ELSEVIER

Journal of Hazardous Materials 104 (2003) 149–161

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Designs that lacked inherent safety: case histories☆

Roy E. Sanders*

PPG Industries, P.O. Box 1000, Lake Charles, LA 70601, USA

Abstract

The fundamentals of Inherently Safer Design were not fully appreciated in the initial design (or re-design) in the following series of case histories. Two case histories involving the basic element of plant layout to minimize property damages and injury will be covered first. Simple physical separation could have reduced the losses. A case history that occurred in a bulk chemical terminal tank farm will highlight designs which allowed incompatible chemicals to react, create a fire and a lingering toxic gas release. The combination of these chemicals caused equipment damage in one case and a threat to the public in another case. This paper will conclude with case histories involving poor piping design or poorly identified piping systems, which needlessly resulted in expensive repairs.

Exercising the principles of inherent safety would have reduced the severity and perhaps the opportunity of these events. We must employ the techniques of inherent safety to improve our performance.

Keywords: Inherently safer plants; Chemical plant accidents; Incompatible chemicals; Chemical plant layout

1. Introduction

"Inherently Safer Design concepts are particularly useful for risk reductions and are highly recognized and recommended by safety professionals as a first choice in process design practices. 'Inherently Safer Designs' are designs where engineers employ a variety of techniques to achieve classical risk reduction through design. These methods include, Hazard Elimination, Consequence Reduction and Likelihood Reduction". This is an opening quote from Moore in a recent excellent paper on Inherently Safer Design [1]. Today's paper focuses on examples of designs that failed to employ one or more of those principles.

☆ This paper was presented at the *Beyond Regulatory Compliance Making Safety Second Nature Symposium* at the Mary Kay O'Connor Process Safety Center on October 29, 2003.

* Tel.: +1-337-708-4322; fax: +1-337-708-4678.
E-mail address: rsanders@ppg.com (R.E. Sanders).

0304-3894/$ – see front matter
doi:10.1016/S0304-3894(03)00241-3

Sometimes we need to see a poor example to appreciate the need for a good design. Several of the examples that follow were from an era when many inherent safety techniques had not been preached or accepted. One example, the Flixborough incident, was the catalyst to spark concerns for the need for Inherently Safer Designs. Other examples of incompatible chemicals and deceptive piping designs occurred in the last decade.

2. Facility siting

Facility siting is a very critical fundamental of Inherently Safer Design. It is one of those concepts that must be applied early in the design to be cost effective.

3. A heater is located too close, an accident and significant damages

A major fire erupted in a non-flammable solvents manufacturing unit in a US. Gulf Coast chemical complex at about 3:00 p.m., on a Wednesday afternoon. Fortunately, no one was injured. A heater tube in a natural gas-fired heater ruptured due to overheating of a stagnant fluid. The heat-transfer oil was combustible. The resulting spill was at least 1800 gal and quickly ignited. The fluid burned intensely and it was described as a “spectacular fire” by a local newspaper. Within about 25 min, the intense hot fire damaged four levels of structure and associated process equipment. The plant on-site emergency squad quickly and properly responded. However, this short-lived event ended up with a price tag of over $ 1.5 million in direct property damage and over $ 4 million in business interruption (costs are in 1979 US dollars) [2].

The solvents manufacturing area utilizes five large 9 ft diameter gas phase reactors to produce solvents. The process design requires a startup heater to bring the gaseous streams to an elevated temperature to obtain the initiation of the reaction. A large volume of high-boiling, combustible, heat-transfer fluid transports heat from the heater to the reactors. A single natural gas-fired, startup heater equipped with 6 in. diameter tubes, is shared by all five reactors.

Chemical plant operators use a single heater to startup one reactor at a time. The reaction, once underway, is exothermic. So once a reactor is up to full production, the heater is shutdown and the operator isolates the heater circulation loop from that reactor. When another reactor is scheduled for startup, the process is repeated. The operator aligns the valves, starts the circulation pump, ignites the heater burner and brings the reactor up to temperature.

