).

4 Identification of Safety Critical Measures

There are several different approaches to identifying Safety Critical Measures:

4.1 Deterministic methods

Deterministic methods for the identification of Safety Critical Measures include:

- ✓ Technical standards:
- API
- ASME
- NFPA (e.g. NFPA30,...)
- DIN
- AD2000
- TRBF
- ✓ Company policy or procedures

Deterministic methods are usually based on experience.

4.2 Analytical methods

Analytical methods are usually based on brainstorming and other structured techniques. They may be purely qualitative, quantitative or semi-quantitative. Quantitative methods may be supported by internal or external databases of reliability and failure data.

4.2.1 Identification of Prevention Barriers

The basis of the decision to implement or modify safety systems is usually a high-quality hazard identification study. Hazard identification techniques include:

- Return of Experience (historical data)
- HAZID
- HAZOP
- HAZAN
- SWIFT (Structured What If Technique)
- FME(C)A (Failure Mode and Effect Analysis)
- ETA (Event Tree Analysis)
- Checklists
- Literature search

These can be used to identify appropriate prevention barriers. The quality of the identification process will depend mainly on the expertise of the people that conduct the analysis and less on the selected methodology.

4.2.2 Identification of Mitigation and Protection Barriers

Most major accidents in the chemical and petrochemical industries involve loss of containment of a flammable or toxic substance. Event trees can be used to analyse the possible consequences of such a release.

The following effects are usually included in these event trees:

- Pool fire
- Jet fire
- Flash fire
- Fireball
- Vapour cloud explosion
- Dispersion of toxic chemicals

Some of the following factors in the event trees can be used to identify possible mitigation and protection barriers:

1. *Duration* of the loss of containment, distinguishing instantaneous from continuous releases
2. *Nature of the substance* released, including the proportion which flashes as the pressure falls to ambient. When the substance is partially flashing, then both the liquid and vapour fractions have to be considered
3. Availability of *detection systems:* (including appropriate action by operators)
4. Availability of *leak limiting devices*: These include emergency shutdown systems, blowdown systems discharging to a flare or closed drum, and flow restriction orifices
5. *Time of ignition*: Ignition may be immediate, delayed or there may be no ignition at all. With immediate ignition, possible physical effects include pool fires, jet fires and fireballs. In the case of delayed ignition, possible physical effects include pool fires, jet fires, flash fires and vapour cloud explosions
6. Availability of *mitigating systems*: The effectiveness of existing mitigating systems will depend on the process accident scenario being considered. Examples of consequence mitigating systems include dykes to contain liquid releases, explosion suppression systems, water curtains and active fire fighting systems
7. Presence of *target objects*: The assessment of possible consequences does not stop with the determination of possible physical effects such as a fire or vapour cloud explosion. Instead, the consequence evaluation needs to include an assessment of the impact of possible physical effects on target objects considered. In many cases, these target objects will be people. If target objects are not present, then they cannot be harmed by any possible physical effects
8. Availability of *protection systems*: Sometimes target objects are protected against possible physical effects. Examples of protection systems include reinforced buildings and passive fire protection (if the target objects are assets). As for mitigating systems, the effectiveness of protection systems will depend on the process accident scenario being considered (e.g. passive fire

protection may be effective against fires but not against the blast overpressure of a vapour cloud explosion)

9. **Process safety time and reaction time**: The process safety time is the period from the time a fault occurs in the process to the time that the process enters a dangerous state. Following a demand (process error) the safety system needs to transfer the process to a safe state within the process safety time. The reaction time of the safety system, which is the sum of the reaction times of the sensor, actuator, and safety controller, needs to be shorter than the process safety time

Other factors that may influence the outcome of the event tree are:

1. **Congestion or confinement:** A cloud of flammable vapour that has not yet found an ignition source can move and accumulate in congested or confined areas. When the vapour does ignite, the result can be a vapour cloud explosion. In the absence of physical confinement or congestion, on the other hand, the vapour cloud will usually burn as a flash fire without generating significant overpressure
2. **Weather:** Meteorological conditions including wind speed, wind direction, atmospheric stability, humidity and ambient temperature can significantly affect how vapour clouds disperse

4.2.3 Assessing the Need for Safety Critical Measures

Analytical methods imply the use of criteria to decide the need for Safety Critical Measures. These decision criteria are usually a combination of the severity and probability of the potential outcome of the hazardous event under consideration.

Appendix II gives examples of some analytical methods together with their decision criteria.

5 Selection of Safety Critical Measures

5.1 General Selection Principles

Some possible general principles for the selection of Safety Critical Measures are outlined below:

5.1.1 Nature of Safety Critical Measures

Safety Critical Measures can be part of the *preventive*, *mitigating* or *protective* safety barriers that are or should be installed to reduce the probability or potential consequences of the scenario under consideration.

5.1.2 Priority rules for Safety Critical Measures

If more than one Safety Critical Measure can be identified for the same accident scenario, then the choice of the safety measures to be designated as Safety Critical Measures may be based on the following principles:

- Preventive barriers have priority over mitigating and protective barriers
- Within each category of safety barriers (preventive, mitigating, protective), the safety barriers with the highest (in order of decreasing importance) reliability/availability/maintainability have priority
- Passive safety barriers have priority over active safety barriers
- Multiple independent barriers may be preferred to a single barrier with the same PFD

For example: two independent barriers each with a PFD of 0.1 may be preferred to a single barrier with a PFD of 0.01

5.1.3 Independence of Safety Critical Measures

Safety Critical Measures are systems or procedures that are usually part of one of the following protection layers:

- BPCS trips
- Process alarms with operator intervention
- Critical alarms or tasks/procedures with operator supervision and manual intervention
- Automatically acting Safety Instrumented Systems (SIS)
- Physical protection systems such as relief valves
- Mitigating measures (SIS, water curtain, site layout, ignition source management,…)
- Site emergency response

If more than one Preventive Safety Critical Measure can be identified for the same accident scenario, then priority may be given to the Safety Critical Measure with the best performance in the following areas: reliability, efficiency, response time, testability, maintainability, availability, fault tolerance. Avoidance of false trips is part of this assessment.

