0260-9576/09/$17.63 + 0.00

Lessons from Buncefield

Mark Hailwood
LUBW, Karlsruhe, Germany

The Buncefield Major Incident Investigation Board (MIIB) have published their final report[1], and the civil proceedings for the compensation of the various parties affected by the fire, explosion and other consequences of the disruption caused by the incident are under way[2]. Criminal proceedings were due to commence in January 2009[3]; however, at the request of the defendants, they have been adjourned until May[4].

Extensive explanations of the most likely mechanisms for the evolution of the explosive petroleum vapour/air cloud have been published, as well as detailed descriptions of the status of flow in the pipelines and the failure of the level gauge, and critically the failure of the overfill protection device to actuate. For the future prevention of similar accidents it is not sufficient to know what happened, it is also necessary that the lessons to be learned are identified and that these lessons are transferred into actions. This article reviews some of these lessons.

Lessons on overfill protection

The central initiating event in the Buncefield incident was the overfilling of Tank 912 at Hertfordshire Oil Storage Limited (HOSL). Despite the tank being fitted with an independent overfill protection device (OPD) this piece of equipment failed to actuate and thus prevent the further flow of petroleum into the tank.

> Overfill protection is not provided by a single device, but by an overfill protection system. That is the OPD — the electronic system initiating the alarm and the response.

The response should ideally be an automatic shut-off of the transfer process, i.e. switching off pumps and closing valves. This may not always be possible due to technical or regulatory difficulties; for example, a particular case being the transfer from a ship or barge which unloads using on-board pumps, but which cannot be brought into the automatic shut-off system. In such cases it is of utmost importance that the hi-alarm and the hi-hi-alarm are accompanied by appropriate audible and visual alarm signals.

> Levels for the alarms should be set so that, taking into account the pumping rates and the response times, there is sufficient opportunity for the operators to respond.

Alarms should be logged and in particular the triggering of hi-hi-alarms should be investigated.

> Where automatic shut-off systems are in place, care should be taken to ensure that the filling of a tank cannot commence with an inactive overfill protection system.

This may be due either to an inappropriate mode of operation being selected (as may be inferred from the MIIB report and the HSE Alert[5]) or the OPD being without power due to it being on another electrical circuit to the pumps and valves, which is out of operation (See Incident 0603 from 04/06/2006 of the German Federal Central Major accident Database)[6].

Lessons on tank design

The tank design in Buncefield is seen by the MIIB as being a major contributor in the development of the vapour cloud. This has led many site operators to

[1]Buncefield Major Incident Investigation Board (2008), The Buncefield Incident 11 December 2005, The final report of the Major Incident Investigation Board, ISBN 978 0 7176 6270 8
[2]Court to decide who is to blame for Buncefield fire, http://www.telegraph.co.uk/news/3118756/Court-to-decide-who-is-to-blame-for-Buncefield-fire.html
[3]Health and Safety Executive, Press Releases 11 December 2008 B002:08, http://www.hse.gov.uk/press/2008/b08002.htm
[4]http://www.hemeltoday.co.uk/news/Buncefield-prosecution-delayed.4899900.jp
[5]http://www.hse.gov.uk/comah/alerts/tavcheclist.htm
[6]0603 (2006-05-04 Überfüllung eines unterirdischen Ethanollagertanks in einem Tanklager), http://www.infosis.bam.de/zema/zema_search_fs.php

discount the relevance of the Buncefield incident for their own site as their tanks are built to a different design. This is particularly the case where tanks have a fixed roof, are completely enclosed and connected to a vapour recovery system. The lesson to be learned in this case is:

> If the overfill protection system fails then without intervention by the operators the tank contents will fill to roof level.

This may seem an obvious statement, however if this is not recognised then the consequences of this may also not be realised. In Buncefield the contents then overflowed through the roof openings as the internal floating cover was pushed up against the tank roof. Where can the liquid go in a completely enclosed, fixed roof tank? Vapour recovery systems are designed, as their name suggests, to receive vapour phase as the tank contents rise in order to reduce VOC emissions to the atmosphere. They are not designed to receive liquid phase and certainly not at a flow rate of several hundred cubic metres per hour. Fixed roof tanks are usually fitted with P-V-valves with flame arrestors in order to avoid the tank collapsing as a result of vacuum or being damaged due to excess pressure during filling operations or thermal expansion due to the effects of weather. However P-V-valves with flame arrestors are not suitable for liquid flow. This means that the least worst-case scenario is that the tank roof will tear at the roof/tank wall weld and the pressure will be released in this way: the alternative is catastrophic failure of tank, which cannot be discounted.

> Thought needs to be given to the degree of integrity of overfill protection systems and the consequences of their failure. Are the systems 'fail safe' and how will the tank design respond?