Investigators determined that during a hectic day of operations, the chemical process operator erred. On this afternoon, he inadvertently tried to startup the heater with the burner firing and the heater tubes isolated from the circulating pump by closed blocked valves. Shortly after firing the heater, the lead operator traveled to the heater and checked the flame pattern. He recalled nothing out of the ordinary.

Within 20–35 min after the heater was fired, a firewater sprinkler system tripped. A heater flame failure alarm occurred a short time later. Witnesses stated flames were over 50 ft high in approximately 5 s after the tube ruptured.

Current property insurance guidelines require a fired heater to be located at least 75 ft from a process structure. However, in this earlier design the heater was located very close to four levels of heat exchangers and other process equipment. Fire and destructive heat damages were much more extensive than they should have been due to the close proximity and the unfavorable 10–12 mph winds carrying the fire into the structure. Fire damages were the greatest on the third and fourth levels of the process unit.

There was an excellent response by the emergency squad with eight hose lines reinforcing the fixed firewater deluge systems. Physical damages were high and the recovery time was long. It took several months to rebuild the damaged systems. Active protection was good, but a 50–75 ft gap between the equipment and heater would have been much more effective and inherently safer.

This incident required a full and detailed investigation by members of technical, engineering, operations and process safety groups. Investigators made numerous interviews and detailed observations. Inspectors found a 6 in. long and 4 in. wide hole on a ballooned section of a heater tube. Normally the tube had a 6.6 in. outside diameter, but it had swollen to about 8.0 in. in diameter at a point about 2.5 ft above the heater floor.

As best as it could be determined after the fire damage, the original protective instrumentation system was still in place at the time of the fire. There were no records documenting that prooftesting and/or preventive maintenance of the instrumentation was achieved even though it was known that some periodic maintenance had been performed. At that time, there was no systematic program in place to ensure periodic inspection, testing and record-keeping of this critical instrumentation [2].

From today's Process Safety Management perspective, some knowledgeable investigators could develop a list of corrective actions in both mechanical integrity and operator training, and other investigators could question the degree of engineered-safety-shutdown systems. They would be correct. Others could say there were human factors involved. They both would be correct.

While human error played a major role, and a weak PSM Mechanical Integrity Program were some of the chief reasons for the accident, a better original layout would have drastically reduced the damages. The severity of the damages was basically a facility siting issue. The gas-fired heater was originally adjacent to the process with little separation. Current property insurance guidelines require that a gas-fired heater be located at least 75 ft from a major process structure. Application of proper spacing can be an effective damage-limiting inherently safer concept.

4. The Flixborough incident and the administration and control buildings

Kletz once wrote, "The explosion in the Nypro factory at Flixborough, England, on 1 June 1974 was a milestone in the history of the chemical industry in the UK. The destruction of the plant in one almighty explosion, the death of 28 men on-site, and extensive damage and injuries, though no deaths, in the surrounding villages, showed that the hazards of the chemical industry were greater than been generally believed by the public at large [3]".

The periodical Fire Protection—The Journal of the Fire Protection Association introduced their article, "Anatomy of a Disaster", on 1 June 1974 an explosion of tremendous power destroyed the works of Nypro (UK) Ltd., killing 28 and injuring 36 of the people working there. In the surrounding districts injuries to 53 people were recorded and hundreds more suffered minor injuries. Buildings and plant on the site were virtually completely destroyed by the explosion an ensuring fire. Outside the works the explosion damaged property as far away as 4 mile from the works [4].

The details of this tragedy are well written in many articles. Some authors describe the tragedy as an explosion of warlike dimensions, in which 1821 houses and 167 shops and factories suffered damage to some degree. The Nypro works (or chemical manufacturing complex) was on a 60 acre site and the area around it was mainly farmland. The villages of Flixborough and Amcotts were each located about a half-mile away [4,5].

Production of caprolactam (an intermediate for making Nylon 6) began in 1967 at this site. A new “phase two” plant was designed and completed in 1972. The phase two area of the plant was the area in which the reactor piping system failed and the vapor cloud originated [4].

The setup for the incident occurred when the Reactor No. 5 of a series of six reactors developed a crack. The pressurized reactors converted a hot flammable liquid, cyclohexane, with a flash point of minus 20 F and a boiling point of 181 F into a mixture of flammable and combustible liquids. This mixture was transferred to another unit then converted into caprolactum and pumped to another area to be converted into nylon.