6 Design of Safety Critical Measures

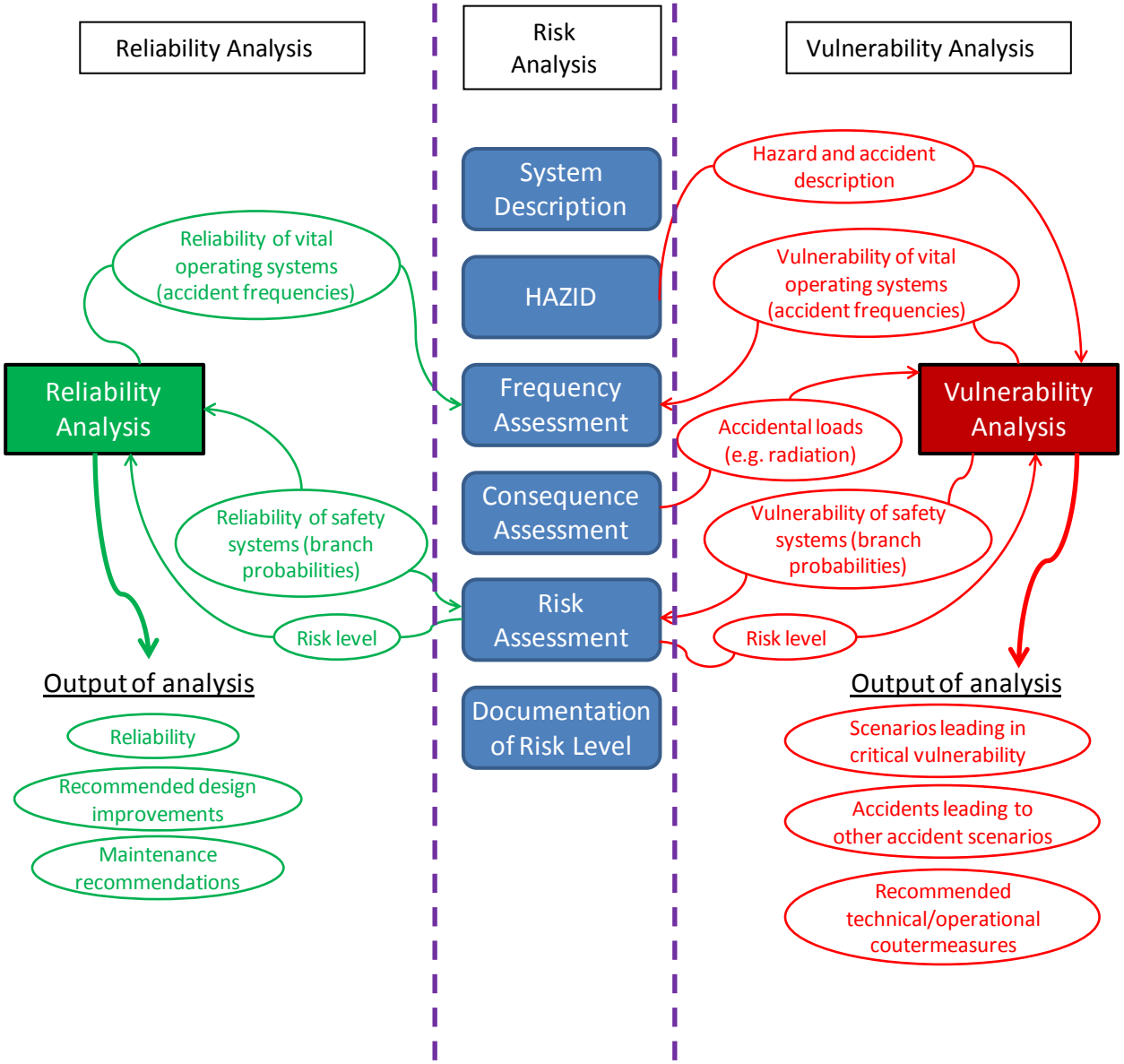
In the design of Safety Critical Measures, some aspects deserve special attention. These include:

- Selectivity
- Independence
- Reliability
- Relevance
- Efficiency
- Response time
- Testability
- Maintainability
- Availability
- Fault tolerance
- Vulnerability
- Diversity (different technologies or measured variables)

As mentioned above, Safety Critical Measures may take the form of equipment, instrumentation or procedures.

Figure 5 shows the relationship between risk analysis, reliability analysis and vulnerability analysis. The central part of the diagram shows the general structure of a risk analysis. During a risk analysis, the need for preventive, mitigating or protective safety measures is identified. The performance of these safety measures is usually assessed in a RAM (Reliability, Availability, Maintainability) study. However, the performance of safety measures may also be affected by accidental loads (heat radiation, blast overpressure, impact of debris,…). The impact of accidental loads on the operability of safety measures is assessed in a vulnerability analysis.

Figure 5 : Vulnerability Analysis of Safety Critical Measures



7 Management of Safety Critical Measures

7.1 General Principles for Testing, Maintenance and Availability

7.1.1 Testing of Safety Critical Measures

- Safety Critical Measures need to be testable when this is physically possible. A rupture disc is an example of a safety measure that cannot be tested
- Test intervals for Safety Critical Measures need to be clearly defined. The frequency of testing needs to be defined in agreement with the required PFD for the Safety Critical Measure under consideration
- **Testing of the operability of a Safety Critical Measure should not be based simply on tests of its individual components. Instead, the complete function of the Safety Critical Measure, including all components in the loop, should be included in a single test when this is physically possible**
- The test status of Safety Critical Measures should be clearly displayed in the control room
- Testing of Safety Critical Measures must be performed by competent people
- A list of non-conformities found during testing of Safety Critical Measures needs to be developed for all Safety Critical Measures
- A formal test procedure needs to be developed for all Safety Critical Measures

