A Study of Tank Overfill Incidents

Purdue University
Department of Chemical Engineering

Colin Jamison

Dr. Ray Mentzer

12/6/19

Introduction

Tank overflow should be a major concern for any facility with vessels handling large volumes of liquid. These liquids are often hazardous with the potential to do major damage if handled improperly. Tank overfill accidents pose safety risks to operators, managers, and the facility itself. In extreme cases, there is also a risk of releasing toxic materials, fires, and explosions. These accidents however, are often predictable and therefore preventable. It is important to look at the causative factors that have contributed to past accidents to prevent future incidents. These factors include human error, inadequate risk analysis, and the lack of hazard recognition.

Tank overfilling incidents occur more frequently than what one may assume. A review of various articles and studies was done to outline the leading root causes of tank overfill incidents and compare them to current industry standards. In a study of 242 tank incidents between 1990 - 2004, 30% of all incidents were due to insufficient maintenance. Tank overflow was the most frequent consequence. A review done on a study of tank incidents between 1961 – 2013 found that between 2000 – 2013, human error contribution increased to 35% compared to previous years, showing that human error is a growing concern. Other leading causes were mechanical failure at 40% and external events at 21% (Hemmatian 2014). External events include fire, explosion, lightning, and extreme temperatures. A study done on tank overfilling incidents by HSE (Chambers 2009) found that an inadequate LOPA (Layer of Protection Analysis) on the processing units was the leading cause, and that human factors were the leading source of initiating these events.

Industry standards have been developed to mitigate or eliminate these mistakes. The three industry standards used specifically to prevent tank overfilling are: API STD 2350 and IEC 61508 / 61511. API 2350 is titled "Overfill Protection for Storage Tanks in Petroleum Facilities," while IEC 61508 / 61511 are used as a guide to functional safety. IEC 61508 gives standards on targeted risk and risk associated with various controller types, and IEC 61511 provides guidance as to how to implement advice from 61508. For any process industry, the use of these handbooks is highly recommended. They contain information on current industry standards used within many facilities across the country, and they will help to reduce the chance of future overfill incidents.

Main Findings

For the main findings from the Buncefield and CAPECO incidents, UK HSE guidance and CSB investigations show three common root causes. These root causes include inaccurate LOPAs, poor management, and poor operating procedures.

With LOPA, a shortcoming can be created in several ways, first occurring during the risk analysis. Although there are general risk values associated with the ATG (Automatic Tank Gauge) and alarms, these values are not always exact under every circumstance. Frequently in tank overfill incidents, plants assumed a risk value from IEC 61511 with very little information to support the values. The ranges in IEC 61511 are used as guidance and a strong analysis should be done to confirm the values that are being assumed. The second problem within LOPA is the assumption of the use of independent systems without confirming this expectation. Systems operating on the same controller don't always act as independent systems. If these controllers are not independent, the risk value associated with said systems will also change, showing the inaccurate analysis by LOPA when making this assumption. Lastly the double counting of the ATG as both a protection layer and an initiating event. According to HSE, the ATG should only be considered as one or the other; an initiating event or a protection layer. It is important to know what to accredit to the ATG in the analysis depending on the function of the ATG being considered. Consistency in this regard is important when assessing risk and protection accurately.

The second shortcoming was poor management. This is best shown in the Buncefield incident. The increase in production at the Buncefield location increased the work load on the operators and managers. This increased intensity and lack of safety culture allowed for previous ATG problems to occur without being recorded. Poor management led to chaos in response to the increasing demands of the plant, leading to a preventable accident. Prioritizing a strong safety culture is crucial to ensure timely maintenance and recording of near misses and incidents. Most importantly, it will also ensure a safer work environment.

The last root cause was insufficient operating procedures. As shown by SISTECH, in some cases the safe fill limit is arbitrarily selected and not as detailed in the calculations as they should be. The operating procedures within these plants often exceed the levels of concern (LOC) for their equipment and product under specific conditions. In other cases, the safe fill limit is outdated in comparison to the changing equipment being used. API STD 2350 states that it is important to re-calibrate all LOCs after any change in material, tank, flow rates, etc.

