Safety practice

Best practices for inherently safer equipment design and process design

Muhammad Zeeshan Ghazi
Process Engineering Department, Sipchem, Saudi Arabia

Summary

There are certain process engineering design methodologies or best practices which, when employed in the equipment design and process design stages of plant design, will deliver an inherently safer design. The inherently safer design thus becomes an intrinsic part of the process plant rather than a form of add-on protective equipment. The methodologies described in this paper for an inherently safer design are best practices, but they are not always practised. By structurally utilising these methodologies, they can and should be developed as RAGAGEPs (i.e., recognized and generally accepted good engineering practices), and used as an integral part of the process engineering design practice.

Keywords: Inherently safer design, equipment design, process design

Inherently safer design

During the conceptual process design and front end engineering design of a process plant, the inherently safer design can be achieved through application of good design practices for equipment design as well as process design. The best practices, which can lead to an inherently safer design, are discussed in the forthcoming sections of this article.

Equipment design opportunities

The equipment design opportunities, for different types of equipment and unit operations, which can result in an inherently safer design are described below.

Selection of appropriate material of construction

In April 2010, an explosion and fire led to the fatal injury of seven employees when a heat exchanger catastrophically failed at the Tesoro refinery in Anacortes, Washington. The draft report of this accident, issued by U.S. Chemical Safety Board (CSB)[1], indicates that the reason for this catastrophic rupture was due to 'high temperature hydrogen attack' or HTHA. CSB states that this accident could have been prevented had the company applied inherent safety principles and used HTHA resistant construction materials to prevent the heat exchanger cracking. CSB determined that inspections for such damage are unreliable because the microscopic cracks can be localized and difficult to identify. Therefore, CSB has concluded that inherently safer design is a better approach to prevent HTHA[2]. Using HTHA resistant materials is relatively better than inspections as these may fail to identify corrosion in large equipment or pipelines.

Similarly, in January 2010, the release of highly toxic phosgene at the DuPont facility in Belle, West Virginia resulted in a fatality. In this accident, a braided stainless steel hose with PTFE lining connected to a phosgene tank suddenly ruptured, releasing phosgene into the air. The hose was isolated from the phosgene tank at the time of accident, and phosgene inside the hose warmed up just before the accident. The heavy corrosion of the stainless steel overbraid, coupled with the time the hose had been in service and thermal expansion of the isolated liquid phosgene, caused the hose to fail catastrophically[3]. It is a known fact that phosgene can seep through permeable PTFE lining and can corrode stainless steel. Since it may be quite difficult to purge the hose every time it is isolated and to keep it phosgene free in all possible operating scenarios, the inherently safer method of avoiding phosgene leakages would be to use Monel hoses. Monel is the best choice of material of construction for phosgene service hoses.

These incidents indicate that using the appropriate material of construction for equipment and piping is the inherently safer design approach rather than using regular inspections or other passive methods.

Design practices for flammable liquid storage and transfer

In July 2007, a static spark resulted in an explosion inside a non-conductive flammable liquid storage tank at Barton Solvents Facility in Valley Center, KS. The incident led to the evacuation of thousands of residents, destroyed the tank farm, resulted in projectile damage offsite as well as extensive damage to the facility, and significantly interrupted Barton's business. The likely cause of the spark was the loose linkage of a liquid level gauging float in the storage tank[4].

From a pragmatic standpoint, such small things in industrial scale process plants cannot always be in perfect condition, and complete plants cannot be made foolproof. The following best practices could make the storage and transfer of flammable liquids inherently safer:

- High flow velocity of flammable liquid discharging into the vapour space of a tank can cause sufficient static levels to

© Institution of Chemical Engineers
0260-9576/15/$17.63 + 0.00

ignite flammable vapour inside the tank. Therefore, for flammable liquids discharging into a tank, a dip pipe submerged in the liquid is highly advised.