7.1.2 Maintenance of Safety Critical Measures

- Safety Critical Measures need to be maintainable, when physically possible
- Maintenance on Safety Critical Measures should be avoided while the system is online unless the availability of the Safety Critical Measure is already significantly reduced
- Maintenance of Safety Critical Measures should be driven by formal maintenance schemes and not by informal or uncontrolled judgement
- Good practice should allow the status of maintenance for Safety Critical Measures to be distinguishable from that of other non-critical maintenance to facilitate monitoring. Work priorities should take account of the criticality of the affected part of the plant. There should be an effective system to manage and close out issues relating to Safety Critical Measures
- The status of the maintenance of Safety Critical Measures should be clearly displayed in the control room
- Action monitoring should ensure that actions are completed and issues addressed with an urgency proportionate to the risk. Delays in the close out of actions related to Safety Critical Measures should be recorded and justified, with a periodic review of completion targets. Maintenance systems should clearly show the status of critical items and highlight any that are overdue

7.1.3 Availability of Safety Critical Measures

- All Safety Critical Measures need to be available for at least 99% of time
- The availability of Safety Critical Measures should not be reduced unless absolutely necessary
- If a Safety Critical Measure is unavailable, equivalent compensating measures should be put in place
- The status of the availability of Safety Critical Measures should be recorded. The list of *unavailable* SCMs shall be clearly displayed in the control room to ensure that operators know the exact status of each SCM
- Before inhibiting any SCM, a formal risk analysis shall be performed. This must include the definition of the compensating measures to be applied and the maximum delay allowed before returning to normal
- When an SCM is inhibited, a return to full serviceability should be expedited without delay. Audit mechanisms should ensure that the existence and duration of inhibits on safety critical components are not overlooked

7.2 General Principles for Managing Safety Critical Measures

The life cycle of any plant contains a number of phases that are especially appropriate to the introduction and operation of Safety Critical Measures. These are typically:

1. Initial design and modifications
2. Construction and commissioning
3. Operation
4. Maintenance, inspection and testing

For each life cycle phase involving Safety Critical Measures, key management tasks are:

1. Knowledge of the risks
2. Use of standards
3. Control of conflicts between safety and production
4. Formal safety studies
5. Safe procedures
6. Competent and sufficient personnel
7. Management of the human factor
8. Supervision and checking
9. Capturing experience

For every life cycle phase, the responsibilities for each of the above management tasks need to be clearly and unambiguously defined and communicated throughout the organisation.

7.2.1 Knowledge of the Risks at Each Life Cycle Phase

A system needs to be in place to deliver knowledge and awareness of hazards, such as the dangers associated with a particular substance, design, process or action and the knowledge of how to control hazards within each life cycle phase. This also includes knowledge of the behaviour of Safety Critical Measures both during normal operation and under upset conditions, and how the Safety Critical Measures interact with the process.

7.2.2 Standards

Standards provide systematic ways of preventing and controlling major accidents such that they are accepted as representing good or best practice. Examples include company standards, European standards, industry standards, and other such as:

- legal requirements
- design codes
- standards setting out frequencies for maintenance, testing and inspection
- standard operating procedures
- special standards for a particular process or hazard

7.2.3 Control of Safety-Production Conflicts

Production and economic pressures often conflict with safety rather than supporting it. This can lead to short cuts, omissions, inattention to safety matters, and delays in carrying out safety-related tasks. It is therefore important to manage these conflicts and to prioritise safety in relation to production and other conflicting goals.

7.2.4 Formal Safety Studies

The management system must provide for formal studies which systematically analyse the dangers, the possible scenarios, their control, and severity of consequences. The system should form a basis for understanding the major accident risks and enable risk reduction measures to be targeted. Methods include process safety studies, HAZOP, QRA, and task analysis.

7.2.5 Safe Procedures

Operating, maintenance and emergency procedures should ensure, rather than compromise, the safety of the plant and the people working on it.

7.2.6 Competent and Sufficient Personnel

There should be a system to ensure a supply of people competent in the tasks which relate to the prevention and control of major accidents. This also means there should be sufficient skills available and sufficient members to manage the workload associated with those tasks.

7.2.7 Management of the Human Factor

Management systems must recognise the potential for human errors, such as omissions or doing something incorrectly, set out the ways in which these might arise, and ensure that they are controlled. This includes ergonomic factors such as man-machine interface and other factors influencing human performance.

7.2.8 Supervision and Checking

It is not enough to have in place procedures relating to Safety Critical Measures. These procedures must also be implemented effectively. Monitoring is an essential step in preventing accidents through encouragement and feedback or positive achievement – but only if it is sufficient, targeted and adequately penetrating. Once implemented, it is important that Safety Critical Procedures are effectively supervised and checked.. Failure to monitor of Safety Critical Procedures can promote a poor safety culture and place the integrity of Safety Critical Measures at increased risk.

7.2.9 Capturing Experience

Principally this is the learning from past experience of how to avoid major accidents and incorporating this into the system. It often involves analyzing past events or experience including incidents and accidents and lessons learned from accidents in other companies.

7.3 Management Systems for Safety Critical Measures

The principles highlighted in Sections 7.1 and 7.2 can be embedded in a management system specific to Safety Critical Measures.

Possible components of a management system for Safety Critical Measures include:

1. Leadership and administration
2. Life cycle analysis and functional safety
3. Functional safety management
4. Resources and competences
5. Planning, implementation, maintenance
6. Requirements for functional safety analysis
7. Auditing
8. Verification protocols
9. Allocation of safety functions
10. Process hazard analysis documentation
11. Methods for allocating SIL targets
12. Requirement specifications
13. Design and application of software
14. Design and engineering
15. Certification of hardware and software
16. Installation, commissioning, validation
17. Requirements for the validation plan (testing, testing methods)
18. Operation and maintenance (responsibilities, proof testing, inspection, review of outcome of proof testing)
19. Review of fault reporting of Safety Critical Measures
20. Training requirements
21. Management of change
22. Decommissioning

Further guidance on management of Safety Critical Measures can be found in publications of the EEMUA (Engineering Equipment and Materials Users Association).

8 Performance Metrics

8.1 Introduction

Studies from the insurance industry show that a workplace accident in which someone is badly hurt or killed often follows a history of "precursor" incidents with similar characteristics but only minor consequences. Based on this finding, the idea that minor safety-related events can be used to predict personal injuries that are less common, but more serious, has become central to safety management

It is believed that a similar predictive relationship exists between lower- and higher-consequence events in process plants. Indicators that are predictive are known as *leading or pro-active* indicators and may be used to identify a weakness that can be corrected before a higher-consequence event occurs.

