Overfill Protective Systems - Complex Problem, Simple Solution

Angela E. Summers, Ph.D., President, and William Hearn, Fellow, SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034
asummers@sis-tech.com, 281-922-8324 (phone), 281-922-4362 (fax)

Presented at Process Plant Safety Symposium, 2009 AIChE Global Conference, Tampa, Fl, April 23-29.

Presented at Mary Kay O'Connor Process Safety 2009 International Symposium, College Station, TX, October 27-28.

To be published in an upcoming Process Safety Progress

Abstract

Overfills have resulted in significant process safety incidents. Longford (Australia, 1998), Texas City (United States, 2005), and Buncefield (United Kingdom, 2005) can be traced to loss of level control leading to high level and ultimately to loss of containment. A tower at Longford and a fractionating column at Texas City were overfilled, allowing liquid to pass to downstream equipment that was not designed to receive it. The Buncefield incident occurred when a terminal tank was overfilled releasing hydrocarbons through its conservation vents.

The causes of overfill are easy to identify; however, the risk analysis is complicated by the combination of manual and automated actions often necessary to control level and to respond to abnormal level events. This paper provides a brief summary of the Longford, Texas City, and Buncefield incidents from an overfill perspective and highlights 5 common factors that contributed to making these incidents possible. Fortunately, while overfill can be a complex problem, the risk reduction strategy is surprisingly simple.

Introduction

Loss of level control has been a contributing cause in three significant industrial incidents:

- The Esso Longford explosion (September 25 1998) in Australia resulted in 2 fatalities, 8 injuries, and A$1.3 billion in losses. Esso's natural gas supply to the state of Victoria for commercial and residential uses was severely affected for 2 weeks. Millions of residents did not have natural gas supply to their homes for over 20 days (1).
- The BP Texas City explosion (March 23 2005) in the United States caused 15 fatalities and more than 170 injuries (2). Facility production was profoundly affected for months after the incident. Losses to BP are in excess of $1.6 billion (2).
- The Buncefield explosion (December 11 2005) in the United Kingdom (UK) injured 43 people and devastated the Hertfordshire Oil Storage Terminal, which was jointly owned by Total UK Ltd and Chevron Ltd (3). Residences and commercial buildings in the area were structurally damaged with

some requiring demolition. The economic impact on regional businesses is estimated to be in the range of £130–170 million (3). Total losses may be as much as £1 billion (3, 4).

These incidents involve three different industries located in three different countries. Esso processed natural gas for commercial and residential distribution in Longford, Victoria, Australia. BP fractionated raffinate, a mixture of hydrocarbons, for recycle within the refinery in Texas City, Texas, US. The Hertfordshire Oil Storage Terminal is part of the Buncefield depot, which is the 5th largest oil depot in the UK (3) and located in Hemel Hempstead north of London. Each incident propagated uniquely, arriving at its final outcome through different mechanisms. Yet, all suffered the same process deviation of high level and all resulted in devastating consequences. This paper discusses significant factors contributing to these incidents and provides a simple 7 step solution for overfill protection

Incident Summaries

ESSO Longford

The Longford incident occurred in the lean oil absorption unit that processed gas from the Bass Strait platform. Lean oil entered the top of an absorption tower and absorbed the heavier fractions (C2-C4) from the gas/condensate feed stream. Rich oil exited the tower just above the bottom section and was sent to downstream equipment, where the lean oil was recovered for recycle and the heavier fractions were collected for further processing. Condensate in the bottom section of the tower was recirculated through a reboiler to enhance removal of light ends.

The incident occurred when excess flow from the Marlin Gas Field (1) introduced more condensate into the absorption tower than it was designed to handle. Condensate overflowed the tower bottom section, mixed with the rich oil, and passed downstream to the rich/lean oil circulation system. The upset affected the demethanizer tower (5) and eventually caused high level in a separator drum initiating shutdown of the lean oil pump.

