



Overfill Protective Systems - Complex Problem, Simple Solution

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

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 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 of the worst industrial incidents in process industry history.

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 residents experienced cold showers and freezing nights 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 provides an overview of how each incident propagated from loss of level control to catastrophic event. It then discusses the following factors that contributed to these incidents:

1. Lack of hazard recognition
2. Underestimating the likelihood of overfill
3. Excessive reliance on operator
4. No defined safe fill limit
5. Inadequate mechanical integrity

Finally, it provides a simple 7 step solution for overfill protection.

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 remove 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 (15) 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 (15) temperature went as low as -48C, causing cold temperature embrittlement (1, 14). 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 achieves a specified set point defined in the operating procedure, the operator controls 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 (10) 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 geiser 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 (5). 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 excess fuel to be fed into a terminal tank for 11 hours (11). The fuel overflowed through the tank conservation vents for approximately 40 minutes (13) prior to ignition, producing a large vapor cloud estimated to be 8 hectares in size (12). At the time of the release, ambient conditions were near freezing with a dense fog. When the vapor cloud ignited, the resulting explosion caused significantly more damage than consequence models predicted. The cold, icy, and wet ambient conditions are believed to have intensified the explosion, which is currently considered the largest peacetime explosion in European history (11) producing a tremor measuring 2.4 on the Richter scale and blowing out windows five miles away from the site (12).

Five gaps

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 the BP and Esso incidents, the normal operating level was significantly below what would threaten the column integrity. At Buncefield, the operating level was simply inventory to be managed and normally varied 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 its structural design limits. Many overfills result in loss of containment when liquid passes to downstream equipment that is not designed to receive it.

At Texas City, the hazard analysis of the raffinate splitter did not consider high level in the splitter to be credible, because it would take more than 3 hours for the splitter to overflow (10). However, lifted column trays are frequently found during internal inspections of columns in the process industry, indicating



that high level does occur in many columns. Experience has also shown that sometimes operators deliberately retain liquid in columns to ride out upsets of downstream equipment.

No hazard analysis was performed at Longford, but it is likely that the team would have assumed that the absorption tower was designed to receive whatever liquids came to it. The likelihood of overflow worsens as debottlenecking allows increased production rates that yield a higher rate of level rise than historical experience indicates. At Longford, the tower rapidly overflowed due to excess flow from the platform (1).

Underestimating the likelihood of overflow

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 in manual operation and closed 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 overflow 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 overflow. 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 overflow is complicated by the combination of manual and automated control that is 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 generally 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 operating 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 will not adequately monitor level, especially during intense work periods. Overflow is a credible event and it takes good operator procedures to reduce its likelihood.

Excessive reliance on operator

In the Esso, BP, and Buncefield events, the initial incident investigation blamed the operator for not maintaining level. BP took disciplinary action against supervisors and hourly employees who were directly



responsible for operating the isomerisation unit on March 22 and 23, blaming operators for ignoring procedures (6). Esso blamed the control room operator for ignoring alarms and not following procedures even though the system generated more than 300 alarms per day (7, 8).

The “blame the operator” tendency is encouraged by the length of time required to reach overflow. 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. Some facilities have been debottlenecked and expanded to increase production. This has increased operator work load and eroded the time available for operator response to abnormal events. In some cases, the available time has been reduced to the point where manual response is no longer effective and automatic level control must be considered.

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 response and means to verify the process response. Further, there should be time to evacuate the area if the process response is not 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 considered to reduce operator exposure to the hazardous event. For significant hazardous events, automated trips ensure protection is continuously provided even when the operator is focused on other duties. An automatic trip can detect high level and prevent filling beyond the safe fill limit.

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.

