3,590 Words

The Argument for Getting It Right

During these challenging economic times, companies are driven to maintain performance at the same time minimizing cost, a formula that can lead to short-cutting.

Among architects and engineers, it is tempting to recycle old designs. Worse, there is a tendency to rely on minimal code compliance and project budgets for fire protection based on "factoring", a formula that may or may not be in alignment with commercial reality. This formula can lead to human tragedy and environmental disaster.

Minimal code compliance is an arena in which best practice and a higher level of technical safety may be sacrificed in the interest of cost reduction. Although fire codes are periodically updated, these minimal measures necessary to secure approval by governmental authorities may nonetheless leave a facility potentially unsafe to operate. The International Fire Code leaves it to the discretion of the local fire official (there may not be one, depending on location) as to whether or not a fire suppression system should be installed on a hydrocarbon storage tank.[1] Fire codes in general are moving from a prescriptive to a more risk and performance based approach, with an industry dictating solutions to the authority having jurisdiction who often does not understand the issues involved in historical prescriptive requirements. At the end of the day, what gets approval – the lowest cost producer – is the outcome of an exercise in commercial evaluation.

During the engineering and construction of downstream petroleum products storage facilities owned by terminal operators and product end users such as electrical power utilities, the authority with the most to lose but the least say on what is permissible is often the insurance underwriter. Unlike legislated national building and fire codes, industry codes and standards such as API, NFPA, and the FM Global system, which on the whole reflect best practice, are not law but merely recommendations. Nonetheless, engineers rely on them as a standard for good practice with which they generally strive to comply.

Insurance underwriters are sometimes held hostage by the industry they endeavour to safeguard. Pipeline terminal operators, for example, have typically not installed fire detection and fire suppression systems on large diameter storage tanks unless the tanks are over 45 meters in diameter, a dimension beyond which local fire codes may require it.[2] Facilities owners are prepared to argue that compliance with the minimal separation distances outlined in the fire codes is sufficient, ignoring the nature of tank and containment area fires which can be multi-dimensional in character and, in the case of a vapour cloud, do not respect fire breaks and other passive fire protection measures.[3] They "risk assess" their way out of needing to adequately protect the tank farm, with risk decisions being made on faulty data.

If the tanks are fire code separated and therefore compliant, underwriters have not become excited enough to deny insurance, although they constantly recommend that active fire detection and suppression systems be installed, especially on large diameter hydrocarbon storage tanks. Insurance is a commodity and relies on commodity-type pricing, therefore it is rare that a facility is denied insurance based on protection levels. In rebuttal, operators will point out that the contents of one burning tank in a grouping can always be pumped back into a pipeline or a holding tank, thereby removing most of the fuel from the fire area and reducing exposure to adjacent tanks, an example of risk assessing one's way out of needing to provide protection. The fall-back is on minimal fire code protection levels.

Of course, this can only be accomplished if the associated pumps are of sufficient capacity and piping is configured to move the fuel to a dedicated emergency holding tank or there is capacity in a pipeline to take the contents of a burning tank. In the real world, the scuttling of a burning tank to anywhere outside the fire area rarely, if ever, happens. Millions of dollars in public money are spent on disaster response while in the end the involved tanks simply burn themselves out. This was clearly demonstrated during a dramatic October 2009 terminal fire in Puerto Rico in which fully half the facility's forty storage tanks were lost to fire.

Unlike offshore spills, large oil companies, pipeline and terminal operators, end users, and their insurance underwriters have not demonstrated great concern for the environmental damage caused by large volume hydrocarbon fires except to say they're sorry. The uncontrolled incineration of millions of gallons of fuel in a single storage tank – or even twenty storage tanks – has not merited the attention of legislators and environmental protection advocates or affected public sentiment in the same way that the image of a tar-coated seagull might do. Consequently, there is little outside pressure to do things better. Technical safety may receive lip service but anything that does not contribute to the bottom line can be, in the end, tagged as overhead and therefore fair game for cost cutters. Minimal code compliance then dictates design criteria.

Obviously, it is better for fires not to occur in the first place than to have to try and suppress them. Designing for safety – and getting it right – would eliminate many of the causes of explosion and fire. Unfortunately, after-the-fact fire investigations often make the same mistake in identifying cause, that is, they point to the level instrument that failed or was bypassed and the monitoring system computer that was down at the same time the overflow ignited and caused the fire that destroyed the tank farm, put many thousands of tons of effluent into the earth's atmosphere and ground water, and forced thousands of people to evacuate their homes.[4] Yet the upstream cause of a fire incident can often be found closer to the drawing board, long before the project itself went into construction.

