5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

# Fitting Safety In Project Engineering

Dinesh Govind., B.Tech, M.E.
Onshore Project Engineering
Qatar Petroleum
P.O. Box 70
Doha QATAR
Phone: 974-4343234
Email: dinesh@qp.com.qa

## INTRODUCTION

Recent trend in developments have resulted in great changes to engineering approach in process industries. A number of factors are involved in these changes. More severe process operating conditions, increase in energy stored in process, limitations in space, stringent environmental regulations, diversification in material selection, day to day developments in electronics, communications, automation and computerization are some of the factors that have influenced the thinking process of management.

The process industries have always been concerned with the safety, operability and reliability of their plants. The effect of scale, depth and pace of technology is to increase the size of the hazards, to make their control more difficult and to reduce the chance of learning by trial and error. High technology systems are particularly demanding in terms of formal management organizations, engineering, procedures, standards and codes of practice, and of competent persons.

This paper is intended to highlight the role of safety in project engineering, for process plants. No attempt is made to discuss issues related to safety during construction and commissioning.

## LOSS PREVENTION PHILOSOPHY

Specifying a loss prevention philosophy for a project is the foundation for safety in project engineering. The primary objective of a specific loss prevention philosophy is to ensure that the design of the facilities reduces the risk to personnel, assets, environment, third parties, production revenue and capital investment to as low as reasonably practicable, during the operation of the facilities. Corporate fire and safety guidelines, standards, codes of practices, local government health, safety and environmental requirements have to be considered while preparing the specific loss prevention philosophy for the project. Sometimes corporate safety philosophies could be used as the basis for implementing safety during various phases of a project ; however, for major projects, it is advisable to develop project specific loss prevention philosophy. The document should highlight the project specific philosophy for

designing fire prevention, fire protection and emergency shut down systems, safety in buildings, requirements for design safety reviews, guidelines for risk assessments, hazard identification, reliability and environmental studies.

## RISK ASSESSMENTS

Identifying fire, explosion or toxic hazards and quantifying the individual and societal risks is very important at the preliminary design phase of a project. Results of consequence analysis are used while finalizing layout of equipment and storage tanks, routing pipelines, determining fire water requirements, specifying type of buildings and material selection. Individual and societal risk figures provide information to understand the risk to the employees, contractor personnel and to the society around the facility. It also assists in justifying budget for implementing risk reduction measures such as design improvement and work control procedures.

A clear understanding of the location, environment, procedures, process parameters and interaction with plant personnel are required for conducting a realistic risk assessment.

For projects related to expansion or modifications to an existing processing facility (brown field projects), the philosophy shall be to minimize the risks to a level as low as reasonably practicable. For such brown field projects, additional procedural controls will have to be implemented to satisfy acceptable risk criteria. However, for new (green field ) projects, results of risk assessments could be implemented with more engineering solutions, which includes spacing and layout of equipment, planning locations for buildings, emergency escape routes, safety instrumented systems, etc.

The UK Health and Safety Executive (HSE) have suggested the boundaries between various risk acceptance criteria as follows[1] :

- For workers, the boundary between the unacceptable and the tolerable region should be an individual risk of fatality of 1 in 1000 per year. This is based upon a consideration of the risks associated with the most hazardous work activities that society appears to tolerate.
- For members of the public, this boundary is set an order of magnitude lower at a level of individual risk of fatality of 1 in 10,000 per year.
- The boundary between the tolerable and the broadly acceptable regions is considered to be an individual risk of fatality of 1 in 1,000,000 per year.

The issue of finding safe location for control rooms and other buildings in process plants has always been a challenge for safety professionals. API RP752 ( Management of hazards associated with location of process buildings) in the US and the UK Chemical Industries Association (CIA) guidance for location and design of occupied buildings on chemical manufacturing sites provides guidelines for determining safe locations for buildings. In order to locate a building with in a process plant, the level of hazards and the frequency with which the levels of hazards (thermal flux, blast overpressure or toxic gas concentration) will occur at a proposed building location are determined. The level of hazard which has a frequency of 1 in 10,000 years generally forms the design criteria.