The crack was discovered at the end of March 1974. Each reactor was about 12 ft in diameter and 16 ft long and operated at about 125 psi and about 311 F (well above the flash point and the boiling point of cyclohexane and one of the chemicals in the mixture). Once the crack was discovered, a decision was made to remove the reactor for repairs and install a piece of 20 in. by-pass piping connecting Reactor No. 4 to Reactor No. 6. The crew must have been proud that they were able to provide this by-pass line and restart the system in less than a day [5].

The temporary 20 in. diameter piping was installed between two expansion joints. The only calculations made were on the capacity of the piping to carry the required flow. No calculations were made to determine the strains that may occur on the expansion joints in this system. No one reviewed any relevant British Standard or other standard to see if this was acceptable. No reference was made to the designer’s guide supplied by the expansion joint manufacturer. No engineering drawings were made, except for a chalk sketch on the shop floor. No pressure testing was performed. Sources indicate it was viewed as routine plumbing job.

No one appreciated the dog-legged assembly would be subject to a turning moment. And no one seemed to be aware that it was supported by scaffolding suitable for working people, but not sturdy enough for supporting heavy liquid-filled piping. Having mentioned all of the shortcomings of the system, the unit operated successfully with the temporary by-pass piping in place for the period from the end of March–29 May 1974. It was shutdown to repair some unrelated leaks.

During startup on Saturday, 1 June 1974, containment was breached. In the first minute or so about 50 t of inventory escaped, vaporized, ignited and resulted in a massive vapor cloud explosion that the world had not seen before within chemical plants.

A British Court of Inquiry held open hearings for a total of 70 days with evidence from 173 witnesses. A full discussion of the incident is well beyond the intent of this paper. Over the past three decades, many individuals refer to this incident as a classical example of the need for a Management of Change (MOC) Program.

However, other lessons on plant layout are equally important. According to all of the official reports and the articles by Kletz [6] and Lees [7] there were some severe layout issues. One section of the Lees' work reads [8]:

> "The blast of the explosion shattered windows of the control room and caused the control room to collapse. Of the 28 people who died in the explosion, 18 were in the control room. Some of the bodies had suffered severe injuries from flying glass. Others were crushed by the roof. No one escaped the control room".

"The main office block was also demolished by the blast of the explosion. Since the accident occurred on a Saturday afternoon, the offices were not occupied. If they had been, the death toll would have been much higher". There may have been up to 100 more deaths within the main office area if the explosion occurred during a regular workday. Diagrams show that the reactor area and its large inventory of flammable material was within 30 m (about 100 ft) to the south of the main office building. The main control room was also about that distance in a northerly direction from the reactor area.

Today's engineering procedures call for a reliance of property insurance guides for layout and/or for vapor cloud calculations to locate buildings in facilities that manufacture or store highly hazardous chemicals.

5. Conclusions on facility siting

To emphasize what we have learned in the past few decades, I will repeat the first two sentences of this section. Facility siting is a very critical fundamental of Inherently Safer Design. It is one of those concepts that must be applied early in the design to be cost effective.

5.1. Incompatible chemicals

Another concern for inherent safety is to keep reactive chemicals isolated until you want them to react. Incompatible or reactive chemicals often appear fairly mild mannered or non-threatening by themselves, but can undergo uncontrolled reactions when improperly processed or combined. These reactions can result in explosions, fires, and toxic releases. Such accidents are not unique to the chemical manufacturing industry but occur in many other sectors where chemicals are stored, handled, and used.

6. Savannah incident background

There were two such reactive chemical surprises occurring at a shipping terminal in April 1995. One design (a recent modification) created a reaction and the initiating fire. The tank farm-fire damage and storage practices created the lingering toxic release. This Savannah, GA, terminal handled liquid chemicals was located a little more than a half-mile from the

Savannah River. It was about 2 mile from the downtown area in Savannah. This transfer facility served the paper and pulp industry and provided chemical storage for "third-party" suppliers. The facility could receive and send chemicals by water, rail and the highway systems [9].