For example, in the BP Texas City design, the column level was measured in the first ten feet of the column only. When the transmitter range was exceeded, the level on the operator display remained unchanged even though the level continued to rise. The high level alarm was also located in the bottom part of the column, indicating an abnormal process condition, but not an unsafe one. It was considered normal during start-up for the column to be filled higher than the alarm set point. The unit had experienced many start-ups with high bottoms level without incident. The problem was that no limit was set on how high is unsafe.

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 set point should allow enough time for the operator to take response to prevent the level from reaching the safety alarm or trip set points. 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 set point and the safe fill limit is the design safety margin. When an alarm is also implemented, the alarm set point should be conservatively set below any trip set point, allowing the operator sufficient time to take the process to a safe state prior to the trip being initiated. The operator must be capable of taking effective action after receiving the alarm; otherwise it will be treated as a trip notification rather than something requiring action.

Inadequate mechanical integrity

The Buncefield and Texas City incidents involved level switches that failed to operate correctly during the incident. This seems to support the concept that level switches are bad. However, evidence shows that the sensor was not installed properly in Buncefield and was not maintained in Texas City. No signal processor – digital or analog - works if the sensor is not installed properly or maintained. 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. This may be good practice for other process variables, but level is different. For columns and storage tanks, the safe operating limit is significantly outside the normal operating level, resulting in the high level alarm or trip sensors being at a very low 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. Consequently, it is an acceptable practice to implement storage tanks with an automated tank gauging system that uses an analog measurement covering the expected normal operating range and a discrete level switch that is used 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 the most expensive device to fail. There are many technologies available for level measurement and detection, from simple float type discrete switches to new advanced guided wave radar transmitters. Each technology has characteristics that make it the right choice for a particular application (9). For most safety applications, the main considerations for equipment selection are the 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 set points. Although transmitters may not increase diagnostics in services that normally do not have level, they do provide the ability monitor and alarm over a chosen 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 set point. Testing must prove that the



equipment can operate as required to prevent overflow. Although diagnostics can detect many types of failures, a proof test is necessary to demonstrate operation at the required set point. This is the only test that proves that the device works as required.

Buncefield had no provisions for full functional testing of the sensor without raising the level to the trip set point. Raising the level is a simple way to demonstrate device operation, but may present unacceptable risk in some applications. At Buncefield, no full test was ever performed, so the flawed installation was never corrected. All safety equipment must be installed with means that allow positive confirmation of their operation at the specified set point. This may include stilling wells or float chambers with facilities to simulate level.

Solution

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

1. Acknowledge that overflow of any vessel is credible regardless of the time required to overflow.
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 set point that provides sufficient time for the operator to bring the level back into the normal operating range prior to reaching a trip set point.
5. When the overflow leads to the release of highly hazardous chemicals or to significant equipment damage, design and implement an overflow protection system that provides an automated trip at a set point that allows sufficient time for the action to be completed safely. Risk analysis should be used to determine the safety integrity level (SIL) required to ensure that the overflow risk is adequately addressed. While there are exceptions, the majority of overflow protection systems are designed and managed to achieve SIL 1 or SIL 2.
6. Determine the technology most appropriate for detecting level during abnormal operation. The most appropriate technology may be different from the one applied for level control and custody transfer.
7. Finally, provide means to fully proof test any manual or automated overflow protective systems to demonstrate the ability to detect level at the high set point and to take action on the process in a timely manner.