Figure 01 shows the general form of the graph.

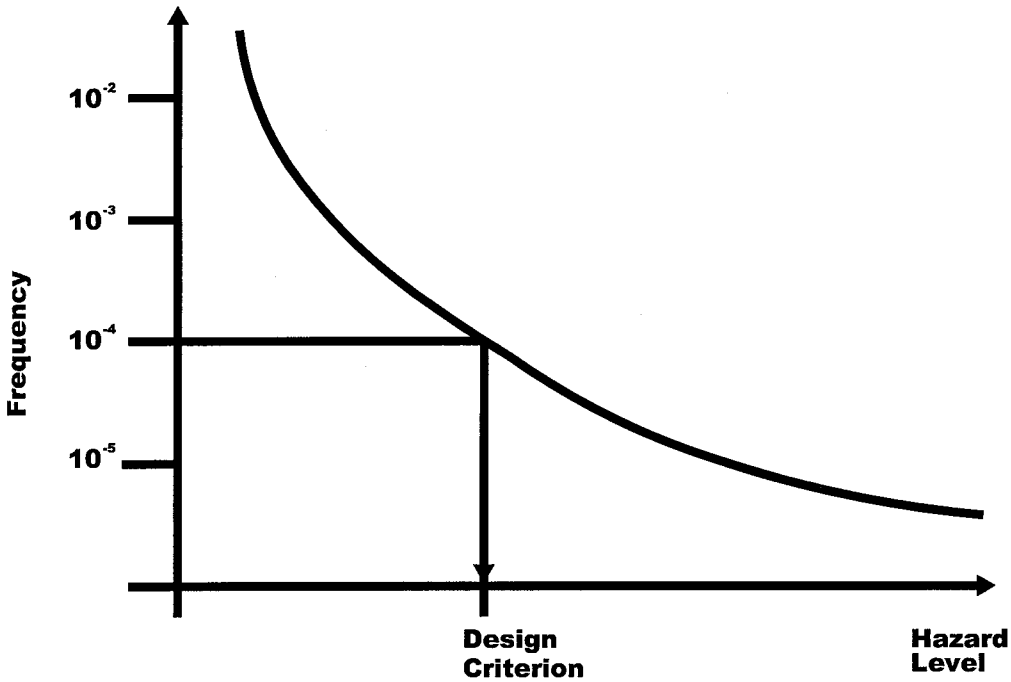


**Figure 01 – General form of graph used to determine design criteria for buildings[2].**

The estimation of fatality or injury caused by a physical effect such as thermal radiation or explosion overpressure requires the use of probit equations, which describe the probability of fatality as a function of some physical effect. The probit equations are based on experimental dose response data and generally take the form

$$Y = a + b \ln V$$

Where Y is the probit (-), 'a' and 'b' are constants determined from experiments and V is the measure of the physical effect such as thermal radiation, peak overpressure, toxic gas release, etc. 'V' is a function of time and dose, generally taking the form $C^n$ x t. Probit is an alternative way of expressing the probability of fatality and is derived from a statistical transformation of the probability of fatality. The relationship between fatality probabilities and probits are given in the text book by Frank P. Lees[3].

Choosing the probit equations to define the hazard end points[4] is very critical in projects, in particular when modifications are carried out on existing operating facilities. For example applying the two probit equations for toxic gas release

$$Y = -31.42 + 3.008 \ln ( C^{1.43} \text{ x } t ) \ldots\ldots\text{Perry and Articola, 1980}$$
$$Y = -36.2 + 2.366 \ln ( C^{2.5} \text{ x } t ) \ldots\ldots\text{Gascon2, 1990}$$

will provide different magnitude of consequence. More conservative equations have to be considered for green field projects.