The entire incident is well described and well documented in a 15-page report by Chung of the United States Environmental Protection Agency. Chung's paper is entitled "Explosion and fire at Powell Duffryn Terminals, Savannah, GA". The focus of the incident could be directed also to the lack of MOC or equipment layout, but today's paper will view a small section of the EPAs report covering reactive chemicals [9].

Just before midnight on Sunday, 10 April 1995, fire erupted at the terminal. The terminal was unmanned at 11:30 p.m. when the fire started. Several witnesses observed a flash followed by an explosion and fireball. The firefighters had difficulty in entering the area due to the intensity of the fire [9].

Flames and thick black smoke from the fire forced residents of the adjacent town-home development to evacuate. The company's office building and records on-site were destroyed. If you are interested in all of the details, the EPA has published a 74-page report available on the worldwide Web. The report is titled: EPA Chemical Accident Investigation Report, Powell Duffryn Terminals, Inc., Savannah, GA, EPA 550-R-98-00, EPA CEPPO (http://www.epa.gov/swercepp/pubs/pdtirept.pdf) [10].

The fire originated within tanks in a diked area roughly 100 ft × 200 ft. The enclosed area contained six tanks that were constructed in April 1992, in accordance to API-650 standards. The six tanks were built in three sizes and the smallest two were about a 237,000 gal (or roughly a quarter of a million gallons).

For the first years of operation there were no flammables in the area. However, the company changed its strategy and started storing class a IC flammable liquids (crude sulfate turpentine) several months before. Safety systems were requested by agencies and planned by the owners, but were incomplete at the time of the incident.

7. Tank vent treatment

Foul smelling fumes from the crude sulfate turpentine escaped the tanks during tank fillings and as the ambient temperatures increased. Malodorous tank vapors must have been routine. The plan was to solve the problem by routing these offensive fumes to drums with activated carbon [9,10].

EPA Investigators determined that the most-likely ignition scenario involved an auto-ignition from the carbon beds. About 2:00 p.m., on the day of the incident the flammable tanks were initially and effectively sealed when firefighting foam chambers were installed on the tanks. That afternoon, after the tanks vent system was closed a tank truck of 6200 gal of crude sulfate turpentine was delivered and off-loaded into the tanks. This meant at least 6200 gal of fumes had to be displaced from the vapor space. The fumes on this unusually hot (90 F) April day were routed through the activated carbon bed in 55 gal drums. The low level of oxygen in the drums apparently averted an immediate fire. Process safeguards for the carbon beds were discussed. A flame arrestor was purchased and received to be placed on the vapor line from the tanks. The flame arrestor was not installed yet.

8. Incompatible chemicals—carbon beds and flammables

The body of evidence points to the oxidation of the flammable material (condensed fumes) on activated carbon as the ignition source. No doubt that cooler evening temperatures caused the vapors in the tanks to contract. Air was drawn into the drums. Auto-ignition of the turpentine on carbon occurred and resulting flame traveled back to the tanks [9,10].

The EPA report describes an article which documents a history of fires in drums containing activated carbon in systems that allow air to be drawn into the drums. The reference article specifically mentions that typically the fires have occurred late at night following a hot sunny day when the nighttime cooling of the storage tanks cause vapor volume to contract and draw outside air into the carbon beds.

9. The fire scenario

Prior to the storage of the flammable liquid (crude sulfate turpentine), there were no flammable materials in this enclosure. A fixed foam-piping fire suppressing system specified by agencies. This protection package was accepted by terminal managers. The system had not been fully completed, despite the fact that flammables had already been stored for 22 weeks [9,10].

When the fire broke out, the more convenient foam fire protection piping system located outside of the enclosure was incomplete and this delayed the extinguishing efforts. Eventually, firefighters were able to enter the enclosure and connect their hoses to the incomplete system to apply foam. The fire was completely extinguished after 3 days.

10. Incompatible chemicals—stored in the same enclosure

If it were not bad enough to have a fire started by incompatible chemicals, think about the results of a severe fire and two reactive chemicals within the same enclosure that would generate toxic fumes when mixed. (This inherent safety blunder could have been covered also in the previous section under plant layout.)