Indicators that focus instead on relatively serious accidents that have already occurred, so as to learn from them, are called *lagging* or *reactive* indicators.

With respect to process safety, this concept goes hand in hand with the Layer of Protection concept. Lagging indicators deal with actual loss of containment, while leading indicators give an indication of our ability to keep the product in the pipe. Leading indicators therefore answer to questions such as:

- Is my process staying within the safe operating limits?
- Are my layers of protection functioning?
- Do I have faith in the mechanical integrity of my installations?
- Am I learning from past experience?

8.2 Performance Metrics and Safety Critical Measures

Monitoring the performance of Safety Critical Measures is important for the following reasons:

- It enables site managers to compare the performance of their Safety Critical Measures against other sites and to find ways to improve when appropriate
- Improvement of leading indicators has been shown to influence the overall safety results of a company

Leading indicators are generally preferred when monitoring performance of activities relating to Safety Critical Measures.

8.3 Examples of Performance Indicators for Safety Critical Measures

The list below gives some possible leading indicators to monitor the performance of activities in the area of Safety Critical Measures:

- Total number of Safety Critical Measures identified at the facility
- Number of Safety Critical Measures inspections (including functional testing) scheduled
- Number of inspections (including functional testing) of Safety Critical Measures completed on schedule
- Ratio of Safety Critical Measures inspections (including functional testing) completed on schedule to inspections planned (including functional testing)

- Number of non-conformities of Safety Critical Measures identified during inspection, testing or normal operation
- Number of failures of Safety Critical Measures found during inspection, testing or normal operation; Ratio of number of non-conformities of Safety Critical Measures found during inspection/testing/operation to number of inspections completed
- Ratio of number of failures of Safety Critical Measures found during inspection/testing/operation to number of inspections completed

---

- Year to date (YTD) total of Priority 1 action items related to Safety Critical Measures
- YTD number of Priority 1 action items related to Safety Critical Measures completed
- YTD number of Priority 1 action items related to Safety Critical Measures completed within planned time
- YTD number of Priority 1 action items related to Safety Critical Measures, that are open but still within their planned completion dates

---

- Number of actions related to Safety Critical Measures following an incident/accident, a safety audit or a risk analysis planned for each month
- Number of actions related to Safety Critical Measures following an incident/accident, a safety audit or a risk analysis effectively completed in the month
- Completion rate of actions related to Safety Critical Measures following an incident/accident, a safety audit or a risk analysis

---

- Total number of Safety Critical Measures bypassed, excluding bypasses for testing;
- Number of Safety Critical Measures bypassed for more than five working days, excluding bypasses for testing

---

- Number of excursions outside the safe operating limits of the process

---

- Number of safety critical tasks scheduled for development or review of safe operating procedures
- Number of safety critical task procedures (development or review) completed
- Ratio of safety critical task procedures completed to those scheduled

9 Auditing and Self Assessment

In principle, auditing of activities in the area of Safety Critical Measures can be based on the items described in Section 7 and Section 8.

The integrity of Safety Critical Measures or Systems can only be assured if there is a regular process of 'Self Assessment' by the user and Audit by a technically competent body or person who is independent of the operations where the measures or systems are required to function. This principle is laid down in the life cycle approach in IEC 61511 and IEC 61508 and is described in the guidance from the Engineering Equipment and Materials Users Association (EEMUA 222). These sources are aimed at Safety Instrumented Systems, but the general principles are applicable to all Safety Critical Measures and Systems.

9.1 Self Assessment and Process Hazard Analysis (PHA)

Self Assessments exist within check lists commonly found in Process Hazard Analysis (PHA), Self Assessment methodologies. These rely on a check being made on the actual state of the operation compared with a clearly stated Requirement or Standard. The process should reveal the degree of conformance and/or non conformance and a 'gap analysis'. The evaluation needs to cover the state of conformance with requirements for:

- Hardware
- Software
- Human intervention and action
- Management of Change

This self assessment will normally include the records of the tests carried out on the Safety Critical Measures and Systems. It is important to note that these tests should include the Human intervention required within a Safety Critical environment.

9.2 Audit

Audits exist at several levels:

- Generalised Environmental Health and Safety Audits
- Audits of the Process Safety Management System
- Process Safety Audits

The audit process practices of EPSC member companies are described in the EPSC Member Report on Auditing, however, the most efficient form of audit takes account of and checks the PHA and self assessment which is in place at the operating facility. This check should be about:

- the degree of conformance with the PHA and self assessment system
- an examination of records of training and tests and inspections

- ‘deep drill’ on specific selected items (selection based on previous history, follow up, incidents, new requirements, records found, physical state of the facility and other relevant drivers