## HAZARD IDENTIFICATION FROM DRAWINGS

Various techniques are used for identification of hazards when the projects are on the drawing board. Depending upon the nature of the project, these techniques are applied at the preliminary design as well as detailed design of the project.

The most versatile technique for hazard identification from drawings is the Hazard and Operability (HAZOP)[5, 6] study. First introduced by ICI ( Imperial Chemical Industries, UK) in 1973, this technique is currently being used not only by the process industry, but also by banks and commercial institutions.

HAZOP studies are carried out by a multidisciplinary team, who review the process to discover potential hazards and operability problems using a guide word approach. Guide words such as 'NO', 'MORE', 'LESS', 'REVERSE', 'AS WELL AS', 'PART OF', 'OTHER THAN' etc are applied on various process parameters such as 'FLOW', 'TEMPERATURE', 'PRESSURE', 'LEVEL', etc. Process Flow Diagrams, Piping & Instrumentation Diagrams (P&ID), Cause & Effect Charts, Equipment layout drawings, Hazardous Area Classification Drawings , Process Design Basis, Equipment data sheets and Vendor package information are required to effectively perform a HAZOP study. However, HAZOP studies are not sausage machines which consumes line diagrams and produces lists of improvement recommendations. It merely harness the knowledge and experience of the multidisciplinary team, in a systematic way.

HAZOP study is not a design review exercise. Prior to HAZOP study, process design has to be completed. PFDs and P&IDs will have to be reviewed and approved by relevant engineering personnel. When process design is incomplete, HAZOP studies turn out to be design review meetings. Pre-HAZOP deign review meetings are essential in order to ensure maximum benefit from a HAZOP study.

Third parties, who are independent to the project, should facilitate the HAZOP studies. Members of design team when facilitating HAZOP studies tend to defend their design and behave with an element of resistance.

HAZOP studies are conducted during the FEED ( Front End Engineering and Design ) as well as EPIC ( Engineering Procurement Installation and Commissioning) phase of projects. Vendor package engineering and equipment data are included in the EPIC phase HAZOP study.

## SAFETY INTEGRITY LEVEL

Safety related system is a designated system that both implements the required safety functions necessary to achieve or maintain a safe state for the equipment under control and is intended to achieve, on its own or with other electric, electronic or programmable electronic safety related systems, other technology safety related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions. Safety Integrity is defined as the probability of a safety related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. The higher the

level of safety integrity of the safety related systems, the lower the probability that the safety related systems will fail to perform the required safety functions.

There are two aspects of Safety Integrity Level (SIL) determination. One is defining a target Safety Integrity Level during the preliminary design stage and later verifying the Safety Integrity Level during the EPIC stage, when design of safety instrumented systems are completed and vendor information are available.

In general, target safety integrity level for a single safety related protection system can be determined using the relation

$$PFD_{TARGET} \leq F_A / F_{SRS} \quad (7)$$

where PFD is the average targeted Probability of Failure on Demand in order to meet the necessary risk reduction, $F_A$ is the acceptable risk frequency and $F_{SRS}$ is the frequency of demand on the safety related system. The frequency of hazardous event is directly related to $F_{SRS}$. Thus, for $F_A = 1 \times 10^{-4}$ and $F_{SRS} = 1 \times 10^{-1}$, targeted PFD will be $10^{-3}$ . From IEC 61508, the calculated target PFD corresponds to SIL 3. Frequency and exposure time risk parameters, consequence risk parameters, possibility of failing to avoid hazard risk parameters , probability of unwanted occurrence and risk graphs are available in IEC 61508 and IEC 61511, which could also be used to determine the target safety integrity levels.

During the EPIC phase, SIL verification exercise is performed using PFD data of various input / output devices, logic cards and system architecture. Fault tree analysis is a widely approved method for quantitative reliability analysis and is well qualified through practical use for several years in different types of industries. A computerized fault tree analysis package could be used for construction and analysis of the modeled scenario. The results of such analysis provide the Critical Safety Unavailability of the safety related system, which is then expressed in terms of SIL values. Table 01 shows correlation between overall risk level and required safety system performance.