In spite of some recent high profile hydrocarbon fires, insufficient expertise continues to be brought to these projects by some design engineers and their contractors. Experience has shown that technical safety in general, and fire detection and suppression systems in particular, are not always designed in sufficient detail to ensure that they meet the performance criteria necessary to reliably achieve their intended role. In some cases the parameters are not even clearly defined. The problem is compounded when the system designer or specifier has not had the operational experience or feedback necessary to ensure system practicability.

An excellent example is the Tacoa Power Station fire of 1982 in Caracas, Venezuela. The design of the fuel storage and distribution facilities at Tacoa was not based on minimal code compliance or driven by an insufficient budget for fire protection. On the contrary, explosion and fire occurred in a code compliant, well fire protected tank farm, nonetheless resulting in the deaths of over 150 persons, extensive capital losses, and a huge environmental disaster. Peering down the shaft of time, it would be impossible to state definitively the ultimate upstream cause of the explosion and fire. Still, it is instructive to compare the occurrence of explosion and fire in this well protected plant with what might occur when minimal code compliance drives the design.

The heavy fuel oil tanks that supplied fuel to the boilers that powered steam turbine generators at Tacoa were compliant with NFPA, FM and other guidelines in terms of separation distances and dyked spill containment areas. Tank No. 8, where the fire started, was a vertical atmospheric storage tank featuring a weak roof to shell seam in accordance with the requirements of American Petroleum Institute (API) standard 650.

The 180 foot (55m) diameter x 56 foot (17m) high tank was equipped with pneumatic heat detectors and automatic fixed foam fire suppression systems engineered to NFPA 11 standard with three foam chambers placed along the top rim. Deluge water sprays were provided at the top center of the tank's cone roof. 317,000 Gallons (1,188,750 liters) of stored fire water was supplemented by seawater. Along the top of the dyke wall were positioned three fixed, 500 gpm (1875 lpm) monitors. All fire suppression equipment, from the three electric and one diesel fire pumps to the foam systems to the water sprays functioned correctly during the fire.

Before the initial explosion occurred, a high-temperature indicator signaled the control room that oil temperature at the boiler end of a feed line to the power plant was above normal. Only two of the six tank steam heating units were operating and one was then shut down. The oil temperature returned to within normal limits. This over-temperature was initially thought to have contributed to the creation of an ignitable fuel-air mixture at the surface of the oil in the tank, something that under normal operating conditions should not have occurred. The flash point of the No. 6 fuel oil in the tank is approximately 150^{o}F (65 ^{o}C). The chart recorder had indicated an oil temperature of 190^{o}F in the feed line.

Because the tank and its steam heaters were later completely destroyed, investigators were unable to determine whether the over-temperature condition was confined to the feed line – a heat tracing control failure – or whether the bulk of the fuel in the tank itself was overheated. Discharge from the tank would have been taken from nozzles located closer to the bottom of the shell rather than at the surface of the liquid where a warmer temperature and vapourization might be expected. As the tank was essentially a large heat sink and would not have returned to within normal operating temperature so quickly after shutting down one of the two operating (out of six) tank heaters, there is reason to believe that an ignitable fuel-air mixture should not have been present inside the tank, the over-temperature condition being confined to the boiler feed line.

The source of ignition probably involved human error when a maintenance crew attempted to gauge (dip) the level in Tank No. 8, although nobody will ever know for certain. At around 6:00 am on December 19, 1982, a three-person maintenance crew approached Tank No. 8, intending to perform a routine dipping operation. One man remained in the dyke area while the others climbed to the tank roof to perform the task. Approximately two minutes later, an enormous explosion ripped off the tank roof.

Speculation suggests that the two operators who proceeded to dip the tank may not have employed an explosion-proof flashlight or perhaps had struck a match to see in the dim light. It was widely believed that the flash point of No. 6 fuel oil is sufficiently high that an explosive fuel-air mixture would not normally occur at the surface of the liquid, even if the tank were heated so that the heavy oil could be pumped to the boilers. The earlier over-temperature in the fuel feed line at the boiler, and its relatively quick return to within normal limits, had not alerted operators to an unsafe condition inside the tank.