According to the EPA report, three of the tanks had a total of 630,000 gal of flammables, one of the tanks contained 34,000 gal of sodium hydrosulfide (NASH) as a 45% solution in water. One tank contained Briquest, a cleaning agent solution and another was nearly filled with a relatively non-hazardous material [9,10].

The fire and explosion extensively damaged tanks and piping within the enclosure. Damaged equipment allowed leakage of Briquest which was a strong acid with a pH of about 1 to react with leaking sodium hydrosulfide (pH 10.4–11.5). Foul smelling, flammable, toxic hydrogen sulfide gas was generated when sodium hydrosulfide is acidified by the Briquest. Naturally, the toxic fumes hampered the cleanup efforts.

You can get an idea of the severity of the situation from a direct quote from page 11 of the technical paper. “At the start of the cleanup operations, after the fire was extinguished, all residents within one-half-mile of the facility were evacuated as a precautionary measure because of the generation of toxic hydrogen sulfide gas. Overall, nearly 2000 people were involved in the evacuation. Most of the evacuees were allowed to return after a few days, but the evacuation lasted more than 30 days for the residents closest to the site of the fire". Based upon hospital records, about 337 people reported to local area hospitals emergency rooms during the fire and cleanup. However, there were no admissions or follow-up treatment required [9,10].

11. Root causes and contributing factors

Here are several of root causes and contributing factors that were identified. The design of the vapor control system was inadequate, including the lack of flame arresters:

- The foam fire suppression system was not fully installed and not operational of the three tanks containing flammables.
- Incompatible chemicals were stored in the same walled enclosure area.

12. Recommendations

The EPA report made the seven major excellent recommendations and many of those could be subdivided into additional recommendations. The following list is a combination of their ideas with the emphasis on reactive chemicals. To see the entire set of recommendations, please see their report:

- Facilities designing or adding on environmental control, fire safety or hazard control must ensure that these systems do not adversely impact the process or equipment. This seems to be an endorsement for OSHAs MOC (for a non-covered process).
- Where such control systems, safety devices, or emergency systems are added they must be properly designed, installed and fully operational. This seems to be an endorsement of OSHAs Pre-Startup Safety Review (for a non-covered process).
- Facilities using activated carbon systems, in conjunction with experts should conduct tests to determine the potential for formation of hot spots, runaway reactions, etc. (This is a sort of reactive chemicals review.)
- Facilities should examine process and storage areas and equipment to ensure that potentially incompatible substances are kept adequately separated. The design should be such that leaks or spills of highly reactive or incompatible chemicals are not collected within the same containment.

13. Afterthoughts

The topic of reactive chemicals has gained considerable attention lately. On 30 May 2002, a press release provided by the Chemical Safety Board (CSB) began with "Reactive chemicals accidents pose a "significant problem" and the relevant federal accident prevention regulations have a "serious gap" according to the preliminary report findings . . . ". The press release continues "CSBs findings were based on an examination of 167 separate incidents that occurred since 1980 and caused 108 deaths related to reactive chemicals". Obviously the limitation in the quantities and control of reactive chemicals is a principle of Inherently Safer Design.

Information on the safety of carbon beds, which should be considered reactive, may be obtained from various sources including the manufacturer, Loss Prevention, vol. 12, American Institute of Chemical Engineers, 1979, etc. However, if you wish to get immediate information from the worldwide Web, the EPA has developed a very helpful *Chemical Safety Alert* entitled "Fire Hazard from Carbon Adsorption Deodoring Systems". The Web address is: http://www.epa.gov/swercepp/pubs/carb-ads.pdf.

14. Deceptive piping arrangements

Another principle of inherently safer plants is to keep instrument controls and piping simple and easy-to-understand. There were both human factors and deceptive-looking piping connections that contributed to the next two incidents.

15. Clearing a piping system

Before sunrise on a November morning, operators were in the process of preparing piping headers for scheduled maintenance. Two well-respected, well-trained, conscientious employees were covering the night shift when they inadvertently connected a utility air hose to the wrong pipeline. They hooked up to the adjacent line which was pressurized with a flashing acidic liquid. This action allowed the higher pressured acidic gas (about 250–290 psi) to backflow into the (90–100 psi) utility air system.