REFERENCES

- Wikipedia, "1998 Esso Longford gas explosion," http://en.wikipedia.org/wiki/1998_Esso_Longford_gas_explosion.
- Wikipedia, "Texas City Refinery (BP)," [http://en.wikipedia.org/wiki/Texas_City_Refinery_\(BP\)](http://en.wikipedia.org/wiki/Texas_City_Refinery_(BP)).
- 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).
- 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.
- Wikipedia, "2005 Hertfordshire Oil Storage Terminal Fire," http://en.wikipedia.org/wiki/2005_Hertfordshire_Oil_Storage_Terminal_fire.
- The Chronicle, Anne Belli, "BP blames staff for blast," May 18, 2005, Houston, Texas, <http://www.chron.com/disp/story.mpl/special/05/blast/3186965.html>.
- Doig, Meredith, "Longford – Why efficiency is the enemy of safety," originally published in The Manager Online Magazine (now ceased) in June 1999, <http://www.unisa.edu.au/corpsocialresp/casestudies/longford.asp>.
- O'Brien, Kerry, "Esso has cover-up strategy: Longford disaster allegations," <http://www.abc.net.au/7.30/stories/s23848.htm>.
- Boyes, Walt, "First the application, then the product," ControlGlobal.com, <http://www.controlglobal.com/articles/2007/022.html>.
- Mogford, J., "Fatal Accident Investigation Report: Isomerization Unit Explosion," Final Report, Texas City, Texas, USA (2005).
- British Broadcasting Station, "Buncefield tank was overflowing," May 9, 2006, United Kingdom, http://news.bbc.co.uk/2/hi/uk_news/4752819.stm.
- The Guardian, David Fickling, "Faulty fuel gauge caused Buncefield Explosion," United Kingdom, <http://www.guardian.co.uk/uk/2006/may/09/buncefield.davidfickling>.
- 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>
- Kletz, Trevor, "Lessons from Longford – The Esso Gas Plant Explosion," Chemical Engineering Progress, September 1, 2001.
- 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/>

