REPEATED ACCIDENT CAUSES – CAN WE LEARN?

Peter Waite
Technical Director, Entec UK Limited

Over the last twenty years major process industry accidents have continued to occur despite the introduction of new regulations, (e.g. Offshore Safety Cases, COMAH and PSM), the efforts of safety professionals and widespread dissemination of "the lessons learned" from incidents.

There are some striking similarities between several of the well reported major accidents such as Piper Alpha, Pembroke Cracker, Texas City and Buncefield. Not all of these have been brought to the attention of all the disciplines which may be affected. This paper will consider two aspects in some detail (the interaction of instrumentation and human factors) to identify the common features which led to disaster despite the design safety, instrumentation and control systems which were designed to manage high liquid levels.

INTRODUCTION

Despite the best efforts of process engineers, equipment engineers and their safety advisers together with the supervision of the regulators, major process accidents continue to occur. Standards of manufacture, inspection and testing have been upgraded and the reliability of instruments and control systems have improved but have still failed to prevent accidents when they and the operators are faced with unusual situations, often described as abnormal or upset conditions. These may occur as a result of external disturbances, such as lightning strikes disrupting power supplies, or sudden changes to operating conditions, flow rates or mechanical failures. Even systematic hazard identification and risk assessment methods have not been able to foresee and help operators prevent accidents.

Experience gained from the study of accidents, reports and the general lessons to be learned, quoted by such as Kletz (e.g. 2001), suggest that many accidents are caused by either misinterpretation of information received by operators from the instrumentation and control systems, or alternatively by the instrumentation and control systems not being able to deliver sufficient information to diagnose and control the situation. Either of these could be described as "human error" but really come about because of a gap in understanding between the operators' mental model of the plant or process and the instrument and control designers' understanding of what the operator needs to know. (Often the design has not distinguished between the needs of operational control and control in abnormal/upset situations).

This paper addresses one particular category of accident cause that appears to recur on a regular basis, albeit in different types of plant. Many accidents have arisen from the over filling of vessels. This is despite the fact that it is a well recognised potential cause of accidental releases of hazardous materials and safeguards are normally in place to prevent it occurring.

The salient features of a number of these accidents are outlined followed by an analysis of the contribution of excess liquids to the accidents.

The reasons for the control systems or operators not taking appropriate action are then discussed.

Finally proposals to prevent and/or mitigate these (and similar) accidents in future are proposed.

LIQUID OVERFLOW

A simple case would be a liquid storage vessel close to ambient pressure as shown in Figure 1. Even before the Buncefield investigation recommendations it would be expected that such tanks for the storage of high hazard liquids would be equipped with a level monitoring device, a high level alarm and high – high level trip to shut-off incoming flow.

Figure 1 shows a system of generic overfill protection for atmospheric liquids storage.

Overfilling of the tank would result in the release of liquid through tank roof vents, as occurred at Buncefield (Newton et al. 2008). Atmospheric storage is equipped with secondary containment in the form of bunds to contain liquid spills but volatile liquid releases will lead to the formation of a vapour cloud which will escape the bund.

The high level alarm, high-high level alarm or trip and the actual overflow level are relatively close but separated by sufficient storage volume to allow operator action to shut off inflow before the next level is reached. There should also be a means of continuously monitoring the liquid level so that the operators can foresee when the normal fill limit will be reached. Until recently there were still some tanks which relied upon manual "dipping" of tanks before delivery of a liquid parcel to ensure that there was sufficient capacity to accept the consignment. It appears that operators may now regularly rely upon the high level alarm as an operational warning of a full tank, in the knowledge that there is a high-high level alarm/trip as back-up. However this effectively removes one level of protection as the high level alarm is designed as a back-up if the operator fails to respond to the continuous level monitor.

It should be noted that in the majority of hydrocarbon atmospheric storage tanks constructed since the 1980s overfilling does not threaten the integrity of the storage tank as they will have been hydrostatically tested to the