Without lean oil recirculation, the system chilled well below normal operating temperatures. The demethanizer reboiler (5) temperature went as low as -48C, causing cold temperature embrittlement (1, 6). The lean oil pump remained unavailable for more than 3 hours and when it was started up the hot lean oil caused the reboiler to stress fracture (1). The release resulted in a vapor cloud that spread outward for 170 meters prior to reaching fired equipment that provided an ignition source (1).

BP Texas City

The BP facility in Texas City, Texas, is one of the largest refineries in the United States with a capacity of 437,000 barrels per day (2). The raffinate splitter is part of the isomerization unit and it fractionated a mixture of hydrocarbons for internal recycle within the facility. The splitter was designed to relieve overpressures through a series of pressure relief valves (PRVs) that discharged into a blowdown drum. The drum was designed to trap mists and entrained liquids for discharge to the process sewer and to relieve vapors to the atmosphere.

During a cold start-up of the raffinate splitter, level is accumulated by starting the feed to the splitter with the outlet valve closed. When the level reaches conditions described in the start-up procedure, the

operator is supposed to control the level by opening the outlet valve manually or by placing the level controller in automatic operation.

The incident occurred when the raffinate splitter was fed at normal rates for more than 3 hours (7) with the outlet closed during a cold start-up. Liquid overflowed the splitter into the vapor discharge header resulting in the opening of the PRVs. Liquid surged through the PRVs into the blowdown drum and began draining into the process sewer. Within seconds, the flow from the splitter overwhelmed the drain capacity yielding a geyser of hydrocarbons from the drum stack that rained down inside and outside the process area. The hydrocarbon vapor and liquids eventually reached an ignition source resulting in the catastrophic explosion.

Buncefield UK

The Hertfordshire Oil Storage Terminal is part of a complex of tank terminals known as the Buncefield Depot. The depot has an estimated capacity of 60 million gallons and serves as a major distribution center for the UK oil pipeline network (8). It provides fuel to Humberside, Merseyside, as well as to Heathrow and Gatwick airports (3).

The incident occurred when the automated tank gauging system failed, allowing fuel to be fed into a terminal tank for 11 hours (9). The fuel overflowed through the tank conservation vents for approximately 40 minutes (10) prior to ignition, producing a large vapor cloud estimated to be 8 hectares in size (11). The vapor cloud ignition resulted in the largest peacetime explosion in European history (9) producing a tremor measuring 2.4 on the Richter scale and blowing out windows five miles away from the site (11).

Factors Contributing To Overfill Events

Lack of hazard recognition

In the majority of processes, level has little significance to plant production or product quality. The absolute level often varies over a large range where the “normal” operating level is not well-defined or tightly controlled. In many processes, the normal operating level is significantly below what would threaten the equipment integrity. In tank farms, the operating level is simply inventory to be managed and normally varies across a large range.

High level is often not a hazard itself. Instead, the hazard is too much mass or volume. Some overfills challenge the tank or vessel where the level is accumulating, causing it to overpressure or to collapse when the retained mass exceeds the equipment structural design limits. Many overfills result in loss of containment when liquid passes to downstream equipment that is not designed to receive it.

Overfill hazards vary depending on the type of vessel and associated upstream and downstream equipment. When interconnected equipment is affected, the hazard analysis should ensure that the high level hazard is prevented and is not allowed to pass downstream. It is rarely effective to allow a high level event to propagate and to depend on downstream process variables to be fast enough to prevent equipment damage. For example, high level in a knock-out drum requires immediate response to protect the compressor from damage. Waiting until high compressor vibration is detected is too late.

Underestimating the likelihood of overfill

Level seems so simple to detect that anyone should be able to recognize it and respond in a timely manner. Unfortunately, high level can rarely be seen directly by the operator. It is just one of many process variables on the display. Compounding this perception, level often does not affect the unit operation or cause any other significant process variable disturbance until the safe fill level is exceeded and suddenly the mechanical integrity of the vessel or interconnected equipment is threatened.

High level may have different causes in each mode of operation, e.g., start-up, normal, or upset conditions. Start-up may require the accumulation of level, so the outlet control valve is initially closed and under manual operation until the normal operating level is reached. Level may vary over a large range during normal operation. During upsets, operators may operate vessels at higher than normal levels to smooth out process operation by using the available capacity as a dampener for upsets in upstream or downstream equipment.