Some recommendations for these incident causes include doing more accurate LOPAs, prioritizing safety culture, and defining safe fill limits by utilizing handbooks like API 2350 and IEC 61508 and 61511. It is also important to maintain LOCs with changing equipment, and to calculate all limits thoroughly. These points are very important to consider when looking at current standards that are in place for different tank types, materials, and controller set ups at different facilities.

Table:

Incident	**Buncefield**	**CAPECO**	**HSE LOPA Analysis (15 studies)**
Capacity	61.6 million gallons	90 million gallons	Unknown
Product filled	Unleaded Gasoline	Unleaded Gasoline	Ethanol, Kerosene, Petrol
Injuries	43	3	Unknown
Fatalities	0	0	Unknown
Monetary Losses	$1 billion	$1.5 billion	Unknown
Protection layers	ATG High level alarm Independent AOPS	Manual reading of float and tape gauging Manually measured levels before and after filling	15 - ATG 15 - High level alarm 11 – HH alarm 4 – AOPS
Failure	ATG failure Failure of independent AOPS	Gauge difficult to read Computer failed to read data	Human error ATG failure

Root Cause	Insufficient management Poor maintenance	Inaccurate volume calculations Failure of safety management system	Risk values of IE and PL assumed incorrectly Poor assumption of independence of PL and IE

Incident Summaries:

Buncefield

Beginning in the 1960's, the Buncefield facility functioned as an oil storage depot for petrol. Between 1960 - 2005, the facility quadrupled its storage, with much of the increase being in 2002. This large increase caused high pressure on operators and supervisors to keep up with the growing demands of the company. In several instances this high stress led to employees ignoring safety to make deadlines. For example, some supervisors worked 12 hour shifts 7 days a week with no fixed breaks. (COMAH 2008)

Buncefield had two forms of control within the facility. These consisted of an Automatic Tank Gauging (ATG) system and an automatic high – high trip switch. There were three levels defined in the procedure when monitoring products in their tanks. The "user high" was set by the supervisor, the "high level" was the maximum working level, and the "high-high level" was the final warning before the trip switch turned on. In the past, there were several instances where operators had reported that the ATG would stick intermittently and give incorrect readings. The system had been serviced in August 2005, but the ATG continued to stick, even sticking as many as 14 times in a five-month period. Although this information was known, mangers didn't respond accordingly to service the tank due to high intensity of work and very long hours. Also, during filling procedures, levels could exceed the "high level" and sometimes up to the "high – high level." There was a strong reliance on the alarms to control the filling process, yet they also did not have very well written filling procedures. This made things more difficult for operators to choose what tank to fill, how high it could be filled, and under what circumstances filling may be appropriate.

On December 10th, 2005 at 6:50pm, 6 million liters of unleaded petrol began being transported to tank 912. On December 11th around 3:05 am, the ATG display stopped registering a change in fill level. Because the level couldn't be recorded, the "high level" did not go off nor

could the “high – high level” automatic shutdown be activated. By 5:37 am, the tank began overflowing from the vents in the tank roof.

In the ‘Journal of Loss Prevention in the Process Industry’ (Atkinson 2014), key researchers analyzed the formation of the vapor cloud from tank 912 and how it generated such a large explosion caused by the overfill. Because tank 912 had a fixed roof, it forced the gasoline liquid to flow out the tank vents. When gasoline overfilled, liquid streamed down the sides of the tank and broke into a cascade of small droplets down the sides of the tank. As the droplets fell through the air, they propelled the air to follow with it. The gasoline then evaporated into a cold vapor. This allowed for the gasoline to stay very close to the tank in a concentrated form and for the gasoline to evaporate much quicker than what was expected. When the gas reached an ignition source, this allowed for a much more concentrated explosion near the tank.

In response to this incident, the HSE recommends having a clear understanding of accident risk and the safety equipment (COMAH 2008). This key understanding should be taught to everyone from senior management to any operators who may be doing maintenance, supplying, or operating these controls. HSE also recommends having a strong safety culture. With this, everyone within the plant would have worked less hours, prioritized fixing the ATG and ultimately avoided any further problem possibly caused by the ATG. Lastly, HSE recommends having an effective auditing system in place. This system would require routine testing on all plant systems to ensure they are working and reading correctly. Having strong mitigative systems in place could also minimize the effects of an incident like Buncefield. With mitigative systems, for example, the tank vents at the top of the tank would have been designed to mitigate the vaporization of gasoline. This may have given operators more time to react to the tank overflow and possibly have stopped the ignition from occurring.