- The discharge velocity of flammable liquids into the tank should not be more than 3 ft/s (i.e., 0.9 m/s).
- It is advisable to inert a tank with nitrogen blanket unless there is a good reason not to.
- Goose necks and relief valve outlet pipes on flammable liquid tanks should have flame arrestors for protection against lightning unless there is a good reason for not doing it (e.g., polymerisation in flame arrestor, etc.).

Safe isolation of equipment

In June 2005, a fire and series of explosions occurred in an olefins production unit at Formosa's plant in Point Comfort, Texas. In this accident, sixteen workers were injured, the process unit was heavily damaged, and a nearby school was evacuated. The fire burned for five days. One of the contributory causes of this accident was the unavailability of remotely controlled isolation valves[5].

Due to the lack of remotely operated valves, Formosa's plant did not have a mechanism for controlling release of liquid propylene from a distillation tower, which eventually engulfed the whole plant. During this incident, plant operators had tried unsuccessfully to reach and close manual valves that could have stopped the release.

Therefore, equipment containing larger inventories of flammable or toxic fluids should have remotely operated emergency isolation valves, which should be as close as practical to the equipment flange and not in the piping away from the equipment. Additionally, for fire cases, air tubing for valve actuator can be of polyethylene, causing the valve to go to a fail-safe condition due to tubing being melted or damaged in case of a fire. If the valve is not located where a pool fire is likely, then additional fusible links in the air tubing can be placed at locations where a fire is likely to occur.

Best practices for preventing backflow

Inherently safer plants are designed to prevent backflow. Inadvertent backflow of streams in plants has caused several accidents in the industry. An inherently safer way to avoid backflow scenarios can be implemented by using:

- a combination of flow element and automated block valve, where the flow transmitter closes the valve on detection of backflow;
- a combination of differential pressure transmitter and differential pressure control valve, where the differential pressure transmitter closes the control valve on backflow.

These positive shutoff methods are considered superior to the conventional use of check valves for the prevention of backflow. Sometimes two check valves in series are used for backflow prevention, though they would not be as reliable as the aforementioned methods. If check valves are used for critical backflow applications, they should be inspected on a routine basis.

Appropriate piping components for avoiding failures

Check valves serve a major purpose in the process industry. Among different types of check valves, spring-loaded check valves provide more positive shutoff than swing check valves. Additionally, the potential for serious water hammer is much reduced if spring-loaded check valves are used. Swing check valves slam shut at the last moment, whilst spring-loaded check valves close smoothly and slowly. Therefore, appropriate selection of check valves also leads to inherently safer design of plants.

Similarly, expansion joints, which are used to minimise or isolate effects of thermal expansion, vibration, load stresses, etc., become the weak link in the system and can be an inherent source of failure. Therefore, expansion joints should be used only where absolutely necessary, and other alternatives such as electronic load cells, piping loops designed for expansion, etc. should be used.

Avoiding seal leak incidents

There have been several incidents in industry involving seal leaks from pumps, which have caused fires or personnel exposure to toxic process liquids. An inherently safer way to avoid such incidents is to use seal-less pumps wherever possible. Seal-less pumps improve safety from reduced seal leaks.

Among seal-less pumps, magnetic drive pumps are safer than canned motor pumps. Magnetic drive pumps have thicker cans, and have greater clearance between rotor and can as compared to canned pumps.

If seal-less pumps cannot be used for some reason, double-seal pump or tandem-seal pumps should be used to avoid seal leak incidents.

Process design opportunities

The process design opportunities, which can result in an inherently safer design are described below. These methodologies are primarily based on the work of Professor Trevor Kletz[6]. Examples from real-life plant incidents are quoted to emphasize the importance of following the design concepts of intensification, substitution, attenuation and limitation.

Intensification

This method employs the concept of using or storing so little amount of hazardous materials that it hardly matters if it all leaks out. This methodology also proposes that when finalising designs of distillations columns, reactors, exchangers etc., we should choose designs with small hold-up of hazardous materials wherever possible.