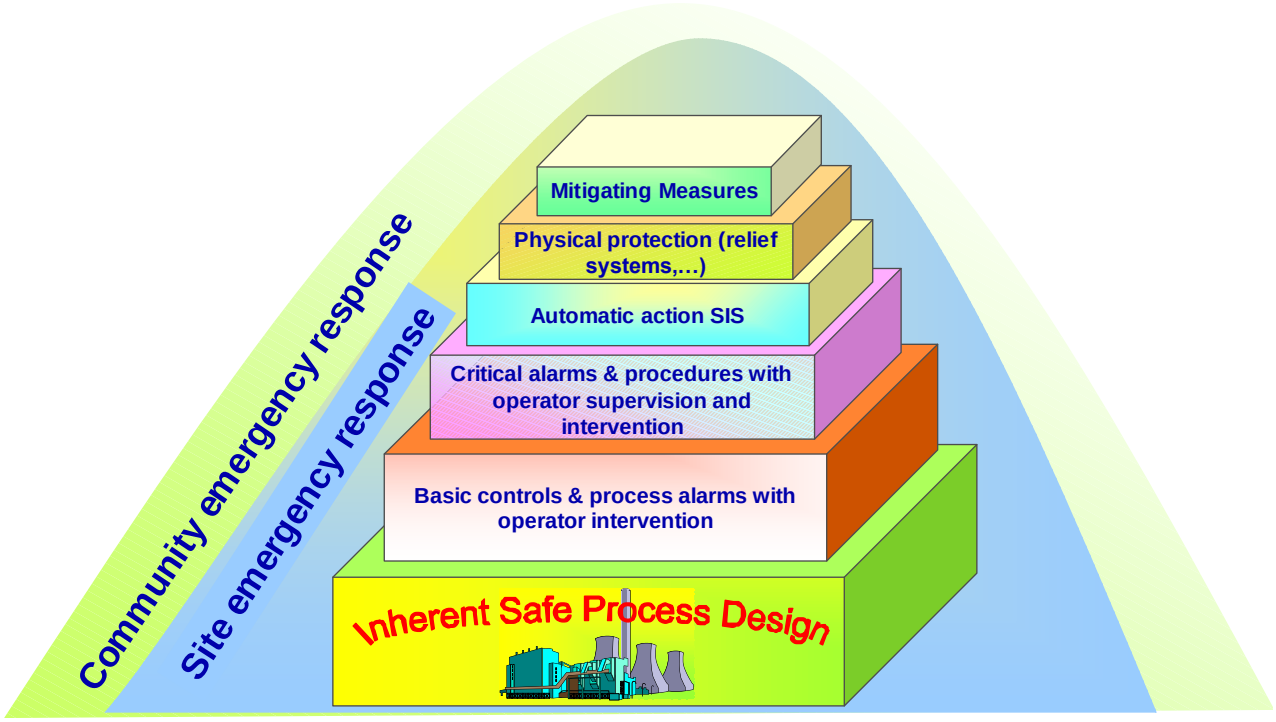
No self assessment, PHA or Audit can function properly without an effective follow up system where deficiencies are addressed in a timely manner. Put simply ‘Plan, Do, Check, Act’.

10 Examples of Safety Critical Measures

10.1 General

This section lists some general categories of Safety Critical Measures. Within each category, some examples are given. The proposed structure of the Safety Critical Measures follows the Layer Of Protection philosophy shown in the figure below.

Figure 6 : Layer of Protection "Onion"



10.1.1 Alarms Associated With Safety Critical Measures With Operator Supervision and Intervention

Alarms associated with Safety Critical Measures with operator supervision and intervention shall be clearly identified as Safety Critical Alarms and not be confused with other alarms generated by the DCS. Possible alarms include:

1. Flammable and toxic gas detection
2. Fire detection
3. Smoke detection
4. Liquid detection
5. Critical high temperature, level, flow, pressure alarms

To ensure that these critical alarms are clearly identified as Priority 1 alarms they should be on a separate panel and not within the DCS.

10.1.2 Safety Critical Procedures

1. Safety Critical Procedure (loading and unloading, decoking, regeneration,…)
2. Mechanical Integrity Program

10.1.3 Automatically Acting SIS and Power Supply

1. Explosion suppression systems
2. Inhibitor or killing agent injection systems
3. Some critical cooling systems
4. Interlocks independent from DCS
5. Pressure control valve to flare
    a. Heat cut-out interlock
    b. Feed cut-out interlock
    c. High level protection
6. Emergency Shutdown System (ESD)
7. Uninterruptible Power Supply (UPS)
8. Emergency power generator
9. HIPS (High Integrity Protection System)

10.1.4 Physical Protection

1. Pressure relief valves to flare
2. Rupture discs to flare
3. Vacuum breakers
4. Blowdown systems

10.1.5 Mitigating and Protective Measures

1. Dyking
2. Water curtains
3. Sprinkler/deluge systems
4. Foam application systems
5. Restricting flow orifices
6. Excess flow valves
7. Blast/fire resistant structures (blast/fire walls, reinforced control rooms, …)
8. Control of ignition sources
9. Active fire protection
10. Passive fire protection
11. Containment systems (containment inside building)
12. Flange protection
13. Devices influencing the direction of leaks

11 Appendix I: Terms of Reference

11.1 Purpose

The purpose of the work group is to share member companies' systems of:

- Defining and identifying
- Managing and maintaining
- Tracking and recording

Safety Critical Measures in the context of:

- Mechanical integrity management
- Protection barriers/layers
- Relief and mitigation systems
- Companies' individual safety management systems
- Recommendations from the Baker Report on the BP Texas City accident; Conformance with industry standards and national regulations (e.g. Seveso II, ATEX, IEC 61511)

11.2 Membership

Membership of the work group is limited to interested EPSC member company representatives. However, the work group may involve non EPSC member entities (for benchmarking, data collection etc.)

11.3 Topics for Discussion and Sharing

These may include for example:

- Equipment inspection and testing
- Mechanical Integrity management
- Protection barriers/layers
- Safety Instrumented Systems
- Safety system software
- Other safety-related protection systems
- Relief and mitigation systems
- Using records to provide failure frequencies and probabilities for quantitative and semi-quantitative risk studies
- Auditing

Members are encouraged to:

- Share their company systems
- Share company-specific reporting criteria
- Share performance metrics according to their own criteria (including history if this is available)

EPSC is not currently motivated to specify criteria or methods. There should be no additional reporting or data conversion to meet a 'harmonised EPSC model' unless the group or parts of the group wish to consider this possibility.

11.4 Sharing of Information

Information is in the first instance for dissemination exclusively between EPSC member company representatives. Contributors may specify that some or all of their information is restricted to the member representatives and does not pass to other people in their respective companies.

The overriding principle is that confidentiality is observed. If information is released outside EPSC it must be with the express permission of the contributors.