CAPECO

CAPECO was a petroleum refinery based in Puerto Rico. This site contained a series of tanks capable of storing 90 million gallons of product. During normal operations, vessels connected to the pipeline would pump to one or more of the storage tanks. Each storage tank contained a float and tape gauge on the side of the tank and a manual tank gauge via gauging tape. The float and tape gauge was usually measured manually by operators and level data was automatically transmitted to the computer. Typically, at the start and end of filling a tank, an inspector is required to manually measure the tank levels by lowering gauging tape into the tank. This confirms the amount of product in the tank, and acts as a second defense against tank overfill as it eliminates the possibility of receiving a faulty reading from the float and tape gauge.

On October 21st, 2009, the Cape Bruny cargo ship arrived to unload a shipment of 11.5 million gallons of unleaded gasoline. Tank 107 had a capacity of 21 million gallons, but it was already holding product before the cargo ship arrived. To balance out the gasoline, CAPECO planned on pumping the gasoline from tank 107 into four smaller tanks. This transfer filling process was expected to take around 24 hours to complete (CSB 2010).

At 6:30 pm, the operator manually calculated the fill rate of tank 409, one of the four smaller tanks, and discovered it would be full by 9 – 10 pm during a shift change. To avoid this, the operator opened a valve of another tank, tank 411, to fill these two smaller tanks at the same time. They did, however, leave tank 409's valve partially closed to slow its filling rate. At 10 pm, tank 411 reached its capacity and the valve was closed. While tank 409 continued to fill, an operator read its level on the side gauge and reported that it would be full at 1 am, but its transmitter was not sending data measurements properly. When operators did a routine walk around at 11 pm that night, they manually reported the level on tank 409 to the supervisor, but also reported that the tank would be full by 1 am as reported earlier. Between 11 pm and 12 am, tank 409 began to overflow spreading a vapor cloud of gasoline around the facility that would eventually reach an ignition source and cause an explosion. The explosion luckily did not result in any fatalities, but the shrapnel caused minor injuries to three people. There was some damage to 232 homes in the nearby neighborhood, but the main damage was to the facility itself. The CAPECO facility spent five million dollars in repairs.

The CSB determined that CAPECO had a history of poor maintenance within its facility. EPA's Spill Prevention Control and Countermeasure (SPCC) discovered problems with leaky valves, leaky lines, and poor secondary containment. In the past, CAPECO had 15 previous tank overfill incidents. Three of which were after 2005. All of these resulted from valves left open, tank gauge malfunctions, or corrosion in pipes. Operators were also told to fill the tanks to the maximum level despite having little to no computer display for the tank levels. By only having manual gauging levels from operators and not enough lighting within the tank, it was very difficult to estimate the tank levels once they reached a certain height. Another cause of error was the ATG reading inaccurately. CAPECO was unable to determine a real time tank level due to not being able to detect flow rates. They were using unreliable gauging equipment and relied heavily on operators to read the tank levels. Lastly, the lack of an independent high- level alarm and AOPS also made detecting overfill more difficult.

The CSB recommends using API STD 2350 as generic guidance for implementing better overflow prevention. API can be useful for providing general guidance on operating procedures, scheduling inspections, improving management for personal and equipment changes, and reporting and recording near misses. NFPA 30 also gives various information on the transportation of flammable liquids from pipelines and marine vessels. It is worth noting that it has three options for tank monitoring, including:

Category one: Gauge tanks in intervals while personnel constantly check the premises

Category two: Tanks are equipped with High-level detection that is independent of gauging equipment or uses a gauging / alarm system with electronic checking to determine if the system has failed

Category three: Tanks are equipped with an independent high – level system that automatically shuts down. (AOPS)

Although CAPECO was compliant with all the requirements of a category one option, this system was not enough to stop the overfilling of tank 409.

The CSB recommends that NFPA 30 update its guidance to strengthen overfill protection through the addition of a required hazard assessment of the facilities considering nearby neighborhoods, businesses, and environment. This assessment should ensure the overfill system functions properly and that the facility maintains protection over site-specific hazards.