Some hazard analysis teams erroneously believe that overfill is not a credible event, because the time required to fill the vessel is generally on the order of minutes or hours rather than seconds. Some events propagate slowly, such as the rise of level in a product storage tank, while others occur quickly through a random event, such as a process upset sending excess liquid to a knockout drum for a compressor. 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 overfill. Believing that high level is non-credible is especially attractive when the existing design has no provision for high level alarm or trip.

Estimating the likelihood of overfill is complicated by the combination of manual and automated control that is often necessary as the equipment is started up and operated. Figure 1 shows the range of automation commonly found in tank farms and terminals. The degree of automation is typically related to the expected rate of level rise and operator work load. Automated control and safety systems are generally added when control changes must be made too often to be continuously managed by the operator or when work complexity has increased to the point where the expected human error rate is no longer acceptable.

A safe fill limit must be specified and the consequence of exceeding it should be explained in the operating procedures. Without clearly stated limits and consequences, the operator may not adequately monitor level, especially during intense work periods. Overfill is a credible event and it takes good operating procedures to reduce its likelihood.

Excessive reliance on the operator

The “blame the operator” tendency is encouraged by the length of time required to reach overfill. In many applications, the operating basis provides adequate time for the operator to control the level within acceptable tolerance, but human error is always possible. Work load and piping network complexity decrease the operator’s ability to reliably control level and maintain process safety. As facilities are expanded to increase production, operator work load increases and the time available for operator response to abnormal events erodes. In some cases, the available time is reduced to the point where manual response is no longer effective and automated overfill protection must be implemented.

Personnel hazards should be considered when directing operators to take manual actions in the process unit in response to high level, such as draining knock-out drums. Local response generally moves the operator into the hazard zone increasing the risk to that individual. Consequently, the design must provide sufficient time for the operator to take action and means to verify the intended process response. Further, there should be time to evacuate the area if the action does not work as expected. When fast response is required, operator drills should be considered to allow the operator to practice the response and to verify the time required to detect and respond. These drills can identify issues with the design, installation, and labeling, as well as with the procedures and training.

Automated controls are often added to increase operating efficiency and reliability. They should also be provided to reduce reliance on operator response near the hazardous event. For significant events, automated trips that are independent from the process control system should be implemented to ensure protection is provided even when the operator is focused on other duties with the added benefit that you are not sending the operator into the hazard zone for event response. Procedures and training must ensure that the automated trip does not become part of normal level control (e.g., high level trip stops pump every fill rather than the operator stopping the pump), so trip initiation should be monitored and reported.

A safety instrumented system (SIS) detects high level and prevents filling beyond the safe fill limit. The SIS can be a simple hardwired system using an independent level sensor (e.g., switch or transmitter) to detect high level and an independent final element (e.g., motor control circuit or block valve) to terminate or divert feed. The SIS is automatically initiated at a setpoint that allows sufficient time for the action to be completed safely. The design should place the setpoint far enough from the normal control range to allow time for effective operator response to pre-trip alarms. Risk analysis determines the safety integrity level (SIL) required to ensure that the overfill risk is adequately addressed. While there are exceptions, the majority of SIS are designed and managed to achieve SIL 1 or SIL 2.

No defined safe fill limit

In many applications, the entire level range from empty to postulated failure point is not displayed. Instead, the expected operating range is covered by the measurement device. This provides the most accurate measurement across the operating range, while unfortunately leaving the operator with no indication of the level when it rises above the normal operating range.

A safe fill limit should be clearly established in the design basis. The safe fill limit is specified based on an understanding of the postulated failure level, the analytical capability of the instrumentation used for the measurement, the fill rate, and the time required to achieve a safe state. The safe fill limit should ensure that action can be completed prior to reaching the postulated failure level. It should be conservatively estimated based on expected measurement drift in the process and environmental conditions.