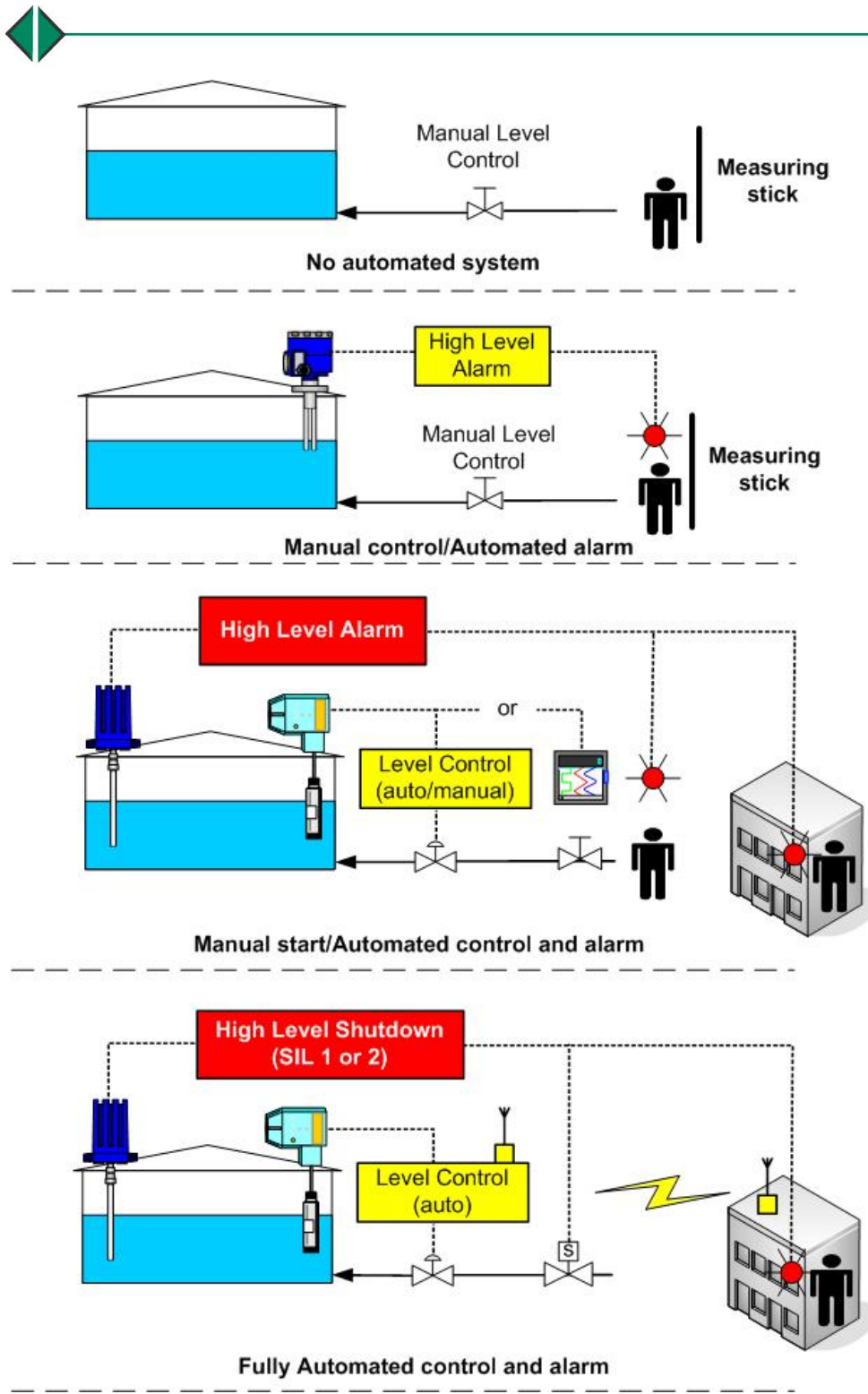


Figure 1. Examples of automation commonly found in tank farms and terminals

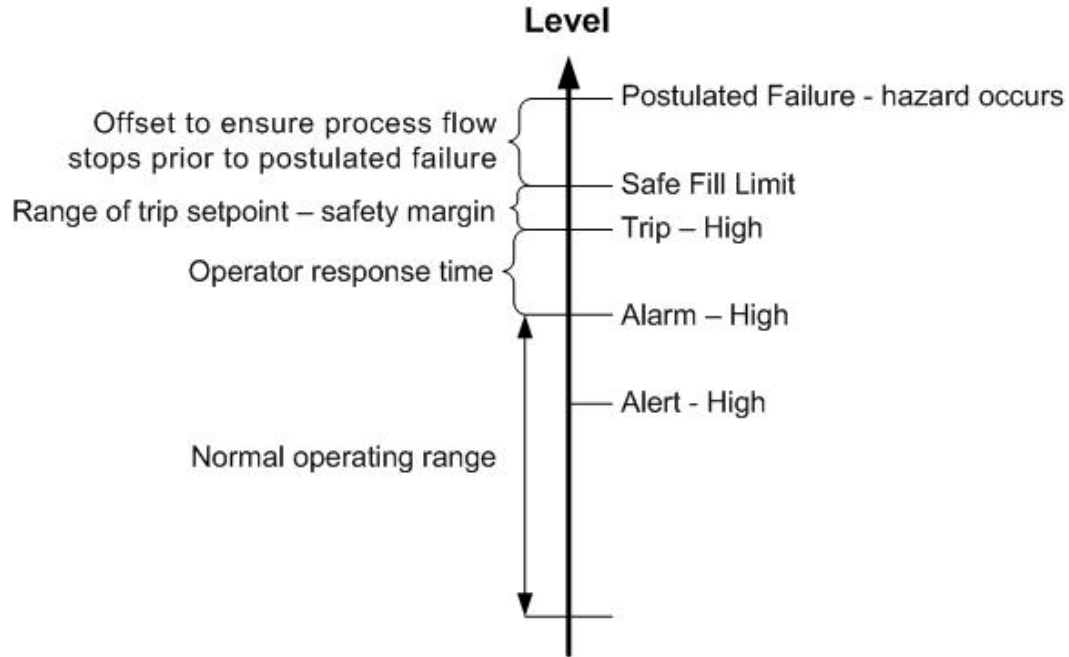


Figure 2. Range of Level Showing Transition from Normal Operating Range to Vessel Failure for High Level Events