The results of the SIL verification exercise will determine additional requirements for the safety related systems. It is often noticed that the SIL is improved by redundancy and voting schemes, diversity, reducing common cause failures and increasing testing frequency. Attempts to improve SIL by increasing testing frequency is not always supported by the inspection and maintenance personnel. In redundancy the installation is duplicated or triplicated. In diversity, the fact that a rise in pressure may be accompanied by a change in temperature or level or some other parameters somewhere in the system is considered and an additional trip initiator on an entirely different parameter is used. Diversity is preferred to redundancy as circumstances may arise which mask the change in the original parameter or inhibit the action of the shutdown system. Furthermore, a disadvantage of redundancy is that the frequency of spurious trip increases which could interfere with production. The cost of additional equipment can frequently be justified by the savings from the avoidance of spurious trips.

| Risk Level | Safety Integrity Level SIL | Required Safety Availability | Probability of failure on Demand (PFD) | Risk Reduction Factor |
|---|---|---|---|---|
| | 4 | >99.99% | < 0.0001 | > 10,000 |
| High | 3 | 99.9 – 99.99% | 0.001 - 0.0001 | 1000 – 10,000 |
| Medium | 2 | 99 – 99.9% | 0.01 – 0.001 | 100 – 1000 |
| Low | 1 | 90 – 99% | 0.1 – 0.01 | 10 – 100 |

**Table 01 – Correlation between Risk level and System Performance.**

Using IEC 61508 risk graph approach, or risk matrix developed by the industry, SIL for applicable HAZOP study recommendations can be determined.

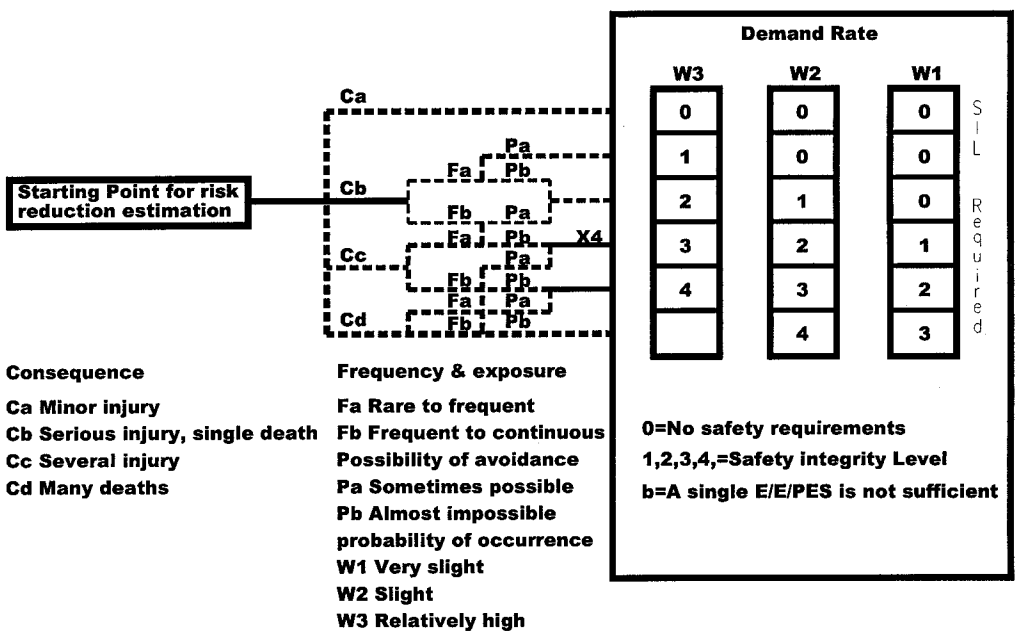


**Figure 02 – Risk Graph[7] - a useful tool to determine SIL during HAZOP studies.**

Sections from work sheets of a preliminary design phase HAZOP study for a 12 inch crude oil loading pipeline to a Single Buoy Mooring facility are shown in Table 02. The crude oil storage tanks and loading pumps are located onshore about 2 kms from the coast. The surge system is located near the crude oil metering area at the shore. During this HAZOP study SIL values were determined using the risk guidelines provided in Figure 02.

