Overfill Protective Systems
Complex Problem, Simple Solution

Angela E. Summers, PhD, PE
President
SIS-TECH Solutions, LP
Esso Longford

September 25 1998

- Excess flow from the Marlin Gas Field
- Too much condensate entering absorption tower
- Led to high level in a separator drum and shutdown of the lean oil pump

- The demethanizer reboiler cold temperature embrittled, leading to stress fracture when the lean oil pump was re-started

2 fatalities, 8 injuries, and A$1.3 billion costs
BP Texas City
March 23 2005

- Raffinate splitter was fed at normal rates for more than 3 hours 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.
- Flow from the splitter overwhelmed the drain capacity yielding a geiser of hydrocarbons from the drum stack.

15 fatalities, 170 injuries, and US$1.6 billion costs
Buncefield
December 11 2005

- Occurred when the automated tank gauging system failed allowing excess fuel to be fed into a terminal tank for 11 hours.

- Fuel exited the tank conservation vents for approximately 40 minutes prior to ignition.

43 injuries and £1 billion costs
Contributing Factors to 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
Lack of hazard recognition

- Absolute level usually not important
  - BP and Esso - normal operating level was significantly below what would threaten the column
  - Buncefield - the operating level varied across a large range
- High level is not considered a hazard
  - At Texas City - did not consider high level in the splitter to be credible
Lack of hazard recognition

- Interconnected equipment hazard missed or underestimated
  - MI challenged when liquid passes to downstream equipment that is not designed to receive it

- The tendency is for:
  - The sending PHA to treat high level as an event that the downstream unit is designed to receive
  - The receiving PHA to treat receiving liquid as an upset that their unit is designed to handle.
Underestimating the likelihood of overfill

- Absolute level often does not:
  - Affect the unit operation or
  - Cause any other significant process variable disturbance until the safe fill level is exceeded

- High level may have different causes in each mode of operation
  - start-up, normal, or upset conditions.
Underestimating the likelihood of overfill

- The slower the event
  - the greater the tendency to believe in the operator
- The more sporadic the event
  - the greater the tendency to believe it will not last long enough
- Especially attractive when the existing design does not have a high level alarm or trip.
Excessive reliance on operator

- Esso, BP, and Buncefield
  - Initially blamed the operator for not maintaining level
  - BP blamed operators for ignoring procedures
  - Esso blamed the control room operator for ignoring alarms and not following procedures
Excessive reliance on operator

- Work load and piping network complexity decrease the operator’s ability to reliably control level and maintain process safety.

- Personnel hazards should be considered when directing operators to take manual actions in the process unit
  - Local response generally moves the operator into the hazard zone increasing the risk to that individual.
No defined safe fill limit

- Entire level range from empty to postulated failure point is often not displayed
- BP Texas City - column level was measured in the first ten feet of the column only
  - the level indicated on the operator display remained unchanged even though the level continued to rise
No defined safe fill limit

- Offset to ensure process flow stops prior to postulated failure
- Range of trip setpoint – safety margin
- Operator response time

Normal operating range

Level

- Postulated Failure - hazard occurs
- Safe Fill Limit
- Trip – High
- Alarm – High
- Alert - High
Inadequate mechanical integrity

- There are no bad level devices
  - technology misapplications
  - improper installations
  - inadequate mechanical integrity programs
- Years of neglect will allow the most expensive device, high technology device to fail
Inadequate mechanical integrity

- Functionality is demonstrated by forcing the sensor to “see the process variable” and to generate the correct signal at the specified setpoint
- Provide means to support complete proof testing
  - stilling wells or
  - float chambers
Solution

- Risk Analysis
- Process Design and Control
- Automatic Overfill Protective Systems (AOPS)
Risk Analysis

- Accept Overfill as credible
  - Regardless of the time required to overfill.
- Identify high level hazards
- Address the risk in the unit where it is caused
- Determine the safety integrity level (SIL)
  - While there are exceptions, the majority are SIL 1 or SIL 2.
Process Design and Control

- Determine the safe fill limit
  - the mechanical limits of the process
  - the measurement error
  - the maximum fill rate
  - time required to complete action that stops filling

- Implement independent high level alarm, when effective
  - Must be sufficient time to stop level risk prior to any trip setpoint.
Automatic Overfill Protective Systems (AOPS)

- Design and implement an overfill protection system
- Determine most appropriate technology for detecting level during abnormal operation.
- Provides an automated trip at a setpoint that allows sufficient time for the action to be completed safely.
- Provide means to fully proof test the systems
  - Demonstrate ability to detect level at the high setpoint and to take action on the process in a timely manner
Summary

- Overfill events can be expensive.
  - > 1 billion Aus, US, £
- The solution can be very simple:
  - Safe Fill Limit
  - Alarm and Shutdown
Questions?