Figure 2 shows the transition of the level from the normal operating range to the postulated failure point. An alert may be provided to support level control and its setpoint should allow enough time for the operator to take response to prevent the level from reaching the safety alarm or trip setpoints. The safety alarm should provide enough time for the operator to bring the level back under control or to take the equipment to the safe state.

The trip point is selected to automatically initiate a feed shutdown so that the level rise is stopped prior to reaching the postulated failure level. The off-set between the trip setpoint and the safe fill limit is the

design safety margin. When an alarm is also implemented, the alarm setpoint should be conservatively set below any trip setpoint, allowing the operator sufficient time to stop level accumulation prior to the trip being initiated. Otherwise the alarm loses merit as a protection layer and simply serves as pre-trip notification.

Inadequate mechanical integrity

There are no bad level devices, only technology misapplications, improper installations, and inadequate mechanical integrity programs. Some companies have mandated that only transmitters be used in safety services, stating that direct mounted switches should not be used due to their lack of continuous signal. For columns and storage tanks, the safe fill limit is significantly outside the normal operating level, resulting in the high level alarm or trip sensors being at a very low signal output for long periods of time. Under this condition, the benefit of a diverse technology sensor, like a switch, may outweigh the advantages provided by a continuous signal. For example, it's an acceptable practice to implement an automated control system that uses an analog measurement covering the expected normal operating range and a level switch to initiate feed shutdown.

A properly maintained level switch can provide years of cost effective and satisfactory service. On the other hand, years of neglect will allow a well-designed device to fail. There are many technologies available for level measurement and detection, from simple float type discrete switches to complex guided wave radar transmitters. Each technology has characteristics that make it the right choice for a particular application (12). For most safety applications, the main considerations for equipment selection are the required accuracy, process operating mode, the operating environment, the historical equipment performance, and the ease of maintenance and testing.

A high level alarm and trip can be implemented with separate level switches at the selected points on the vessel or with a transmitter that covers both setpoints. Although transmitters may not improve the diagnostics in services that do not normally have level, they do provide the ability to monitor over a chosen range and to alarm at various points in the range.

No matter what technology is selected; the mechanical integrity of the equipment must be maintained throughout its installed life. Functionality is demonstrated by forcing the sensor to "see the process variable" and to generate the correct signal at the specified setpoint. Testing must prove that the equipment can operate as required to prevent overfill. Although diagnostics can detect many types of failures, a proof test is still necessary to demonstrate operation at the required setpoint. This is the only means to fully prove that the equipment works as required.

Solution

Catastrophic overfills are easily preventable. When overfill can lead to a fatality, follow these 7 simple steps to provide overfill protection:

1. Acknowledge that overfill of any vessel is credible regardless of the time required to overfill.
2. Identify each high level hazard and address the risk in the unit where it is caused rather than allowing it to propagate to downstream equipment.
3. Determine the safe fill limit based on the mechanical limits of the process or vessel, the measurement error, the maximum fill rate, and time required to complete action that stops filling.

4. When operator response can be effective, provide an independent high level alarm at a setpoint that gives the operator sufficient time to stop accumulation of level before the trip setpoint is reached.
5. 5. When an overfill leads to release of highly hazardous chemicals or to significant equipment damage, design and implement an automated overfill-protection system.
6. Determine the technology most appropriate for detecting level during abnormal operation. This technology may differ from the one applied for level control or custody transfer.
7. Finally, provide means to fully proof test any manual or automated overfill protection system to demonstrate its ability to detect level at the specified setpoint and to take action in a timely manner.