| Parameter : Pressure | | | | | |
|---|---|---|---|---|---|
| Deviation | Cause | Consequence | Safeguard | Recommendation | SIL |
| HIGH | Ship side valve closed | Pressure surge, potential for pipeline rupture and fire | High Pressure Alarm<br><br>Surge valve opening into a dedicated surge tank. | | 2 |
| Parameter : Level | | | | | |
| HIGH | Surge valve opens (due to high pressure on loading line)<br><br>. | Possible overflow of surge tank. Potential for fire. | High level alarm for surge tank.<br><br>Operator procedures | Provide instrumented shutdown of crude oil loading pumps, on high high pressure. | 3 |

**Table 02 : Modified HAZOP work sheet, including SIL.**

Using risk graphs and modified HAZOP worksheets, SIL for safety systems falling under 'safeguards' as well as 'recommendations' could be determined during HAZOP sessions. Risk path followed in the above cases were Cc-Fb-Pa-W2 for high pressure in the pipeline and Cc-Fb-Pa-W3 for high level in surge tank. A separate SIL determination exercise was not performed for this project.

## COST BENEFIT ANALYSIS

It is the nature of project management to show resistance to implementation of mitigation measures recommended by Quantitative Risk Assessments, HAZOP or SIL studies. Some of the recommendations could cause a significant impact on the cost as well as schedule of the project. Recommendations during the FEED phase of the project has less cost impact when compared to its implementation during EPIC phase. For example, a preliminary design phase (FEED) HAZOP study recommendation to include an additional heat exchanger will have relatively lesser impact on project costs and schedule when compared to an EPIC phase recommendation to provide an additional 16 inch motor operated valve.

Cost benefit analysis seeks to assess the benefit of mitigation measures by comparing the risk benefit (in terms of lives saved) with the cost of the proposed measure. If the cost of mitigation measure over its life is greater than the monetary benefits in terms of lives saved, then the measure would not be justified, and vice versa. In order to convert the risk to a monetary value operating company will have to define the Cost of Averting a Fatality (CAF).

Quantitative Risk Assessment (QRA) for an additional crude oil inlet manifold project recommended the following mitigation measures :

- Gas detection
- Shutdown valves at the manifold
- Fire detection
- Water deluge

A cost benefit analysis was carried out for the above mitigation measures as follows :

Benefit of mitigation measure = CAF x Reduction in PLL x Operating Life.
Cost of mitigation measure = Capital Cost + Maintenance Cost + Operating Cost.

where, PLL is the Potential Loss of Life = Individual Risk x Number of Expected Fatalities.

From operating philosophy of the plant, it was determined that a maximum of 2 people would be exposed to major accident at the manifold area, at any time. The QRA had determined the individual risk as $2.7 \times 10^{-5}$. The operating company defined the cost for averting fatality to be US$ 5,000,000/-.

$$PLL = (2.7 \times 10^{-5}) \times 2 = 5.4 \times 10^{-5}$$

Benefit of mitigation measure per year = $5,000,000 \times (5.4 \times 10^{-5}) =$ US$ 270 /-

Considering operating life of plant as 30 years, the benefit of mitigation during the life of plant will work out to be US$ 8100/-

From the above calculations it should be noted that there is very little benefit, in terms of lives saved, even should a mitigation measure be found to totally remove the risk. Benefit of implementing the mitigation measures recommended will be US$ 8100/- only. It was found that implementing the four mitigation measures will not be cost effective. Estimation indicated that implementation of shut down valve alone will cost US$ 120,000. Only implementation of gas detection system will be less than US$ 8100. It was decided to implement the recommendation on gas detection.