11.5 Timing

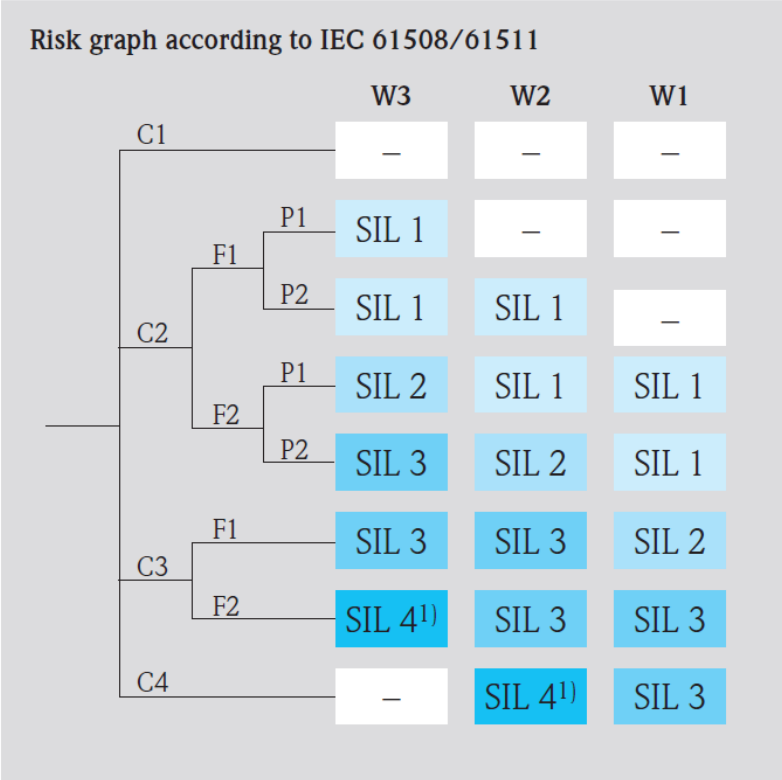
The work group was launched at the Technical Steering Committee in October 2008. Decisions on the life cycle of the group shall be made by the group's membership.

11.6 Drivers

- Member companies' external reporting
- Responsible Care®
- Baker Report recommendations
- Seveso II compliance

12 Appendix II: Examples of Analytical Methods

12.1 Example of Risk Graph



Consequences
C1 minor injury
C2 serious permanent injury to one or more persons; death of one person.
C3 death of several persons
C4 very many people killed

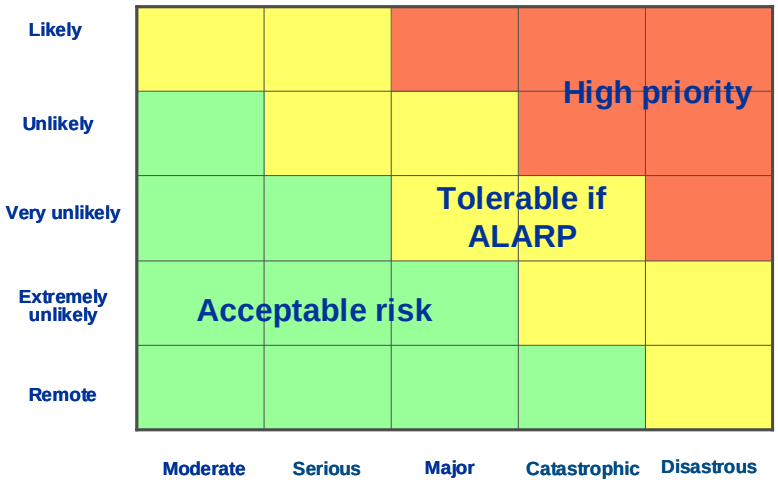
Exposure time
F1 rare to more often
F2 frequent to permanent

Avoidance of hazard
P1 possible under certain circumstances
P2 almost impossible

Probability of unwanted occurance
W1 very slight
W2 slight
W3 relatively high

12.2 Example of Risk Matrix

12.2.1 Matrix



12.2.2 Definitions for Severity Categories

Severity	Safety	Environment	Assets
Moderate	On site: - no permanent injury - recordable injury without lost time - medical treatment External: - no effect	Spill or release of pollutant requiring a declaration to authorities, but without environmental consequences	< 200 k€
Serious	On site: - permanent injury - lost time accident External: - non permanent effects	Moderate pollution within site limits	0.2 – 2 M€
Major	On site: - lethal effect on one person - several permanent invalidities External: - permanent effects	Significant pollution external to the site Evacuation of persons	2 – 10 M€
Catastrophic	On site: - lethal effect on several persons (several fatalities) External: - lethal effect - one fatality - several injuries	Important pollution with sustained environmental consequences external to the site	10 - 100 M€
Disastrous	On site: - many fatalities External: - lethal effects on large inhabited zones - several fatalities	Major and sustained pollution external to the site and/or extensive loss of aquatic life	> 100 M€

12.2.3 Definitions for Likelihood Categories

Likelihood	Frequency (1/yr)	Definition
Likely	$> 10^{-2}$	Could occur several times during plant lifetime
Unlikely	$10^{-2} \rightarrow 10^{-3}$	Could occur one time for 10 to 20 similar plants during 20 to 30years of plant lifetime
Very unlikely	$10^{-3} \rightarrow 10^{-4}$	One time per year for at least 1000plants. One time for 100 to 200 similar plants in the world during 20 to 30 years of plant lifetime Has already occurred in the company but correctives actions has been taken
Extremely unlikely	$10^{-4} \rightarrow 10^{-5}$	Has already occurred few times in industry but correctives actions has been taken
Remote	$< 10^{-5}$	Event physically credible but has never occurred or only few times during a period of 20 à 30 years for a large amount of units (>few thousands, ex: wagons, process drums,…)