The piping arrangement under nighttime conditions was deceptive in geometry and camouflaged by the rust colored primer versus the bright yellow colored paint of the adjacent fittings. There were three parallel 2 in. pipelines below the grating on the second level; each line had purge connections that confused the team (see Fig. 1 for details).

Each of the three pipelines had individual 3/4 in. horizontal purge piping connections were equipped with 3/4 in. quick connection fittings for purging. This piping and associated 3/4 in. valves were near the grating level. There were also three 4 in. diameter vertical bottles which were properly labeled. However, the purge connection for the north bottle was directly in front of the middle bottle. The purge connection for the middle bottle was directly in front of the south bottle and the purge connection for the south bottle was not painted the same bright yellow color. Lighting was fair.

The task of clearing pipelines for maintenance is almost second nature to well-experienced operators in this unit. Typically, pipeline clearing is routine and is uneventful. This time, however, the dry-air system was also being utilized as a source for instrument air in the operating area. Hence this corrosive material could backflow and create expensive instrument damages.

Initially fumes were found throughout the area. It was difficult to identify the source of the leak. As a good operator response, the operators stopped the clearing procedure which isolated the source, even though they were unaware of this at the time. Residual acidic gases

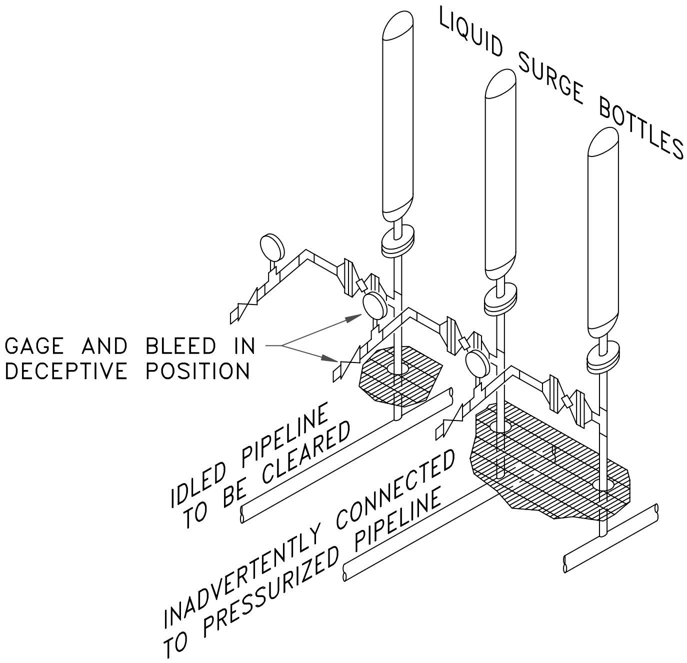

Fig. 1. Pipeline clearing incident.

in the header began to leak from air bleeds, purge points and leaks and continued for over 4 h. Most of the material was recovered to the sniff system.

A preliminary investigation into the incident was begun immediately as the leak was underway. The erroneous hose hookup was identified, as the source about 6:00 a.m., despite the fact it was isolated much earlier. Immediately after that steps were taken to clear the line and recover the fluid. A formal investigative team was formed. The team members included the Unit Supervisor, the Emergency Coordinator during the incident, an Engineering Services Supervisor and others.

16. Impact and conclusions

Damage to analyzers and instrumentation from the intrusion of acid gases into the instrument air system was extensive. Repair costs were about $ 300,000.

The investigating team concluded:

- The investigating team determined the accident was a result of human error by talented, well-trained, dependable operators. The operator took several steps to change fittings to make the hose connection. The piping arrangement was deceptive in both geometry and paint color. Under nighttime lighting conditions the piping connections are even more misleading.

- The use of the 100 psi dry-air system for instrument air must be reviewed.
- The release resulted from backflow of a corrosive into a utility air header as a result of human error, and the subsequent leaking from purges, bleeds and leaks on the instrument air system that was being supplied from the utility air system.
- Quick response by the operators in shutting down the clearing operation, even though it was not suspected to be the source, aided in minimizing the amount entering the air system. The professional response by the emergency squad was very good.