**FIRE PREVENTION AND PROTECTION**

Safety engineers specify the fire prevention and protection requirements for a process plant. This includes plant location, equipment layout, fire and gas detection systems for outdoor and indoor applications, fire water systems, foam and gaseous fire protection systems and passive fire protection for structures and buildings.

Location of plant, layout of equipment, piping, storage tanks, roads, fence, etc are determined based on results of risk assessments, environmental data, process conditions and land utilization value. When location and layout are finalised, hazardous areas are determined and drawings are prepared to show the extend of classified areas. API (American Petroleum Institute) or IP (Institute of Petroleum, UK) guidelines are used to develop the hazardous area classification drawings. These drawings are used as guidelines for defining requirements for electrical equipment and instruments, locating vents, drains and air intakes to buildings and establishing plant roads and emergency escape routes.

Determining the location of detectors, specifying the correct type of detectors and defining the executive actions are the key elements of fire and gas system design. There are no known codes or standards which could be used to find location or density of gas detectors in process

plants. Results of consequence analysis, environmental data, process fluid characteristics and operating parameters are considered while locating fire and gas detectors in the field.

Some of the typical executive actions for flammable gas detection are

One flammable gas detector reaching 20% LEL (alert) or 50%LEL( danger)

- Alarm to Control Room

Two or more flammable gas detectors in an array of three or more reaching 20%LEL ( 2 out of 'n' detectors)

- Alarm to Control Room
- Initiate Plant General Alarm

Two or more flammable gas detectors in an array of three or more reaching 50% LEL (2 out of 'n' detectors)

- Alarm to Control Room
- Initiate Plant General Alarm
- Initiate Emergency Shut Down and Blowdown.
- Shutdown building ventilation and fire dampers.

Requirements of executive actions upon detection of gas is frequently debated. Some owners have 'Alarm Only' philosophy and actions are initiated by experienced operators, based on review of the hazard situation. Cause and Effect charts are developed to reflect various shutdown actions Logic, loop and termination diagrams for the fire and gas detection system are developed with reference to the Cause and Effect charts. Upon completion of projects, these charts have been found to be a valuable tool for operators and maintenance personnel.

Fire protection system design includes determining fire water requirements, specifying a fire water system, which includes, fire pumps, fire water network with hydrants / monitors, deluge or sprinkler systems, engineering and specifying foam systems, gaseous systems, combination systems such as the hydrochem system and establishing the passive fire protection requirements applicable for the project.

There are various codes and standards on fire prevention and protection. Application of the standards require clear understanding of their intent.

## CONCLUSION

The progressive cost conscious management approach and the increasing need to operate the plant closer to risk situation requires refined methods for eliminating problems at the project engineering phase. Risk assessments, hazard identification exercises, specifying safety integrity levels for instrumentation and specifying adequate fire prevention and fire protection requirements will ensure safe operability of process plants. Experience and knowledge of safety and loss prevention engineers play a significant role during various facets of project execution.

## REFERENCE


1. Health and Safety Executive 1999. 'Reducing Risks, Protecting People'. Discussion Document.
2. UK Chemical Industries Association 1998. Guidance for the location and design of occupied buildings on chemical manufacturing sites.
3. Lees,F.P., Loss Prevention in the Process Industries, 2nd Edition, Butterworth-Heinemann,1996.
4. John B. Cornnel and Jeffrey D. Marx, The significance of Hazard End Points in Quantitative Risk Analysis, Quest Consultants Inc. USA.
5. Ellis Knowlton. R., "An Introduction to Hazard and Operability studies; The Guide word approach", Chemetics International Company Ltd., Canada, Feb,1989.
6. Henry Ozeg and Lisa M. Bendixen., "Hazard Identification and Quantification", Chemical Engineering Progress, April 1987.
7. The IEC (International Electrochemical Commission) standard 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.