A good example of intensification is the production of nitroglycerin. Historically, nitroglycerin was produced batch-wise in large stirred pots containing about a ton of material where temperature was closely monitored. It was later revealed that the chemical reaction of reactants for the production of nitroglycerin is not slow – it is the mixing of reactants that is slow and therefore demands reactors of bigger inventories and longer residence times. In the new design, the

© Institution of Chemical Engineers
0260-9576/15/$17.63 + 0.00

reactor was very well mixed and this reduced the residence time from 120 minutes to 2 minutes. This new design resulted in significant reduction of inventory of hazardous materials in the plant as well as a significantly smaller reactor with less add-on protective equipment[6].

Substitution

This methodology is about replacing a hazardous material by a less hazardous one.

An example of substitution is the use of cyclohexane as a solvent instead of benzene, which was used in the past. Benzene is immediately toxic in high concentrations and produces long-term toxic effects in low concentrations. Cyclohexane is less toxic than benzene and has a higher flashpoint, and this makes cyclohexane inherently safer[6].

Attenuation

This method focuses on the fact that if we have to store or handle large amounts of hazardous material, we should store or handle it in the least hazardous form.

An example of attenuation is compounding the ammonium nitrate fertiliser with calcium carbonate (limestone) which eliminates the risk of explosion in its storage, transportation, and handling. The massive explosion in West, Texas in April 2013, which caused 14 fatalities and hundreds of injuries, was caused by detonation of approximately 30 tons of ammonium nitrate stored in a warehouse[7]. Calcium ammonium nitrate fertilisers have been widely used in Europe, and are inherently safer throughout the supply chain of this fertiliser.

Similarly, storing or transporting organic peroxides, which are liable to decompose spontaneously, in solution form is another example of moderation.

Limitation

This technique involves limitation of effects by equipment design or by limiting the energy available, rather than by adding on protective equipment.

For example, if unstable chemicals have to be kept hot, the heating medium should be incapable of overheating them. In Seveso's accident in Italy in 1976, a batch reactor heated by steam at 190°C went into a runaway reaction as the steam temperature from an extraction turbine rose to about 300°C[6]. An inherent process design approach would avoid the increase in steam temperature beyond its normal temperature set point.

Conclusion

As demonstrated by several real-life examples in the preceding sections, it is clear that utilising best practices for equipment design and process design can lead to an inherently safer plant with significantly less instrumentation and add-on protective equipment. This methodology not only improves the safety of the plant but also reduces the capital as well as the operating expenses of the plants. Therefore, the inherently safer design approach should be developed as an integral part of the process engineering skills set, to be widely used during process engineering design activities.

References

1. U.S. Chemical Safety Board, Tesero Draft Report for Public Comment, Report No. 2010-08-I-WA, January 2014
2. CSB News Release about 2010 Tesoro Refinery Fatal Explosion, 29 January 2014, http://www.csb.gov/csb-investigation-finds-2010-tesoro-refinery-fatal-explosion-resulted-from-high-temperature-hydrogen-attack-damage-to-heat-exchanger/ (accessed Feb. 10, 2014)
3. U.S. Chemical Safety Board, DuPont Belle Toxic Chemical Releases, Report No. 2010-6-I-WV, September 2011
4. U.S. Chemical Safety Board, Barton Solvents Explosion and Fire, Report No. 2007-06-I-KS, June 2008
5. U.S. Chemical Safety Board, Formosa Plastics Propylene Explosion, Report No. 2006-01-I-TX, July 2006
6. Kletz, T. What Went Wrong. 5th Edition, 2009
7. Preliminary Findings about 2013 West Fertilizer Explosion and Fire, http://www.csb.gov/assets/1/19/West_Preliminary_Findings.pdf/ (accessed Feb. 10, 2014)

© Institution of Chemical Engineers
0260-9576/15/$17.63 + 0.00