HSE LOPA Analysis:

In a study done by HSE on a total of fifteen tank overfilling incidents, they concluded that none of the overfill prevention systems were up to date with what is recommended in BSN EN 61511. BSN EN 61511 is the IEC 61511 of the United Kingdom. Eleven of these studies contained ATG high level alarms with an operator response PL (protection layer) and a high – high level alarm with operator response. The other four incidents contained an ATG high level alarm with operator response and a high – high AOPS. While they both had ATG systems, only four had an automated shut off system when the level reached a dangerous level.

The most frequent problem in the initiating events data was the reliance on data given by BS EN 61511 without any reasoning or justification behind the use of the specific data. These values are only suggested ranges and should be justified beyond the brief explanatory text. This is especially pertinent when discussing human error based initiating events. Several of these cases used non-SIL rated ATG and based the probability of failure on demand (PFD) on 1×10^{-5} cases / year. This is an improper practice as BS EN 61511 has determined you cannot claim these values for non SIL equipment. In many cases these values were claimed with very little information supporting them.

The ATG was also calculated differently in various LOPAs. In some cases, it's accounted for in the PL category, some in the IE, and some in both. The ATG is usually accounted for in the IE category and the high – high level alarms with operator response are usually counted in the PL category. Although the wrong category allocation was incorrect, the main problem is the double counting of the ATG. Several of these LOPAs also assumed the initiating events to be independent without considering their logical dependencies. This similar problem occurred when analyzing the protection layers.

HSE recommends replacing the high – high level alarm systems with SIL rated safety instruments. In general, this means the addition of an AOPS which can shut down the process if needed. Secondly, HSE recommends doing more detailed risk assessments to guarantee that risk values are being selected correctly and not just because they are a specific controller. This includes a detailed analysis to prove systems are completely independent of one another. Lastly, HSE recommends having the correct information and training for a LOPA. LOPA requires a strong knowledge of not only standard operations but operations under emergency conditions as well. The LOPA practitioner needs strong experience in numerical safety studies to ensure mistakes like selection of poor data, double counting, and poor assumptions are not made.

HSE LOPA Analysis Company B

In an example of the HSE review of LOPA analyses, HSE examined Company B who transported large quantities of petrol by pipeline and railcar. Each tank in Company B had its own ATG with operator response to the alarms, a partially independent high – level alarm, and operator response to the feed pipeline. There was, however, no AOPS equipped to the tanks, so when high level was close to being reached, operators were left to respond to the high – level alarm on their own.

There were several initiating events that led to the overfilling of one of the tanks that Company B was responsible for. They did an incorrect calculation on how much lost material they had. In this event, the supervisor also failed to divert the material, and diverted material to the wrong tanks. The exporter also failed to close the export valve. The standards followed by Company B allowed too much room for accidents due to human errors.

The main issues with Company B's LOPA was with regard to the conditional modifiers and protection layers. In the conditional modifiers, the probability of a failure to detect an overflow and the probability of ignition were assumed to be unrealistically low compared to information given by BS EN 61511. They underestimated the likelihood of an accident occurring as a result of negligence, and they assumed that they were operating at safer conditions than what were actually present. In the protection layers, Company B used generic failure rate data. Although this is acceptable, it is recommended to treat this data with caution because of the varying conditions that the equipment could be used. The failure rate data does not efficiently consider real-world variation of plant facilities.

In conclusion, the risk analysis in the initiating events and conditional modifiers should have been used from BS EN 61511 instead of generating arbitrary numbers. Using information from the handbook is very useful, but it should be used cautiously as these numbers can't always be used directly on equipment. A strong PHA should be done to prove these values are comparable to the handbook.

SISTECH

In the article, "Overfill Protection Systems – Complex problem, simple solution" (Summers 2010), the lack of hazard recognition was the most frequent contributor to accidents in Buncefield, ESSO Longford, and the BP Texas City disasters. Although the hazard itself wasn't the problem, it was how each of these facilities handled the hazard that eventually led to these disasters. Summers analyzed that underestimating an overfill, having excessive reliance on operators, and having no defined safe limit were the main causes of these incidents.

Hazards to tank integrity is rarely given as much attention as the risk of overflow. Overfills can cause the tank to collapse through overpressure, and this can cause a series of problems when other systems downstream receive material they are not designed for. When there is interconnected equipment, the hazard analysis should ensure that these hazards cannot affect

the downstream equipment. This mitigative method should be done quick enough to guarantee that little to no unwanted material enters the wrong equipment.

