To Mary Kay O'Connor Process Safety Center Home Page
To Program details for Day 1
To Program details for Day 2

Safety Integrity Levels in Design

Mark Moderski, Sankar Mahalingam, Mark A. Eidson
Stone and Webster Engineering Corporation
1430 Enclave Parkway
Houston, Texas 77077-2023

Paper presented at the 1st Annual Symposium of the Mary Kay O'Connor Process Safety Center,
"Beyond Regulatory Compliance, Making Safety Second Nature",
George Bush Presidential Conference Center, College Station, Texas
March 30-31, 1998.

ABSTRACT

The hazards identified with a new or modified chemical or petroleum refining process can be mitigated in numerous ways. If a system cannot be designed so that it is inherently safe, then other safeguards such as instrumented systems, mechanical controls or operating procedures need to be implemented. If an instrumented system is to used to mitigate the hazard then some consideration must be given towards the integrity of this system based upon the risk presented by the hazard. Based upon recent ISA standards, the integrity level of this instrumented system must be specified so that the corresponding probability of failure on demand can be achieved. This paper discusses the overall process of mitigating hazards including the role of safety integrity levels for instrumented systems.

SAFETY INTEGRITY LEVELS IN DESIGN

The term safety integrity level (SIL) is based upon the ISA standard S84.*01 Application of Safety Instrumented Systems for the Process Industries*, and refers to the reliability requirements of an

instrumented system. However, before getting to the point of determining if an instrumented system is going to be used to mitigate a hazard and then determining the SIL of that system, there may be many other alternatives that can be used to mitigate the hazard.

In Stone & Webster Engineering Corporation's (Stone & Webster) work process, the hazards of a process are identified early in the life of the project. As the design develops, certain design decisions are made by Stone & Webster individually and / or jointly with the client. During this decision making process, design alternatives are considered for each of the hazards identified. These alternatives typically fall into one of the following categories:

1. Mitigate the hazard through an inherently safe means,

2. Mitigate the hazard through mechanical or instrumented systems.

3. Mitigate the hazard through operating procedures or administrative controls.

Identification of Hazards

The identification of hazards in the design of a chemical process is traditionally performed using the hazard and operability (HAZOP) technique. Unfortunately, in order to ensure that there is sufficient design details for the HAZOP to be effective, the HAZOP is often performed late in the design stage. As a result, unacceptable hazards identified during the HAZOP can lead to significant design changes which will correspondingly impact the project cost and schedule.

In order to minimize the financial and schedule impact of a HAZOP, Stone & Webster performs preliminary hazard reviews (Pre-HA) on many of its projects. These reviews are performed as soon as the basic process schemes have been developed and there is sufficient information on the process chemistry and technology.

The review technique varies according to the type of project and information available, but in most instances it is either a "Checklist" or "What-If" method. The review considers very few safeguards because they are usually not represented on the documents reviewed during this early stage of the project. If special metallurgy or emergency shutdown systems are not represented, then they will have to be confirmed during design development whether they were assumed to be safeguards during the Pre-HA or not. The key here is to ensure that credit is given where credit is due.

As a result of the Pre-HA, the obvious and inherent hazards along with the unique hazards are documented for each piece of equipment or study node. As the project proceeds and the design develops, addendum's are added to the Pre-HA report if any additional hazards are identified or if the basic process scheme changes.

The Mitigation Process

Mitigation of the hazards identified during the Pre-HA begins immediately after the review and continues up until the next hazard review which is often the HAZOP. Most of the mitigation is accomplished during the development of the P&ID's which includes the selection of metallurgy, design conditions, mechanical safeguards and instrumented systems.

Mitigation decisions can be made jointly with the client or not depending upon the type of project, but the primary objective of mitigation is to always ensure that the level of risk represented by the chemical process is consistent throughout the process and consistent with the client's and Stone & Webster's level of acceptable risk.

Mitigation through Inherently Safe Design

During initial process development, processes technologies are selected and optimized in order to achieve the most efficient operation with the lowest capital cost. During this stage of the project, substituting chemicals and operating conditions are considered from a safety aspect and equipment sizes are minimized to both lower the capital cost and minimize hydrocarbon inventories. Stone & Webster has repeated experience with ethylene and petroleum refining processes, so opportunities for further inherent safety are primarily found during design development.

During design development the following critical inherently safe design decisions are made such as:

- selection of metallurgy
- determination of design pressure
- determination of design temperature
- location of equipment to minimize inventories or impact to one another in case of an accident
- minimization of large inventory lines

Providing an inherently safe design is obviously the most desirable option. However, often these solutions may not be cost effective, and other alternatives may be pursued.

Mitigation though Mechanical Controls

If a hazard cannot reasonably be mitigated through inherently safe solutions then reliable mechanical means are then considered. These include:

Prevention

basic process control

relief valves and flare systems

tandem pump seals

UPS

spare equipment (process pumps, lure oil pumps,)

Detection

process alarms

gas detectors

Control

emergency isolation valves to minimize releases

fire protection systems

dikes

building design

Mitigation through Instrumented Controls

Instrumented systems would normally be considered mitigation through mechanical controls, but with the requirements of ISA SP84.01, instruments must now be considered separately. If an instrumented system is to be used to mitigate a hazard, then this system is categorized as a safety instrumented system (SIS). In most instances these are the emergency shutdowns, trips and interlocks.