REFERENCES

1. Wikipedia,"1998 Esso Longford gas explosion," http://en.wikipedia.org/wiki/1998_Esso_Longford_gas_explosion.
2. Wikipedia, "Texas City Refinery (BP)," http://en.wikipedia.org/wiki/Texas_City_Refinery_(BP).
3. Buncefield Major Incident Investigation Board, "The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board," ISBN 978 0 7176 6270 8, (2008).
4. British Broadcasting Station, "Buncefield blast could cost £1 bn," December 11, 2008, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/england/7777539.stm.
5. Longford Gas Plant Accident and Victorian Gas Supply Crisis, Australian Government, Attorney General's Department, Emergency Management Australia, http://www.ema.gov.au/ema/emadisasters.nsf/
6. Kletz, Trevor, "Lessons from Longford – The Esso Gas Plant Explosion," Chemical Engineering Progress, September 1, 2001.
7. Mogford, J., "Fatal Accident Investigation Report: Isomerization Unit Explosion," Final Report, Texas City, Texas, USA (2005).
8. Wikipedia, "2005 Hertfordshire Oil Storage Terminal Fire," http://en.wikipedia.org/wiki/2005_Hertfordshire_Oil_Storage_Terminal_fire.
9. British Broadcasting Station, "Buncefield tank was overflowing," May 9, 2006, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/4752819.stm.
10. The Daily Mail, "Petrol tank 'overflowing' before Buncefield blast," May 9, 2006, United Kingdom, http://www.dailymail.co.uk/news/article-385607/Petrol-tank-overflowing-Buncefield-blast.html
11. The Guardian, David Fickling, "Faulty fuel gauge caused Buncefield Explosion," United Kingdom, http://www.guardian.co.uk/uk/2006/may/09/buncefield.davidfickling.
12. Boyes, Walt, "First the application, then the product," ControlGlobal.com, http://www.controlglobal.com/articles/2007/022.html.