The first problem that these incidents displayed was underestimating the risk of an overfill. High level was rarely seen by an operator due to the absence of an alarm and the lack of variation between the overflow indicator and the other systems on the display. Without an alarm, the indicator is not an immediate red flag to an operator monitoring several aspects of the tank and material at once. Secondly, the level of material is only seen as a concern when the safe level is exceeded. High level is commonly defined differently between loading, operational, and unloading conditions.

Ironically, the slower the event, the greater the tendency to believe that the operator can adequately address the event. Likewise, the more sporadic the event, the greater the tendency to believe the event will not last long enough to cause an overfill (Summers 2010). Operators commonly will overestimate how much time they have to respond to a lower risk incident. This is a double negative because in both situations, the risk of an overfill is underestimated by operators (Summers 2010). The consequences of overfilling, especially during high intensity work, should be clear to the operator.

The second problem (COMAH 2008) these incidents displayed was the reliance on operators. As facilities expand to increase production, the operator work load also increases. This causes the time allotted for operators to respond to unusual events to decrease. When fast responses are required, drills should be implemented to allow operators to practice for high intensity scenarios. Automated controls should also be considered to reduce the pressure on operators, increase efficiency, and reduce the risk of a hazardous event. Independent automated trips should also be used to reduce the likelihood of a significant event. This will also reduce the risk of operators being distracted with other work and reduce the risk of operators needing to go to a hazardous area to shut down or record information.

The last problem was not having a defined safe fill limit. In many cases, the entire level of the tank is not measured and instead only the operating range is measured. In a case of an overfill, an operator will not have accurate tank levels. A safe fill limit must be defined based on failure level, level range of ATG, fill rate, and action time required to stop filling. This level should be conservatively measured in case of variance in measurement.

Industry Standards:

API STD 2350

API STD 2350 is an excellent handbook for general information on creating operating procedures, defining level alarms, and categorizing tanks. API STD 2350 categorizes tank filling in three categories.

- Category one is a fully attended facility. This may include instrumentation, but these instruments do not transmit information to alarm the transporter. This means that all information reading is based on operator readings and transmitting information back to the controller of the plant.
- Category two is a semi attended facility. This usually includes an ATG with a local control center, but the high-level alarm is not independent of the ATG.
- Category three is an unattended facility. This category usually has an ATG with an independent high – high level alarm system. This can also include an independent AOPS as well.

Depending on the material being handled and the risk desired, processing facilities should look to these three categories for a general idea of the system they need to set in place. One criticism of API is that it doesn't give any recommendation for which category and system is adequate for a given process. When using this handbook, it is best to approximate what alarms or systems to use conservatively.

After the tank categories are defined, plants need to decide what the operational levels of the tank should be. This gives facilities an idea about the amount of spacing that should be present between the different alarms levels based on risk and category. A criticism of this document, however, is the lack of information on how to define the operating level and high level to begin with. Although there is some variation with what material is being used and the risk from controller types, there should be some type of guidance for where to start (Meyers 2018). Another large criticism of API is the lack of information on risk assessment. This is pointed out in Endress and Hauser's "Guidebook for Overfill Prevention and Tank Gauging" and by the CSB during the Buncefield investigation (Meyers 2018). The CSB states that API 2350 should require a risk assessment and information on how to conduct one properly. API should also give clear guidance for bare minimum of equipment that is required (CSB 2010).

API also includes several useful tips to take note of, one example being that the AOPS should be set below the critical high to account for the time it takes for the controller to respond to the overfill. API also states that the LOCs generally should be re-calibrated every five years assuming there are no incidents. If there is any maintenance done on any of the equipment or incident, re-calibration should be done again at that time. Some examples of maintenance include changing product, new seals on the tank, changing maximum flow rates, or changing lines.

IEC61508 and 61511

IEC 61508 and 61511 provide very useful information on risk associated with controllers and assessing this risk. IEC 61508 is defined as "Functional Safety of Electronic safety-related systems." It includes how to determine target risk values for SIL (Safety Integrated Layers) and how to design SIS to achieve these targets. IEC 61511 is defined as "Functional Safety – Safety Instrumented Systems for the process industry sector." Both handbooks should be used for advice on how to improve the safety of a processing facility.