17. Recommendations for this piping incident

The investigation report stated:

- Ensure that elements of this incident are discussed with a large group of operators throughout the complex to remind them of the significant problems that can occur with hoses and the value of double and triple checking.
- Improve the situation to reduce the deceptive appearance of this area and check for similar situations in that area.
- Study of the 100 psi dry-air to determine proper use of the air system. The focus of this study is to discourage the habitual use of the dry-air system as an instrument air source.

The investigating report did not specifically say that there was also human error on the part of the piping designer/installer that contributed to the deceptive appearance and the people that reviewed the installation, but it could have done so. These type of situations cannot be seen on P&IDs. Piping systems and situations that appear "counter-intuitive" can yield mistakes more easily.

18. A well-intended change yields a storage tank collapse

A perfectly good low-pressure solvent tank ended up as useless scrap metal after the vent system had been "improved". This early 1990s mistake cost about $ 100,000 to correct. Fortunately, there were no leaks and only egos were injured when the 20 ft in diameter and 30 ft tall vessel was destroyed. Prior to the incident, this unit was reducing volatile organic emissions step-wise within a tank farm by replacing simple hinged-breather vents with a more sophisticated nearly zero leakage system [11,12].

Plant supervision properly recognized this environmental improvement project as requiring a simple MOC Review. The evaluation was complete. Pre-startup training for the newly installed but not yet operational vent compressor system was underway, but had not been given to each shift of operators. Engineers focused the training on the new compressor system. The training did not cover the newly installed-piping and the unique valving associated with the new over- and under-pressure devices.

The solvent tank was returned to service and was filled to the proper level. The roof and top two courses of 1/4 in. thick vertical walls were dramatically sucked in the first time the contents were pumped out after vent improvements. The product was analyzed and a transfer from the tank was started in the early evening. The collapsed sections of the tank were observed before sunrise the next morning.

For two decades this non-flammable solvents tank successfully operated with a nitrogen pad to reduce moisture intrusion and a simple hinged-breather vent to provide overpressure and vacuum protection. The modification (installed and completed just 3 days prior to the failure) provided a vent compressor and a new state of the art nearly zero leakage pressure/vacuum device and some unique piping features [11,12].

The unique feature was a block valve on the impulse line to the pressure/vacuum device and the nitrogen regulator. It conflicted with the plant's normal engineering practices for relief devices, but was normal for control instrument impulse.

Investigators established that the root causes of the incident were:

- Failure to train employees on proper operation of the modified tank vent system.
- Failure to make sure that *all* personnel involved had been properly trained.
- Failure to follow MOC guidelines before putting new equipment in service.

With all due respect to the findings of the investigating team, the root cause appears to be an inherent unsafe design. The new piping system looked simple but in fact this unique system was confusing. A check valve was installed on the vent header to prevent cross contamination. A small block valve was installed on the vacuum relief impulse line to provide easy isolation (see Fig. 2 for more details).

A small block valve is usually installed at the tank on any instrument impulse line just in case a leak develops on the small tubing. In this unit block valves are generally avoided on overpressure or vacuum relief devices. If a block valve which can defeat an overpressure device cannot be avoided, such a valve is locked open or car-sealed opened and a