Definitions

Term	Definition
Accident	Event or chain of events which causes, or could cause, injury, illness, and/or damage (loss) to assets, the environment or third parties (ISO 17776, first edition 2000-10-15). Sudden unintended departure from normal operating conditions in which some degree of harm is caused (A Guide to QRA for Offshore Installations, CMPT, 1999). Process accidents refer to accidents related to process facilities, utilities, transport and storage.
Availability	Ability of a system to perform a required function under given conditions, at a given instant or during a given time interval, assuming that all necessary external resources are present.
Audit (in the context of IEC61511)	IEC 61511 emphasises the importance of auditing to ensure long-term safety performance. The operation of any Safety Instrumented System (SIS) operation must be audited to determine the actual demand rate, i.e. process excursions resulting in SIS action. SIS device failures should also be recorded and the actual failure rates (both safe and dangerous) determined.
Common mode failure	Common mode, or common cause, failure t refers to events which are not statistically independent. That is, failures in multiple parts of a system caused by a single fault, particularly random failures due to environmental conditions or aging. An example is when all of the pumps for a fire sprinkler system are located in one room. If the room becomes too hot for the pumps to operate, they will all fail at essentially the same time, from one cause (the heat in the room). This is particularly important in safety-critical systems using multiple redundant channels. If the probability of failure in one subsystem is p, then it would be expected that an N channel system would have a probability of failure of pN. However, in practice, the probability of failure is much higher because they are not statistically independent
Barrier	Equipment, system or set of procedures (hardware, software or organisational) which lowers the probability of hazard occurrence (prevention), or the severity of the consequence (mitigation, reduction of vulnerability).
Consequence	The magnitude of the harmful effects. This term relates the quantified effect of an accident to the level of sensitivity of a vulnerable element or “target”: damage induced in a vulnerable element.
Effect	This term qualifies the type of physical phenomenon that may induce damage, following an incident. This is generally limited to: pressure wave, thermal flow, projectile, toxic concentration, pollution.
Environment	Everything external to the facility. Hazards related to the external environment include natural hazards (e.g. earthquakes, hurricanes) and hazards from third-party facilities (e.g. explosion in neighbouring plant, ship colliding with an offshore platform, aircraft crash).
Frequency	A rate which expresses how often a particular event occurs within a stated time period. Frequency is defined as the reciprocal of the average time

Term	Definition
	between events, and thus is often expressed in terms such as 1 per 1000 years (ISO 17776, first edition, 2000-10-15).
Functional Safety Assessment	As per IEC 61508 and IEC 61511, a functional safety assessment should be performed to ensure that risks inherent in a process and its associated equipment are duly controlled. This assessment should be applied through all the stages of the life cycle described in IEC 61508 and IEC 61511, from initial risk analysis to decommissioning. The assessment can be performed after each stage of the safety life cycle or after concluding a specific number of stages, including the safety life cycle of the SIS and its software. Notably, the Functional Safety assessment can be performed on SISs: • at the design stage • during installation • in installed systems In this way, the user or company acquiring a SIS is certain that all the steps set forth by IEC 61508 and IEC 61511 are followed at each stage. The assessment should conclude with recommendations for accepting or modifying the functional safety of the system. IEC 61511 requires that at least one senior, "competent" and independent person takes part in the Functional Safety Assessment. This competent person should be able to review the hazard analysis, design, implementation, and testing to ensure that everything has been successfully completed and must have the authority to prevent the start-up of the process if necessary.
Harm	Human injury, damage to the environment, damage to property, or a combination of these (ISO 17776, first edition 2000-10-15). Adverse consequences of accidents, such as sickness, injury, death, damage to property, degradation of the environment, or interruption of business ("A Guide to QRA for Offshore Installations", CMPT, 1999).
Hazard	Potential source of harm (ISO 17776, first edition, 2000-10-15).
Hazard Analysis (or HAZAN)	Method of identifying possible undesirable events, analysing the mechanisms by which they could occur, and (usually) estimating their consequences. Hazard analysis sometimes includes consideration of the likelihood of key events (A Guide to QRA for Offshore Installations, CMPT, 1999).
Hazardous event	Incident that occurs when a hazard is realised (ISO 17776, first edition, 2000-10-15). Also sometimes called an "Undesired Event". Examples: Release of a substance, release of energy, fire, loss of buoyancy.
Hazard Identification	Systematic identification of all the hazards that may affect, or arise from, the particular operation under consideration (ISO 17776, first edition, 2000-10-15).
HAZID	Acronym for Hazard Identification and especially for a particular form of Hazard Identification commonly applied to upstream installations. HAZID is a systematic (group) review of the possible causes and consequences of hazardous events (A Guide to QRA for Offshore Installations, CMPT, 1999). Sometimes this analysis includes consideration of the likelihood of key events.

Term	Definition
HAZOP	Acronym for Hazard and Operability Study: a systematic critical group review of a process plant design, to evaluate the effects of deviations from normal operating conditions. HAZOP is normally used to generate recommendations to improve the safety and operability of a design, but it can in principle be used to identify hazards as well (A Guide to QRA for Offshore Installations, CMPT, 1999).
Incident	Relatively minor accident: an unintended departure from normal operating conditions causing little or no harm (A Guide to QRA for Offshore Installations, CMPT, 1999).
Initiating event	Event directly causing a central Hazardous Event.
Intensity	Quantified effect of an accident.
Likelihood (or Chance)	Expressions that indicate, in general terms, the possibility of something happening (ISO 17776, first edition, 2000-10-15). See also Probability and Frequency.
Mitigation	Attenuation of the effects of a central Hazardous Event, such as by reducing the duration or rate of a release, or by stimulating dilution or dispersal. Mitigation includes the effect of passive elements such as walls located close to the source.
Major accident (Seveso II Directive)	According to the more general definition of Article 3 of the Seveso II Directive, a "'major accident' shall mean an occurrence such as a major emission, fire, or explosion resulting from uncontrolled developments in the course of the operation of any establishment covered by the Directive, and leading to serious danger to human health and/or the environment, immediate or delayed, inside or outside the establishment, and involving one or more dangerous substances".
Prevention	Reduction of the occurrence frequency of a central Hazardous Event.
Probability	The ratio of the number of chances that a particular event may occur to the total number of chances. It is expressed as a number in the range 0 to 1, zero being the certainty that the event will not occur, and 1 the certainty that the event will occur. It is also normal to express probability in percentage terms (ISO 17776, first edition, 2000-10-15).
Protection	Reduction of the severity of the consequences on a particular target; reduction of the vulnerability of a target.
QRA	Acronym for Quantitative Risk Analysis (not Quantitative Risk Assessment in the context of this report). QRA is a mathematical means of estimating numerical risk from a particular hazardous activity. It involves making numerical estimates of hazard outcomes in terms of frequencies and consequences, and aggregating them into overall measure of individual or societal risk.
Reliability	Ability of a system to perform a required function, under given conditions, within a given period of time. Approximately, the system failure probability P increases as a function of a failure rate λ and a test period T according to the equation: $P = \lambda.T$
Risk	The combination of the likelihood that a hazard will be realised and the consequence of that hazard; the chance of a specific event occurring within a specific period (A Guide to QRA for Offshore Installations, CMPT, 1999). When using the more experience-based qualitative approaches, it is normal to express risk as the direct product of the frequency of occurrence and the severity. In some situations, however, it is necessary to define risk in