Lessons on scenarios and models

Prior to Buncefield, the general assumption in many cases, not just in the UK but also throughout the rest of Europe, was that the worst case scenarios which needed to be considered were: a single tank fire; a fire in a single bund; or the failure of the largest tank within a bund. Assumptions were made and theories postulated on the effectiveness of fire-fighting measures and cooling systems without considering their own vulnerability to the effects of fire or explosion. This was despite the fact that large-scale multiple tank fires in Europe were known and that above ground pipe-work for foam and water distribution is extremely exposed to fire, explosion or missile damage.

> The loss prevention community needs to take account of past events in developing scenarios for safety reports and emergency plans.

The use of current models together with the selection of the relevant parameters to take account of the materials stored and the geometry of the site indicate that an explosive atmosphere could occur which would lead to peak over-pressures in the order of those observed in the Buncefield incident. The consideration of multiple tank fires based on the newest models shows a more intense thermal radiation than is predicted from the consideration of single tanks.

However it should never be forgotten that all models have limitations and that events occur which lie without the bounds of these models.

> It is important that scenarios are developed using suitable models and that the calculations are carried out using data which is relevant to the situation being considered.

This leads to a number of other questions in relation to petroleum storage facilities:

- How many of the calculations are carried out based on summer gasoline and on winter gasoline? The difference in the proportions of the individual components leads to markedly different characteristics.
- How many of the sites storing gasoline have considered the consequences of the addition of ethanol to the chemical and physical properties of the fuel? This relates not just to the flammability and explosibility limits (Note: the presence of ethanol requires different flame arrestors to standard gasoline), but also to the change in water solubility/miscibility which alters the potential for environmental contamination.

Lessons on safety management

The lessons on safety management are drawn from observations from outside the MIIB investigation and from journalistic reporting on the civil proceedings in the High Court. This means that they are inferred and not necessarily based on statements of fact from the MIIB. The criminal prosecution has, at the time of writing, not yet commenced. The statements made here should not be taken to indicate personal blame or culpability.

Those who operate major hazard sites should clearly define who, within which organisational structure is responsible for the overall and for the day-to-day operation of the facility. This is particularly important for operations which are run, for example, as joint ventures or under the umbrella of a holding company, which either may not have an independent organisational character of their own or even employ any staff of their own. As the civil dispute in the High Court has clearly shown, this matter can come to a head when the question of liability is raised. This is not just a matter of financial regulation, it defines the culture and the regime in which the whole safety management system is embedded and this has a marked effect on the overall safety of the facility.

> The roles and responsibilities of individuals and organisational units for the overall operation and the day-to-day running of the facility should be clearly defined.

Within the standard operating procedures for any facility the operating envelope should be clearly defined. This means that the filling levels, temperatures, pressures, flow rates, etc. should remain within these defined limits and that the process should not be run on trips and alarms. This accordingly means that alarms should be managed. If a plant operator discovers (by whatever means, be it oral tradition, trial and error, or habit) that the process 'runs just as well' using trips and alarms and that this is tolerated by management, then this will over time become accepted practice. The manual over-riding of alarms is also a practice which management should regularly and critically review. Whilst not mentioned in relation to the Buncefield incident, it is not unknown for an 'economic optimisation of the storage facility' to take place by utilising the volume between the hi-alarm (where normal storage ends) and the hi-hi-alarm (which is often close to the maximum physical capacity of the tank). This is a potentially dangerous practice and in some countries constitutes a breach of the operating licence and is a criminal offence.

> Management should define the operating conditions for the facility, the triggering of alarms and trips should be documented, and a regular review be carried out.

Management should bear in mind that employees are generally not maliciously breaking rules (they should also be aware that there are exceptions to this) and that whenever activities take place which are not in accordance with the defined procedures, then there is an underlying cause which needs to be identified and appropriate measures adopted. Reviews of procedures should take place regularly and involve the operating personnel.

Concluding remarks

Space does not permit a detailed review of the Buncefield MIIB recommendations, thus this article is restricted to a few, more general lessons. These lessons can be applied to other facilities and are in no way specifically limited to petroleum storage facilities. Whilst major fires in tank storage facilities are relatively infrequent, they have occurred in the past. The existing technology and operating knowledge should be used to ensure that tanks are not overfilled and that loss of primary containment events are prevented. Further work is necessary to understand the complexity of vapour cloud explosions and the intensity of multiple tank fires, however this should not distract from the fact that overfilling of tanks is preventable and should be achieved. In this respect there needs to be further cooperation with maritime and inland shipping authorities to ensure that the ship to shore transfer of hazardous products can be integrated into the onshore safety systems.