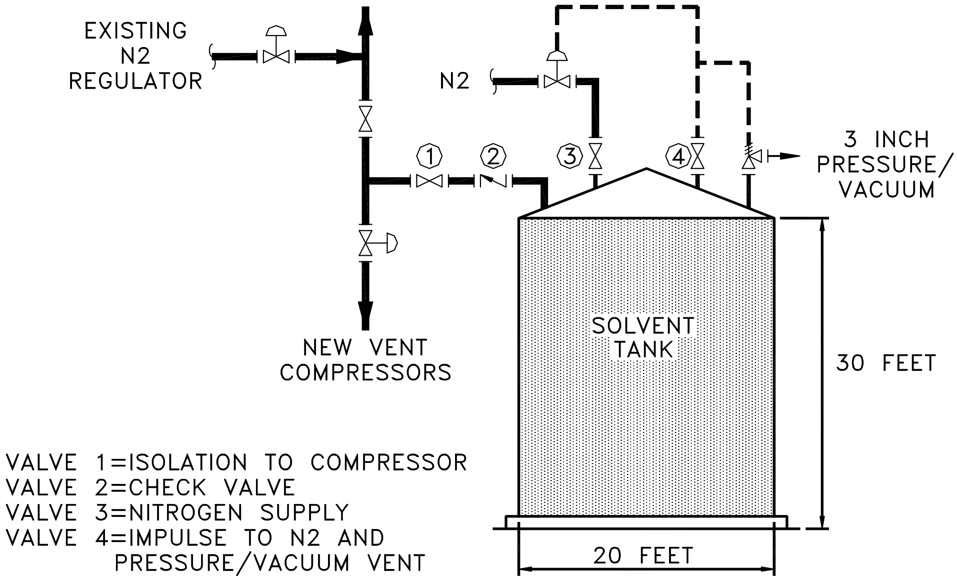

Fig. 2. Blocked impulse valve incident.

protocol is developed to administratively control accidental closing of such a prime safety feature.

The investigating team made several training and MOC recommendations and decided to eliminate the impulse valve (valve no. 4) connected to the pressure/vacuum vent. The elimination of the impulse valve removed the unintended trap for the operators.

19. Afterthoughts on deceptive piping arrangements

Plant designers must strive to develop user-friendly piping, layout and control schemes, as well as clear, unambiguous labeling on equipment safety systems to reduce opportunities for human factor failings.

20. Conclusions

Why Inherently Safer Designs? If Inherently Safer Designs were employed, these five case histories may have been prevented or at least diminished to the point that you would not be hearing about them.

References

[1] D.A. Moore, Incorporating Inherently Safer Design into process hazard analysis, in: Proceedings of the Mary Kay O'Connor Process Safety Center Symposium on Beyond Regulatory Compliance Making Safety Second Nature, College Station, TX, 1999, p. 327.
[2] R.E. Sanders, W.L. Spier, Monday morning quarterbacking: applying PSM methods to case histories of yesteryear, in: Process Safety Progress, Winter, American Institute of Chemical Engineers, New York, 1996, p. 189.
[3] T.A. Kletz, Learning from Accidents in Industry, Butterworths, London, 1988, p. 63;
T.A. Kletz, Learning from Accidents in Industry, 3rd ed., Gulf Publishing, Woburn, MA, 2001, p. 83.
[4] Anatomy of a Disaster—Flixborough Report, Fire Protection—The Journal of the Fire Protection Association, vol. 110, August 1975, UK, p. 13.
[5] S.F. Warner, The Flixborough disaster, Chem. Eng. Prog. 71 (9) (1975) 77–84.
[6] T.A. Kletz, The Flixborough cyclohexane disaster, loss prevention, Am. Inst. Chem. Eng. 9 (1975) 106–110.
[7] F.P. Lees, Loss Prevention in the Process Industries, vol. 3, 2nd ed., Appendix 2, Butterworths/Heinemann, London, 1996, pp. A2/1–A2/19.
[8] F.P. Lees, Loss Prevention in the Process Industries, vol. 3, 2nd ed., Appendix 2, Butterworths/Heinemann, London, 1996, p. A2/7.
[9] D. Chung, Explosion and fire at Powell Duffryn Terminals, in: Proceedings of the 34th Annual Loss Prevention Symposium (LPS 2000), Savannah, GA, American Institute of Chemical Engineers, Session 48, March 2000.
[10] EPA Chemical Accident Investigation Report, Powell Duffryn Terminals, Inc., Savannah, GA, EPA 550-R-98-00, EPA CEPPO, May 1998. http://www.epa.gov/swercepp/pubs/pdtirept.pdf.
[11] R.E. Sanders, Human Factors: Case Histories of Improperly Managed Changes in Chemical Plants, Process Safety Progress, New York, Fall 1996, pp. 150–153.
[12] R.E. Sanders, Chemical Process Safety: Learning from Case Histories, Butterworths/Heinemann, London, 1999, pp. 30–34.