Term	Definition
	somewhat more precise terms; here the usual approach is to express risk as the probability that a specified hazardous event will occur in a specified time period or as a result of a specified situation (ISO 17776, first edition, 2000-10-15). This approach uses the definition of the frequency of a number of different consequences to give the overall risk picture.
Safety Critical Measures	A subset of safety measures that are required to avoid or control the impact of major accident scenarios (see also section 3.2 of this document)
Safety Instrumented System (SIS)	A Safety Instrumented System (SIS) consists of an engineered set of hardware and software controls which are especially used on critical process systems. A critical process system can be identified as one which, once running and an operational problem occurs, the system may need to be put into a safe state avoid adverse consequences. An SIS is composed of the same types of control elements (including sensors, logic solvers, actuators and other control equipment) as a Basic Process Control System (BPCS). However, all of the control elements in an SIS are dedicated solely to the proper functioning of the SIS.
Safety Instrumented Function (SIF)	Refers to the specific control functions performed by an SIS. An SIS is engineered to perform "specific control functions" to failsafe or maintain safe operation of a process when unacceptable or dangerous conditions occur. They are implemented as part of an overall risk reduction strategy which is intended to eliminate the likelihood or consequences of a, previously identified, hazardous event.
Severity	The severity of an accident results from the combination of intensity and the vulnerability of the target.
System	The object of the assessment, which can include many equipment items.
Validation	The process of proving that a SIS or by extension any Safety Critical Measure works in practice. Validation involves a complete test from input to output and can be performed as part of the pre-startup test.
Verification (in context of Safety Instrumented Systems)	Demonstration that the output of a Safety Instrumented Function (at each stage of the life cycle) satisfies prescribed requirements. Verification methods include testing, review and analysis.
Vulnerability	Sensitivity of a target to a particular type of effect. A vulnerability analysis defines a relationship between the intensity of incident effects and consequent damage.
Process safety time	The period from the time at which a fault occurs in the process to the time when the process enters a dangerous state. Following a process error, the safety system needs to transfer the process to a safe state within the process safety time.
Reaction time	Referring to the complete safety system, the sum of the individual reaction times of the sensor, actuator, and safety controller. The reaction time needs to be shorter than the process safety time.

Abbreviations

Abbreviation	Term
API	American Petroleum Institute
DCS	Distributed Control System
ESD	Emergency Shut-Down
HAZID	HAZard IDentification
HAZOP	HAZard and OPerability Study
ISO	International Organization for Standardization
PFD	Probability of Failure on Demand or Process Flow Diagram (depending on context)
QRA	Quantitative Risk Analysis (in the context of this document).
SCM	Safety Critical Measure
SIL	Safety Integrity Level
SIS	Safety Instrumented System
UPS	Un-interruptible Power Supply

References

1. TOTAL – Industrial Safety Division SG-SEI
   Guidance Note on Safety Critical Measures (2009)
   HSE-SRD-016

2. Det Norske Veritas
   Risk Assessment Training Course (1995)
   Project no: 21045

3. Det Norske Veritas
   QRA Training Course for the Process Industries (1999)

4. Bellamy, L J (2003)
   SAVRIM Handbook (dec 2000)

5. Gowland, R (2003)
   Layer Of Protection Training Course
   University of Manchester

6. De Wilde, B (2004)
   Design of Safety Instrumented Systems, rev1

7. Baker Panel (2007)
   The Report of the BP U.S. Refineries Independent Safety Review Panel

8. Mogford, J (2005)
   Fatal Accident Investigation Report
   Isomerization Unit Explosion
   Final Report
   Texas City, Texas, USA

9. Buncefield Major Incident Investigation Board (2005)
   The Buncefield Incident
   The Final Report of the Buncefield Major Incident Investigation Board

10. International Electrotechnical Commission (IEC)
Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7
IEC 61508: 1998 – 2000

11. Engineering Equipment and Materials Users Association (EEMUA)
Alarm Systems - A Guide to design, management and procurement
EEMUA 1999
ISBN 0 85931 076 0

12. Deming, W E (1975)
On probability as a basis for action
The American Statistician, 29(4), pp146–152

13. Keynes, J M (1921)
A Treatise on Probability
ISBN 0-333-10733-0

14. Knight, F H (1921)
Risk, Uncertainty and Profit
ISBN 1-58798-126-2

15. Shewhart, W A (1939)
Statistical Method from the Viewpoint of Quality Control
ISBN 0-486-65232-7

16. Wheeler, D J & Chambers, D S (1992)
Understanding Statistical Process Control
ISBN 0-945320-13-2

17. Guidelines for Safe and Reliable Instrumented Protective Systems (2007)
Center for Chemical Process Safety

Working Group Members

Member Name	Company
Herman van Lochem	Akzo Nobel
Volker Arndt	BASF
Hans Schwarz	BASF
Volker Stellmacher	Bayer Technology Services
Joep Duerloo	Chartis Insurance
Eric Lenoir	Chartis Insurance
Klaus-Juergen Niemitz	Clariant
Klaus Wischnewski	DuPont
Lee Allford	EPSC
Richard Gowland	EPSC
Martin de Zeeuw	LyondellBasell
Nigel Cairns	Marsh
Carlos Videla Ivanissevich	Repsol
Philippe Walsdorff	Solvay
David Sullivan	Tata Steel Europe
Dirk Roosendans	Total

Guest Speakers

Member Name	Company
Thomas Helmer	Consultant
Chris Blackmore	DNV
Bert Knegtering	Honeywell Process Solutions
Sören Altes	SwissI Process Safety