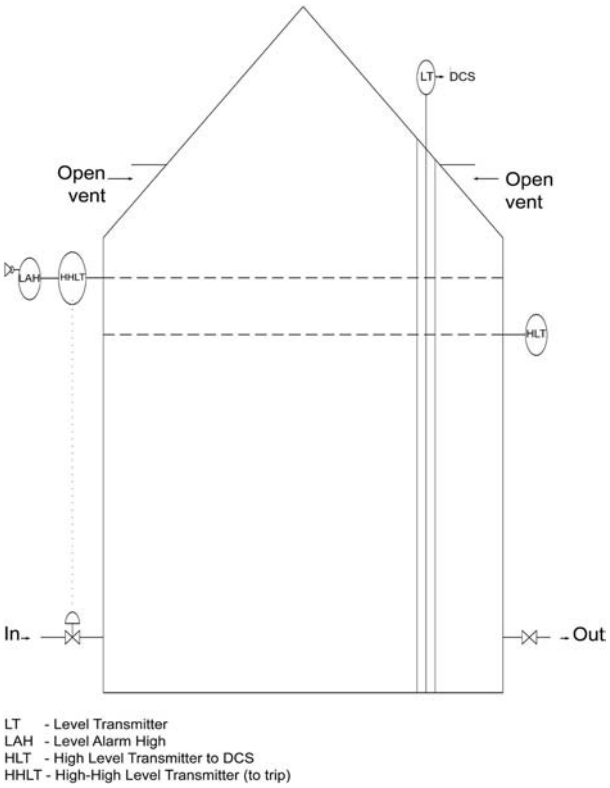

Figure 1. Generic overfill protection for atmospheric storage of flammable liquids

maximum fill level and the normal contents are less dense than water.

At Buncefield operators failed to realise how quickly the storage tank was filling, particularly after an increase in flow rate to the tank. This suggests that the liquid level was not being monitored and for normal operational control reliance was placed on High and High-High level alarms, thus permanently reducing the levels of protection. If the High-High Level Alarm/Trip was inoperative then there would be no additional levels of protection, because there was absolute reliance on the High Level Alarm as the operating control or monitoring device and no back-up. Hailwood (2009) discusses this in more detail and the methods for improvement.

EXCESS LIQUIDS IN PROCESS

Accidents have been caused by flooded columns and excess liquid in knock-out drums. In some cases columns have been deliberately over filled above normal operating levels (to make start-up easier, e.g. Texas City) and in other cases operators have failed to detect a blocked outlet (Pembroke Cracker). Knock-out drums have been overfilled due to a combination of inadequate/unavailable liquid removal capacity (Piper Alpha), or failure to switch to rapid liquid removal, combined with lack of accurate information on liquid level (Pembroke Cracker).

Figure 2 shows a typical arrangement similar to Texas City (Mogford 2005). There is level detection but the alarms are only set around the normal operating range. Therefore there are no alarms or trips set to prevent flooding or overflow above this range. But the operators adopted the practice of filling the column above the normal operating maximum during start-up to avoid difficulties if the minimum level was reached during the fluctuating conditions until stability was established. On the day of the accident the operators did not realise how full the column became and had no instruments to warn them or trip system to prevent overflow.

A similar situation occurred at the Pembroke Cracker in 1994 (HSE 1997) when a blocked outlet in the debutaniser column caused an accumulation of liquid. It was not

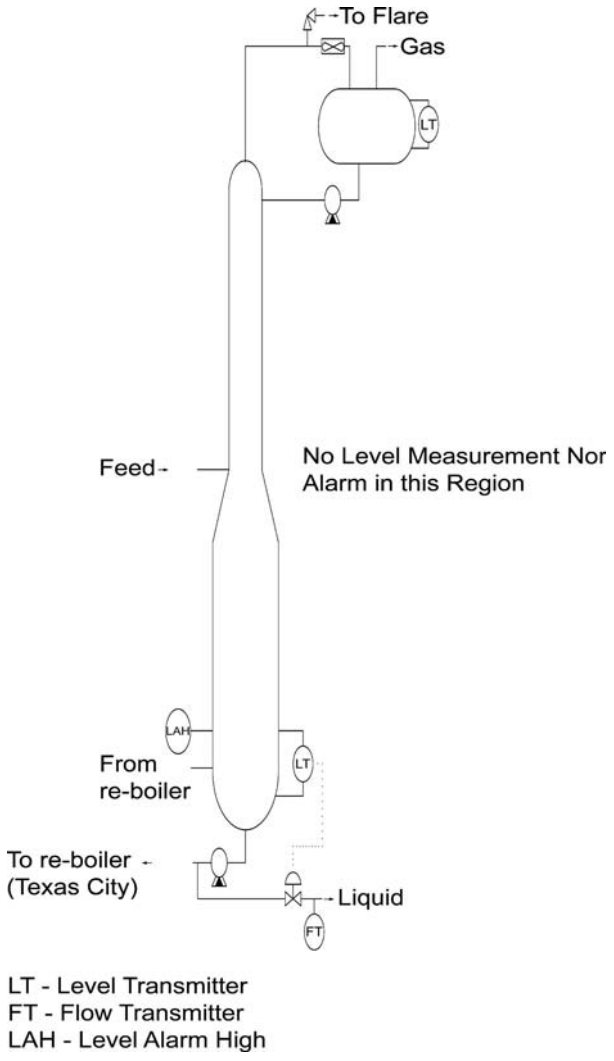

Figure 2. Typical arrangement of Process Vessel/Column – Splitter or Fractionation.

possible for the operators to ascertain the liquid level as this was not directly recorded and no high level alarm was in place although all the columns in the fractionation unit were operated on level control they only operated over the normal level range.