The power generation plant had no fire brigade. By the time the district fire brigade had arrived and assessed the situation, it was decided that the fire would simply be left to burn itself out. At that point it became a spectator fire. The fixed foam systems, water sprays, fixed monitors, and fire fighters' hose streams proved to be of no use in extinguishing the blaze, some of the equipment having been damaged by the initial explosion. In addition to the toll in lives, the cost of the fire in terms of atmospheric pollution caused by the burning fuel was not, then as now, taken into account or subjected to public scrutiny by environmental watchdogs.

Approximately six hours after the initial fire had started, a violent boil-over occurred, killing over 150 persons including 17 plant employees, 40 fire fighters and many bystanders. More than 1000 feet (300m) away from the fire, people jumped into the sea to escape the intense heat and several reportedly drowned. The main plant was only saved by a concrete security wall that stopped the fire. It was then that the full impact of the disaster hit home in people's minds. Still, the fire was attributed to component technical failure, specifically, over-temperature of the heavy oil in the feed line to the boilers located at some distance from the tanks.

What had occurred was, in fact, a chain of failures that began at the engineering stage long before the power station and its tank farm were erected, possibly compounded by faulty fuel handling procedures and methodology during routine operation. Process upset was likely coincidental with the fire that led to the boilover, a contributing factor in the unsafe conditions that resulted in extensive deaths. The concept of double jeopardy in hazard and operability studies (HAZOP) tends to get design teams and owners off the hook for many protection schemes, as reliance on passive devices, components that one has no way of confirming are operating and that can be jumpered out for weeks or months, is generally considered enough. When operators resort to routinely dipping a tank rather than spending money on replacing a faulty level instrument, they may never return the instrument to service. In fact, many significant losses have occurred due to the failure of more than two levels of protection (double redundant). In this scenario, the importance of post-event fire control then becomes paramount.

So what single predominant element caused everything else to go wrong?

First, there was a general misunderstanding of the nature of the petroleum product being stored. It is commonly believed that a boil-over will not occur in No. 6 fuel oil. In practice, however, the blending of No.6 fuel oil was commonplace in the US market in 1982 and, although the contents of Tank No. 8 conformed to ASTM standards for No.6 fuel oil, it was blended from a wide selection of light and heavy components.

The fact that there had been no previously recorded instance of a boil-over involving No. 6 oil simply meant that such an event had not yet occurred.

Routine blending of No. 6 fuel oil can result in a product with a wide range of boiling points and therefore a propensity for boil-over. Although the product may be ASTM compliant, normal heating of heavy fuel oil to enhance pumpability can result in a fuel-air mixture above the lower explosive limit occurring at the surface of the liquid in the tank as the lighter ends vapourize. Atmospheric cone roof tanks are not intended for storage of a product exhibiting characteristics more typical of a Class I than a Class III liquid.

The second oversight on the part of the engineers, as well as the owner, was to have relied on NFPA 11 when designing the fire detection and fire suppression systems for the tank farm. The fixed fire suppression systems were certainly state-of-the-art technology in 1982, yet incapable of suppressing the fire and thereby avoiding the boil-over that caused the fatalities simply because conventional foam system design principles cannot be scaled up to the size of tanks in common usage at oil terminals and electrical power plants, typically greater than 115 ft (35m) in diameter. This fact was known from research conducted as early as the 1950's and readily available in the fire protection literature.[5]

NFPA 30, Tables 2-1 through 2-4 suggest there is little possibility of extinguishing fire in a tank that exceeds 150 ft (45m) in diameter using top mounted foam chambers. Testing and experience has shown that the maximum tank diameter for which a fire can be successfully extinguished is actually very much less. Only in recent years have fixed fire suppression systems such as Instant Foam and Foam Fatale been developed that can effectively extinguish fires in these large diameter storage tanks. In the early 1980s when the Tacoa fire occurred, better awareness of the nature of the product being stored and selection of appropriate storage methods as well as instrumentation for remotely monitoring product levels (rather than dipping), would have built technical safety into the installation instead of relying on a misplaced faith in installed fire detection and foam systems to control or extinguish fire after the fact.

