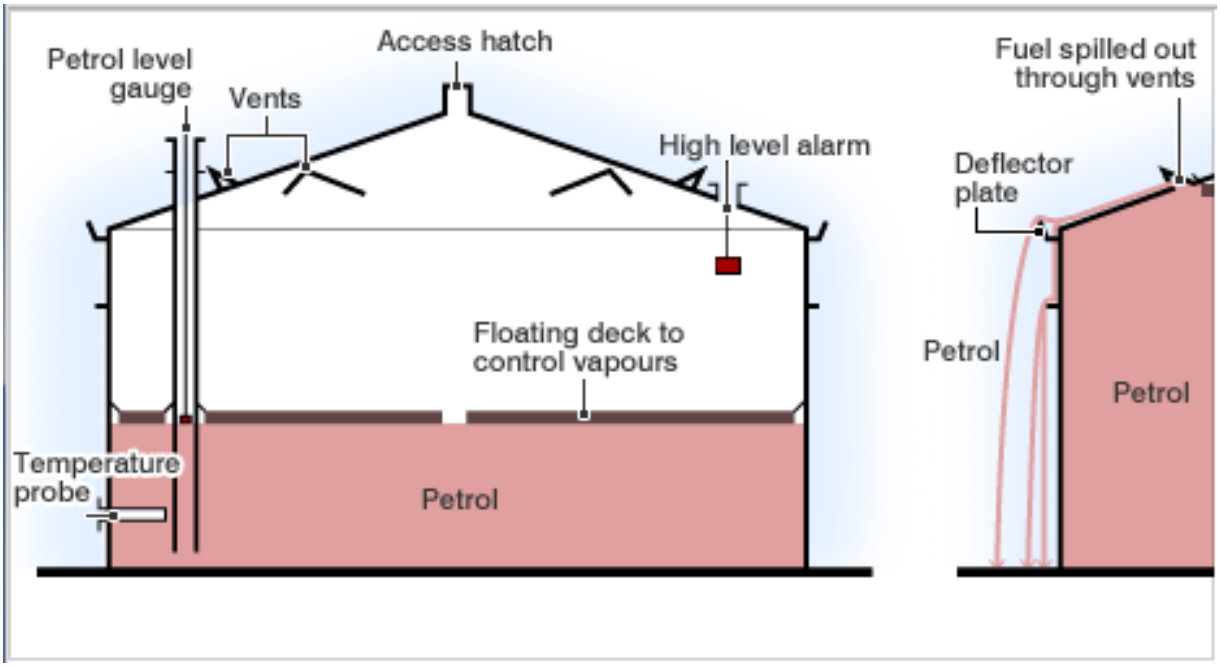
SIS-TECH
12621 FEATHERWOOD, STE 120
HOUSTON, TX 77034
713-909-2100

Case Study: Hemel Hempstead, England (December, 2005)

In the following example, an ineffective instrumentation maintenance and repair program combined with undermanaged instrument change and other automation deficiencies, leading to a vapor cloud explosion.

Impact: Explosion and fire; 43 injuries; 2,000 evacuated, commercial and residential damage

Vessel Diagram:



Summary:

Gasoline was being delivered to Tank 912, starting on the day before the incident. Early the next morning, the Automatic Tank Gauging (ATG) system displayed an unchanging level in Tank 912, although the tank continued to fill. A 'flat-lined' signal, where the sensor or transmitter output is stuck and the signal it sents to the control system is no longer related to the process condition, is a known dangerous failure mode for the level guage technology used in this vessel. This type of failure can be difficult to detect by operators,

because the output is still within the acceptable range for the process variable. A review of the instrumentation data revealed that the level gauge in this tank had 'flat-lined' 14 times in the 3.5 months leading up to this incident, but this frequent malfunction was not recognized as being an abnormal situation and so was not escalated to senior supervision for resolution prior to the incident.

The 'user', 'high', and 'high high' level alarms used the same tank level transmitter, so the failure of the shared transmitter rendered these alarms inoperative. By practice, the operator controlled level by terminating transfer upon receipt of the 'user' alarm. Since it was not available, the operator did not take action to terminate transfer.

An independent high-level switch, set above the ATG high-high level, was designed to close inlet valves and activate an audible alarm, but it also failed. Eighteen months prior to the incident, the high level switch had been changed out for a different technology which the instrument maintenance team did not fully understand. The high level switch became disabled when maintenance, not understanding the full outcome of their decision, failed to reinstall a lock on the switch test arm after performing work. Without the lock, the level switch was not activated when the float was lifted. This systematic failure demonstrates the importance of ensuring that maintenance and repair procedures, labeling, and training be used to sustain integrity.

By late afternoon, the tank overfilled and contents spilled out of tank roof vents. A vapor cloud was formed and noticed by tanker drivers and by people outside the facility. The fire alarm was activated and firewater pumps were started. An explosion occurred a short time later, likely ignited by the startup of the firewater pumps.

Instrumentation and Controls Gaps:

- Inadequate / no risk assessment
- Analog level gauge not maintained, 14 dangerous failures (stuck) in preceding 3.5 months
- Analog level gauge criticality not recognized, safety implications of frequent dangerous failures not noted or logged.
- Analog failure unnoticed, lead to ATG system malfunction / 'flatline'
- 3 alarms failed to activate as a result of analog level failure
- Level switch technology changed without adequate change management
- Incorrect level switch installation
- Separate high level interlocks failed
- Inadequate ATG HMI
- No measurement validation / deviation alarm
- ESD shown on HMI but never implemented

Key Automation Learning Points:

The test facility disabled the high level detection when a padlock was not replaced on the test arm. The manufacturer manual contained a warning that the padlock needed to be in place. It is critical to train maintenance staff on how to properly test new or modified equipment and how to verify that the equipment has been properly returned to service. Labeling and warning signs should be considered to enhance recognition of critical features and configuration.

In addition, instrument repair procedures should include a check for unacceptably high failure rates. For example, the analog level gauge in this case had failed many times in the few months preceding the event. Written instructions should be provided on how to escalate these situations to maintenance and facility leadership for investigation and correction.

Sources:

HSE. 2007. Buncefield Standards Task Group (BSTG) Final Report. UK: Health and Safety Executive.