(Emerson 2019) IEC 61508 defines SIL using requirements defined in two categories; hardware safety integrity and systematic safety integrity. The objective of this handbook is to develop a product that is more reliable and documented. This process can be quite rigorous, but the benefits associated with certification are un-matched. SIL rated products include documenting failure modes and effect analysis, comprehensive testing, proof tested procedures and a safety manual. The benefits of rating SIL products are quality assurance, quantified reliability and proper documentation covering through the SIL life cycle. It is important to achieve SIL certification from IEC 61508 because only then can risk values associated with products be assumed in any risk analysis.

IEC 61511 is considered the benchmark standard for the management of safety in the process industry. It defines the SIS lifecycle and how a product's safety should be managed throughout the lifecycle. The lifecycle includes hazard and operability studies, allocation of safety functions to protection layers, safety requirement specifications, safety design, factory testing, installation, validation, operation and maintenance, modification, and documentation (Ravindran) . However, it's important to know that this handbook does not include information on process design, overfill management and non-safety layers. Non-safety layers include basic process control, passive protection, and emergency response layers. An added benefit of IEC 61511 is that the lifecycle process is very applicable to other protection layers. In many cases, other companies have applied these processes to other instrument systems and obtained comparable results.

Conclusions

In conclusion, there were three common root causes found in the Buncefield, CAPECO, HSE, CSB, and SISTECH investigations. These root causes include inaccurate LOPAs, poor management, and poor operating procedures.

LOPAs common shortcomings occur within the risk analysis of PLs and IEs, first being the risk values assumed from IEC 61511 on the ATG, level alarms, and AOPS. This is outlined in the HSE LOPA analysis of 15 different overfill incidents. It was incredibly common for a facility to assume a value given in these handbooks with very little justification or reasoning whatsoever behind the use of this non-specific data for their equipment's specific environments. In some cases, it was common to apply these values to equipment that hadn't been SIL rated. IEC 61508 and 61511 are excellent handbooks for determining risk, but the correct analysis must be done to justify the assumptions that this data can be applied to those specific facilities. Another frequent mistake in the LOPA was the double counting of the ATG in PLs and IEs. The ATG should be in either the PL or the IE category when conducting a LOPA, but not in both. The double counting of the ATG will reduce the overall risk factor and give a false sense of safety and confidence to the facilities. LOPA also incorrectly assumed system independence. All of the IEC 61511 risk values are associated with completely independent systems. It was common for a LOPA analysis to make the independent assumption with no reasoning. When IEC 61511 is testing risk values, the environment is very controlled with little effect from other

systems. In a process system, there is a high possibility for other factors or systems to affect the product. This will increase the risk value associated with this product. It is crucial to complete a detailed analysis to determine the risk value and independence.

The second shortcoming that led to overflows in these investigations were poor management. It was common for processing units to prioritize reaching demands of the plant over safety. This is best shown in Buncefield and CAPECO. In Buncefield's case, the increase in output increased the work load on operators and managers. This increase in work load led to employees prioritizing deadlines and output over preventative maintenance and safety. In CAPECO, the equipment was severely outdated, especially for a plant with so many hazards. Both Buncefield and CAPECO had a history of problems with their systems reading tank levels incorrectly, but no maintenance or analysis was done to correct the problem. Prioritizing a strong safety culture is crucial to ensure timely maintenance and recording of near misses and incidents.

The final shortcoming that was found was poor operating procedures. In Buncefield, the "safe fill limit" was commonly exceeded during filling operations. In CAPECO, operators were told to fill the tank completely despite having little computer display. As pointed out by SISTECH, the safe fill limit in these cases was calculated poorly and commonly exceeded. Secondly, the slower the event, the greater the tendency to believe that the operator can adequately address the event before a disaster. Likewise, the more sporadic the event, the greater the tendency to believe the event will not last long enough to cause an overfill (Summers 2010). Even when operators weren't planning to exceed the safe fill limit, they still did accidently. The common source is the need for better defined operating procedures that should not be exceeded. This will reduce the impact of human judgement during a possible emergency scenario, and instead have employees follow steps that have been critically analyzed and pre-determined.

Recommendations

Some recommendations include improving the LOPAs, placing greater emphasis on safety culture, and improving operating procedures.