In the end, it would have been better to store the heated oil in a low pressure tank that was inerted with nitrogen or blanketed with natural gas, thereby avoiding the creation of an ignitable vapour-air mixture inside the tank. Both NFPA 30 and the International Fire Code state that "*Liquids with boilover characteristics shall not be stored in fixed roof tanks larger than 150 feet (45.720 mm) in diameter unless an approved gas enrichment or inerting system is provided on the tank.*" [6]

Had the propensity for boil-over been known to engineers at the design stage, the tanks at Tacoa would not have been code compliant. To what extent, therefore, must due diligence be conducted, particularly in tank farm layout, selection of appropriate storage and handling equipment, as well as the design of fire detection and suppression systems?

There is a general misunderstanding of what happens during large volume hydrocarbon fire fighting. When oil containing components with a variety of boiling points, begins to burn, the heavy ends sink below the surface while the lighter ends vapourize and burn off at the surface of the liquid. The sinking heated layer transmits heat to the cooler oil below as the light components make their way upwards to feed the fire. As the heat wave moves toward the bottom, the heavier components increase in size and density, reaching 300 to 600^{o}F (115 to 315^{o}C).

This is not a problem as long as there is no water in the bottom of the tank. But when the heat wave reaches a water or water-emulsion layer at the bottom, a layer that is augmented by water-based (97%) foam and fire water pouring into the tank from fixed foam systems and hand lines, it superheats the water causing it to flash to steam in an expanding ratio of 1700 to 1. The resulting fire ball that issued from the Tacoa Tank No. 8 was estimated to have reached 1000 feet (305m) in diameter and 6,000 feet (1830m) high.

The wide range of boiling points inherent in the blended No. 6 oil, as well as water poured into the burning tank by the fixed foam system and fire fighters' hose streams, led to the boil-over, the volcano-like eruption that occurred when 3.5 million gallons (13,125,000 liters) of burning oil erupted from the tank, and the loss of 150 human lives. If the trail of evidence is picked up and followed far enough backwards, it becomes apparent that technical safety was compromised by a lack of awareness of the makeup of the stored oil, long before process upset and operator error were blamed for the explosion, fire and boil-over. Due diligence had not revealed No. 6 oil's propensity for boil-over under conditions that occurred at Tacoa. In retrospect, the fuel in Tank No. 8 could even have become contaminated, however, available records indicated that the last delivery of fuel conformed to ASTM specifications for No. 6 fuel oil. Investigators did not reveal evidence of post-refinery contamination of the product.

The US Chemical Safety Board has urged refineries, pipeline and terminal operators to improve their commitment to technical safety. The admonition applies equally to end users. By merely identifying the widget that broke or malfunctioned, or shifting blame to the operator most closely associated with the failure – who is often a victim of an operating budget insufficient to keep instrumentation and safety equipment functioning properly – the ensuing responses aimed at preventing similar recurring incidents are seriously compromised. This approach simply returns an improperly designed system or plant to status quo and encourages cookie-cutter style engineering of new facilities.

The role and responsibility of the design engineer is to bring the highest level of competence to the job. It means assigning people with the right qualifications and skill sets to the work from the feasibility study stage through to detail engineering, construction and commissioning. This is what the owner is paying for and what the general public, the people who sometimes bear the brunt of a catastrophic industrial failure, deserve.

The engineer must deliver "beyond zero" safety through all stages of project development, through the operating phase and leading up to the last day the plant is in operation before decommissioning and owners should be willing to pay for it. This may indeed become the norm once the full downstream environmental impact of large volume hydrocarbon spills and fires are assessed to facility owners instead of being absorbed by insurance companies and the general public. Designing for minimal fire code compliance will then be not quite enough.

To avoid the recurring theme of human and environmental catastrophe, hazards must be reduced by means that are built into the design of the facilities and inseparable from them. In other words, inherent technical safety is built into and stays with the facility for the lifetime of the asset. For a little extra care and attention at the design stage of a project, owners and their operating personnel, insurance underwriters, environmentalists, and the public at large will rest a lot easier.

References

1. 2006 International Fire Code, 3404.2.9.1.1.
2. 2005 National Fire Code of Canada, 4.3.2.5(1)
3. U.S. Chemical Safety Board, November 17, 2009, Investigation Details: Caribbean Petroleum Refining Tank Explosion and Fire.
4. CNN, November 17, 2009, Puerto Rico fire linked to faulty gas tank monitoring system.
5. Swedish National Testing and Research Institute, Brandforsk Project 513-021, Tank Fires, Review of fire incidents 1951-2003
6. 2006 International Fire Code, 3404.2.9.1.4.