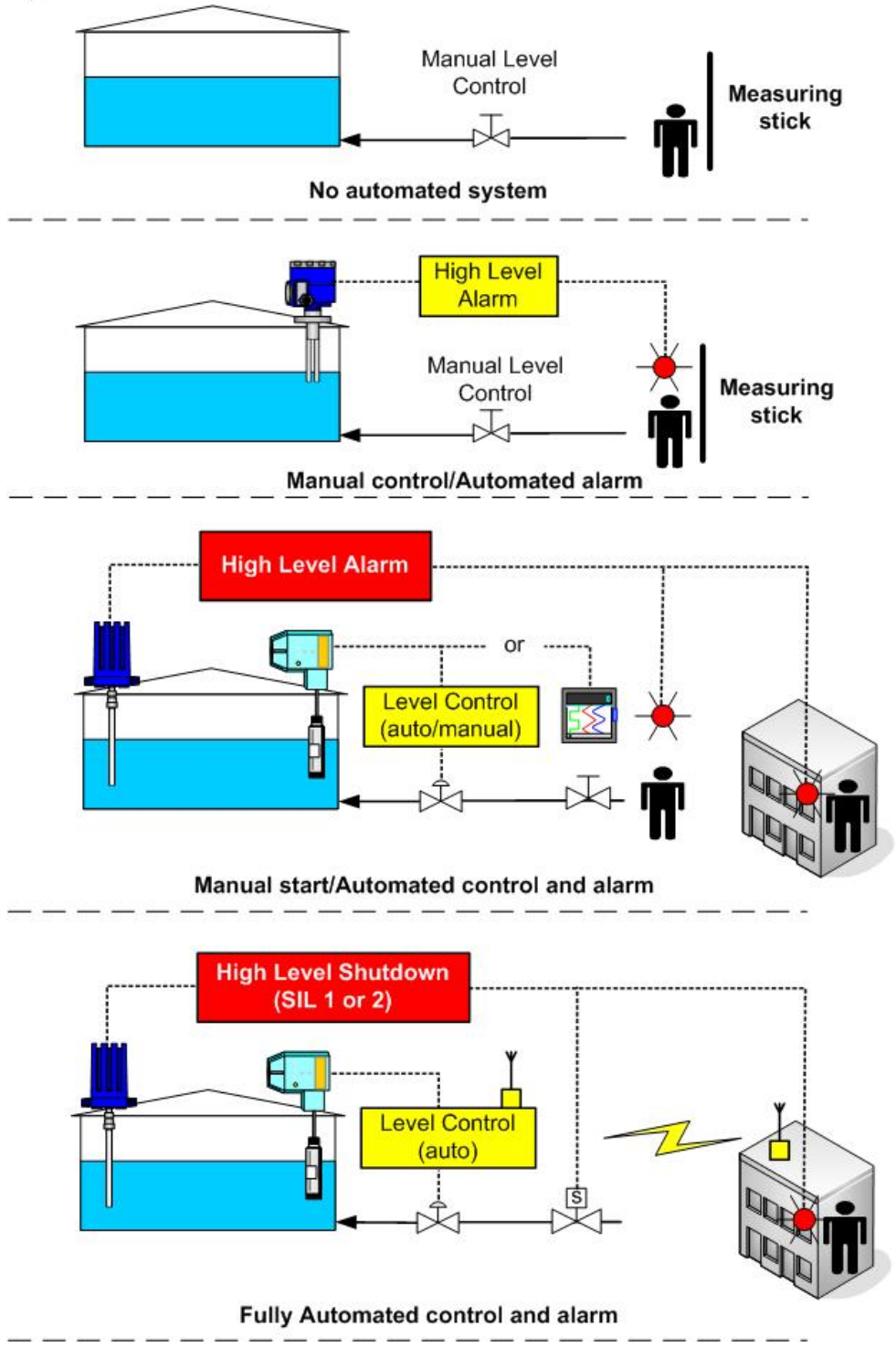

Figure 1. Examples of automation commonly found in tank farms and terminals

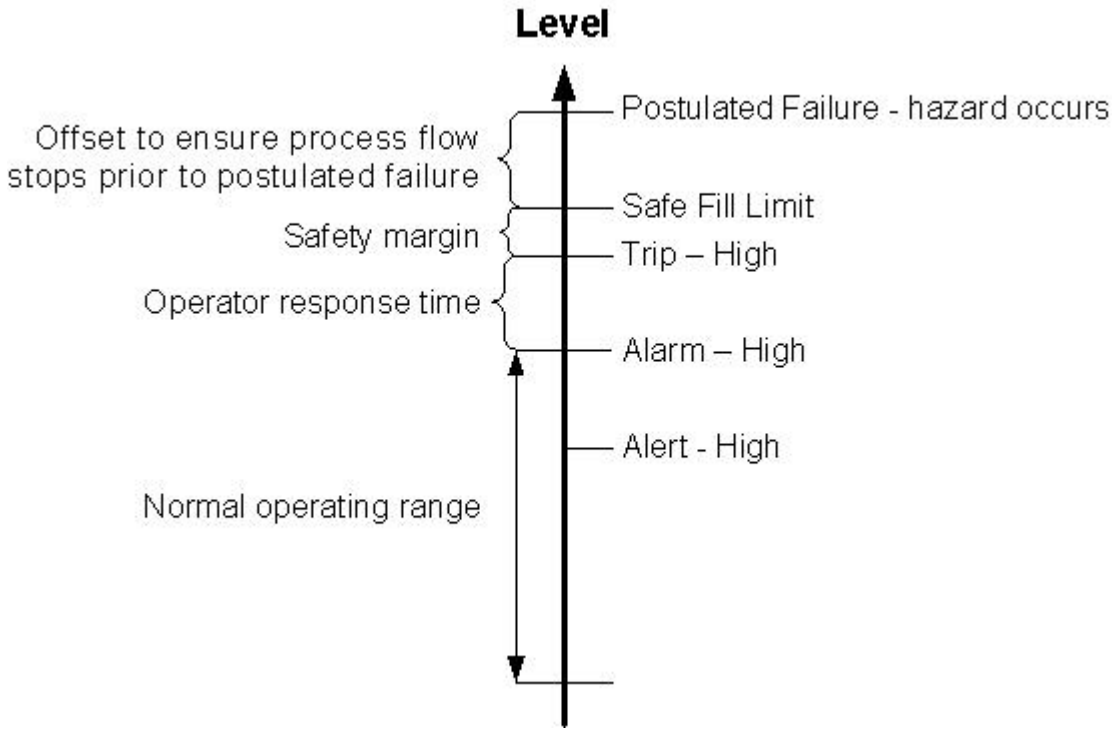

Figure 2. Range of Level Showing Transition from Normal Operating Range to Vessel Failure for High Level Events