In the LOPA analysis, it is important to do a detailed analysis of all process equipment to determine the specific risk value associated with it. This is important when acquiring an accurate risk analysis for the facility, and to ensure that the facility is more aware and better prepared for possible accidents. This more accurate risk analysis can also be obtained by ensuring that aspects of the analysis are not double counted; like in the case of the ATG being accounted for in both the PL and IE categories. It's also very important to analyze risk values after any equipment changes or additions to guarantee independence.

To improve management and safety culture, it should be clear to everyone in a facility that safety is the top priority. No matter the cost or time, preventative maintenance should be done. It is better to spend the time and money on eliminating the potential problem rather than on cleaning up the mess after an accident. To improve procedures, it is also important to analyze and define clear operating procedures for employees to follow. The procedures should be

critically examined to be fail-safe. From this improvement, less dependence will be placed on operators' judgments and more will be placed on the defined operating procedures set by the facility.

IEC 61508, 61511 and API 2350 are excellent handbooks that should be used as general guidance for these site improvements. API has general information on improving operating procedures and LOCs. LOCs should be re-calibrated every five years assuming there are no incidents or changes in equipment or maintenance. A common criticism of API, however, is the lack of risk analysis and details for LOCs. This should be kept in mind when consulting API. IEC 61508 and 61511 are both useful in these areas. To determine risk values associated with equipment, it is highly recommended to go through the IEC 61508 certification process. Although this process is expensive and lengthy, it is very beneficial because it establishes quality assurance, quantified reliability, and proper documentation covering all the SIL life cycle. Adopting the practices in all three handbooks will greatly reduce the possibility for an overfill incident to occur.

References

1. *Atkinson, Graham, et al. Flammable Vapor Cloud Generation from Overfilling Tanks: Learning the Lessons from Buncefield. Journal of Loss Prevention in the Process Industries, vol. 35, 2015, pp. 329–338., doi:10.1016/j.jlp.2014.11.011.*

2. *Buncefield: Why Did It Happen? COMAH, 2008, www.hse.gov.uk/comah/buncefield/buncefield-report.pdf.*

3. *Caribbean Petroleum Tank Terminal Explosion and Multiple Tank Fires. U.S. Chemical Safety and Hazard Investigation Board, 2010, Caribbean Petroleum Tank Terminal Explosion and Multiple Tank Fires.*

4. *Chambers, Colin, et al. A Review of Layers of Protection Analysis (LOPA) Analyses of Overfill of Fuel Storage Tanks. HSE, 2009.*

5. *The Engineer's Guide to Overfill Prevention: 2019 Edition. Emerson Process Management, 2019, www.emerson.com/documents/automation/engineering-guide-engineer-s-guide-to-overfill-prevention-rosemount-en-79906.pdf.*

6. *Meyers, Philip, et al. Guidebook for Overfill Prevention and Tank Gauging . Endress + Hauser, 2018.*

7. *Overfill Protection for Storage Tanks in Petroleum Facilities . 2350th ed., API , 2012.*

8. *Ravindran, Suresh K. Automatic Overfill Prevention System (AOPS) - Learning from CAPECO Incident, www.honeywellprocess.com/library/marketing/whitepapers/White%20Paper-AOPS-for-petroleum-storage-facilities.pdf.*

9. *Smith, David J, and Kenneth G L Simpson. The Safety Critical Systems Handbook . Elsevier, 2016.*

10. *Summers , Angela. "IEC 61511 and the Capital Project Process - A Protective Management System Approach ." Journal of Hazardous Materials , 2006.*

11. *Summers, Angela E., and William Hearn. "Overfill Protective Systems-Complex Problem, Simple Solution." Journal of Loss Prevention in the Process Industries , vol. 23, no. 6, 2010, pp. 781–783.*

Abbreviations

ATG – Automatic Tank Gauge

AOPS – Automatic Overfill Protection System

API – American Petroleum Institute

CSB – U.S. Chemical Safety and Hazard Investigation Board

EPA – Environmental Protection Agency

HH – High high level

HSE – Health and Safety Executive, UK

IE – Initiating Events

IPL – Independent Protection Layer

LOC – Levels of Concern

LOPA – Layer of Protection Analysis

PFD – Probability of Failure on Demand

PHA – Process Hazard Analysis

PL – Protection Layer

SIL – Safety Integrity Level

SIS – Safety Instrumented System

SPCC – Spill Prevention Control and Countermeasure, EPA