Major Accident Case Studies

Buncefield explosion and fire

Summary

On the night of Saturday 10 December 2005, Tank 912 at the Hertfordshire Oil Storage Limited (HOSL) part of the Buncefield oil storage depot was filling with petrol.
The tank had two forms of level control: a gauge that enabled the employees to monitor the filling operation; and an independent high-level switch (IHLS) which was meant to close down operations automatically if the tank was overfilled. The first gauge stuck and the IHLS was inoperable – there was therefore no means to alert the control room staff that the tank was filling to dangerous levels. Eventually large quantities of petrol overflowed from the top of the tank. A vapour cloud formed which ignited causing a massive explosion and a fire that lasted five days.

After the incident

After the incident

Before the incident

The gauge had stuck intermittently after the tank had been serviced in August 2005.
However, neither site management nor the contractors who maintained the systems responded effectively to its obvious unreliability. The IHLS needed a padlock to retain its check lever in a working position. However, the switch supplier did not communicate this critical point to the installer and maintenance contractor or the site operator. Because of this lack of understanding, the padlock was not fitted.
Having failed to contain the petrol, there was reliance on a bund retaining wall around the tank (secondary containment) and a system of drains and catchment areas (tertiary containment) to ensure that liquids could not be released to the environment. Both forms of containment failed. Pollutants from fuel and firefighting liquids leaked from the bund, flowed off site and entered the groundwater. These containment systems were inadequately designed and maintained.

Failures of design and maintenance in both overfill protection systems and liquid containment systems were the technical causes of the initial explosion and the seepage of pollutants to the environment in its aftermath. However, underlying these
immediate failings lay root causes based in broader management failings:

- Management systems in place at HOSL relating to tank filling were both deficient and not properly followed, despite the fact that the systems were independently audited.
- Pressures on staff had been increasing before the incident. The site was fed by three pipelines, two of which control room staff had little control over in terms of flow rates and timing of receipt. This meant that staff did not have sufficient information easily available to them to manage precisely the storage of incoming fuel.
- Throughput had increased at the site. This put more pressure on site management and staff and further degraded their ability to monitor the receipt and storage of fuel. The pressure on staff was made worse by a lack of engineering support from Head Office.

Cumulatively, these pressures created a culture where keeping the process operating was the primary focus and process safety did not get the attention, resources or priority that it required.

immediate cause
The immediate cause of this major incident was the failure of both the ATG and the IHLS to operate as the fuel level in Tank 912 increased. This was a loss of 'primary' containment.

This report also serves to reinforce some important process safety management principles that have been known for some time:

There should be a clear understanding of major accident risks and the safety critical equipment and systems designed to control them.
This understanding should exist within organisations from the senior management down to the shop floor, and it needs to exist between all organisations involved in supplying, installing, maintaining and operating these controls.

There should be systems and a culture in place to detect signals of failure in safety critical equipment and to respond to them quickly and effectively.
In this case, there were clear signs that the equipment was not fit for purpose but no one questioned why, or what should be done about it other than ensure a series of temporary fixes.

Time and resources for process safety should be made available.
The pressures on staff and managers should be understood and managed so that they have the capacity to apply procedures and systems essential for safe operation.
Once all the above are in place:
There should be effective auditing systems in place which test the quality of management systems and ensure that these systems are actually being used on the ground and are effective.
At the core of managing a major hazard business should be clear and positive process safety leadership with board-level involvement and competence to ensure that major hazard risks are being properly managed.

Underlying causes – deficiencies in following areas

- The independent high-level switch
- The automatic tank gauging system
- Redundant emergency shutdown
- System security
- Alarm function
- Control of incoming fuel
- Increase in throughput
- Tank filling procedures
- Pressure of work
- Inadequate fault logging
- Motherwell Control Systems

- Loss of secondary containment – bund joints, tie bar holes, Pipe penetrations and tertiary containment
- Emergency arrangements
- Safety management systems, managerial oversight and leadership

‘Clear and positive **process safety leadership** is at the core of a major hazard business and is vital to ensure that risks are effectively managed. It requires board-level involvement and competence. Board-level visibility and promotion of process safety leadership is also essential to set a positive safety culture throughout an organisation. ’

In relation to the Buncefield incident:

- the process safety controls on safety critical operations were not maintained to the highest standard;
- senior managers did not apply effective control;
- effective auditing systems were not in place. Auditing and monitoring arrangements focused on whether a system was in place; the audits did not test the quality of the systems and, most importantly, did not check whether they were being used or were effective.

Some of the managerial failings:

- poor communications at shift handover;
- lack of engineering expertise on site; and
- failure to implement management of change processes.

Buncefield explosion and fire - inoperative high level alarms and IHLS

The sticking gauge and inoperative IHLS were the technical causes of the overfilling of Tank 912. Failures of design and maintenance in both overfill protection systems and liquid containment systems were the technical causes of the initial explosion and the seepage of pollutants to the environment in its aftermath.

Alarms

1. **Three 'high level' alarms. These were:**
   - the 'user high' which could be set by the supervisor to indicate that intervention was required;
   - the 'high' level – set at a level in the tank below its maximum working level; and
   - the 'high-high' level – set below the level at which the IHLS was intended to operate.

2. **Independent high-level switch (IHLS)**

At 0305 hrs on Sunday 11 December the ATG display 'flatlined', that is, it stopped registering the rising level of fuel in the tank although the tank continued to fill. Consequently, three ATG alarms, the 'user level', the 'high level' and the 'high-high level', could not operate as the tank reading was always below these alarm levels. the control room supervisor was not alerted to the fact that the tank was at risk of overfilling. The level of petrol in the tank continued to rise unchecked.

The tank was also fitted with an independent high-level switch (IHLS) set at a higher level than the ATG alarms. This was intended to stop the filling process by automatically closing valves on any pipelines importing product, as well as sounding an audible alarm should the petrol in the tank reach an unintended high level. The IHLS also failed to register the rising level of petrol, so the 'final alarm' did not sound and the automatic shutdown was not activated.

System security

The security arrangements on the ATG system were lacking. It had its own built-in security system but this had been set so that all control room staff could modify any parameter including being able to change the alarm settings.

'Process safety protection systems should not rely on operator response to alarms and that overfill protection should be independent of normal operational monitoring'.

Additional resources:

https://www.hse.gov.uk/comah/buncefield/index.htm
https://www.hse.gov.uk/research/rrpdf/rr1129.pdf
https://www.hse.gov.uk/comah/guidance/response-programme.pdf
https://www.bbc.co.uk/news/uk-10266706