A distinction must be made during the mitigation process between those systems which function as basic process control systems (BPCS) and a SIS. The SISs are then listed and based upon the level of risk presented by the hazard, a safety integrity level is assigned so that the system will satisfy the required probability of failure on demand (PFD) value. The keys to this process are documenting which systems are SIS and the basis for the SIL.

With this information, the detail design such as the need for redundant inputs, solenoids or isolation valves can be finalized. Also considered during detail design is the ability to perform maintenance on these SISs without shutting down the process.

Mitigation through Operating, Maintenance or Administrative Procedures

Operating, maintenance and administrative procedures are usually the least reliable of hazard mitigating controls. Their use often depends upon current client or industry standards, and the unfeasibility of other mitigation mechanisms.

Example

During the design of one of Stone & Webster's ethylene plants, a design problem was encountered that could have had several alternative solutions. The process consisted of the vaporization of high pressure liquid ethane to a lower pressure so that it could be fed to the cracking furnaces. Failure of the pressure control scheme could potentially result in the overpressure of downstream equipment. Potential solutions to this problem included:

1. inherently designing the system by specifying its design pressure to be the same as the incoming source of ethane.

2. providing relief valves with sufficient capacity to prevent overpressure due to pressure control valve failure, or

3. providing a high pressure signal on the equipment that will trip the feed.

The first alternative was not deemed practical because of the impact to so many pieces of equipment and the high capital cost. Also, the pressure reduction of the feed has to occur prior to the cracking furnaces, so if not upstream of this equipment, then immediately downstream would be required, and the same overpressure scenario would still exist.

Evaluation of the relief valves was also discarded, because they would be extraordinarily large (and many).

The selected solution was to use a safety instrumented system to shut-off the feed on high pressure. The consequence of overpressuring the equipment and releasing high pressure liquid ethane was determined to have a very severe consequence. Since the failure of only one pressure control scheme could initiate the incident, a SIL of III was selected for this SIS. Final design of the system consisted of multiple inputs (high pressure trips) closing two independent valves on the feed line.

Example 2

The decoking of the inside of cracking furnace tubes is accomplished by isolating the furnace to be decoked from the process, and then slowly introducing air into the tubes to perform a controlled burning of the coke. Improper isolation of the hydrocarbon feeds or cracked effluents while decoking can lead to a release of hydrocarbons to the atmosphere or combination of air with the hydrocarbons within the process piping.

Depending upon the application of Stone & Webster or different client philosophies, mitigation of these hazards through the isolation of the decoking air has been accomplished in a variety of ways.

1. The decoking air line has a removal spool piece that that must be installed to begin the manual decoking process. The primary mitigation mechanism in this case is operating procedures.

2. The decoking air line has automatic valves that isolate it from the process. Prior to opening these valves, several permissives must be in place to insure that there are no hydrocarbon releases of mixing of the air and hydrocarbons. This was considered to be a SIS and an integrity value of SIL III was required.

3. As a third alternative, a combination of the two methods above was selected. Automatic valves were utilized, but spectacle blinds had to be turned prior to starting the process. In this case, the SIS for the automatic valves was required to only be a SIL I because of the additional protective layers.

Summary

During the normal course of process plant design, there are numerous opportunities to mitigate the hazards of the process. If the identification and mitigation of these hazards occurs in the early stages of the project, then the most opportunities for providing inherently safe opportunities or other means to remedy the hazard can be analyzed, and they can be implemented with minimal design and schedule impact.

With the publication of ISA SP84.01, the mitigation of hazards with instrumented systems has taken on an additional requirement of specific reliability requirements. Identification of process hazards and their consequences early in the project, also helps to specify these systems with minimal impact to the project design.

The ISA standard and comparable DIN and IEC standards primarily focus on safety to personnel and the environment. However, similar mitigation methods should also be utilized when mitigating hazards that do not necessarily impact personnel, but can damage equipment or cause business interruptions.

With all hazard mitigation, there is often several means to mitigate the hazard to an acceptable level of risk. In some instances several solutions might be utilized together to mitigate the hazard. When this is done, consideration should also be given to the independent relationship of these layers in determining their effectiveness. In regards to SISs, other layers of independent mitigation can be considered when

determining the SIL for the SIS. In some instance the SIL requirement can be reduced.

References

Center for Chemical Process Safety (CCPS). Guidelines for Safe Automation of Chemical Processes. New York: American Institute of Chemical Engineers.

Instrument Society of America (ISA). ISA-S84.01-1996, Application of Safety Instrumented Systems for the Process Industries. Research Triangle Park, NC: ISA.

To Mary Kay O'Connor Process Safety Center Home Page
To Program details for Day 1
To Program details for Day 2