Also, in the same incident at Pembroke when the process fluids were vented to flare, liquid was knocked out as intended, in the flare knock-out drum. (Figure 3 shows the salient features of the knock-out drum.) But as the cracker unit was operating in an unusual condition (following trips of fans and pumps in the fractionation section and shut down of other units on the refinery), the liquids were lighter than expected. Therefore instruments measuring level using pressure gave erroneous liquid levels. Although operators checked the sight glass level gauge they could not establish the actual level because the level was outside the range covered by the sight glass and no interface could be seen. As a result the operators assumed (wrongly) that the level was low and falling and the compressor could be restarted to assist in the removal of liquids accumulating elsewhere by re-establishing the correct flows through the fractionation unit. In addition the high level in the knock-out drum should have resulted in the manual activation of the rapid dumping of liquid to a slops tank. When the plant was rebuilt a high reliability automatically activated rapid dumping system was installed.

COMMON THEMES

The methods employed by the operators for overcoming practical problems did not follow the procedures envisaged by the designers of instruments and alarm/trip systems and possibly by any HAZOP studies. The designs had furnished measurement and control either side of the normal operating conditions but had not foreseen the need to provide additional information on level or alarms/trips when the liquid accumulations would lead to carry-over. Where there is a large gap between the normal operating range and these unacceptable levels the operators may be aware of the "extra capacity" that they can use for convenience and which would not result in an incident unless they fail to track the situation and so grossly overfill a vessel. Clearly at Texas City operators were distracted or several operators became involved. At Pembroke the operators did not monitor liquid accumulation as there was a false positive outflow being recorded. If instrumentation was provided then the startup procedure could include resetting the set-point/high-level/high-high level alarms and trips. But the management of change procedure is often so laborious that this is impractical. The ability for a supervisor to make short term changes to instrument settings and then to restore them to normal value, would make it practical to make temporary changes – but would need to be documented, passed from shift to shift, and monitored to ensure that the normal operational settings were restored as soon as possible. As well as keeping the alarms operative, it might emphasise to operators that they are working in abnormal conditions. Obviously designers could consider this option and its practicality should be discussed with operations representatives.

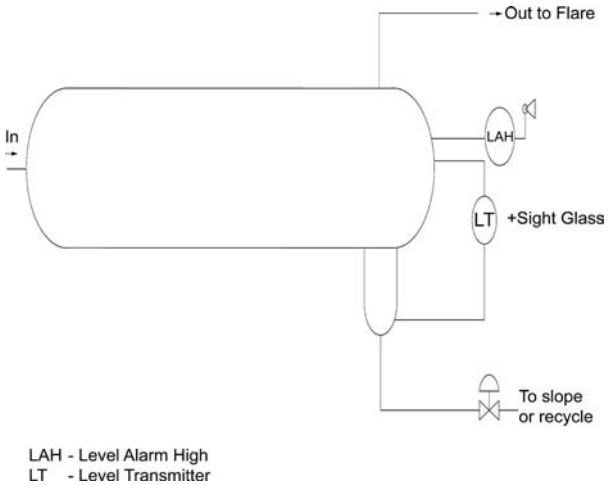

Figure 3. Flare Knock-Out Drum.

In other cases (e.g. Buncefield) operators failed to monitor instruments continuously recording levels so that progress in filling tanks could be followed and the time to fill the vessel estimated. Rather reliance has been placed on alarms/trips which are designed as layers of protection against the operator's failure to take appropriate action. Thus the levels of protection are eroded and a failure of the alarm/trip system will lead to overfill.

In some cases the level may be deduced by the instrument system indirectly via measurement of pressure (often misleadingly described as liquid head) and an assumption on normal density. Clearly in these cases overfill can occur when lighter than normal liquids are present and if there is no alarm to alert the operators or trip to initiate shut-down. Note that liquids arising from process blow down will often be lighter than normal process streams because additional liquids will condense at the lower temperatures arising from the Joule-Thompson effect. These lighter fluids may also contribute to greater liquid accumulation in overhead reflux drums.

POTENTIAL FOR IMPROVEMENTS

There are several approaches to review of the process plant and its safe operation which may be considered to identify whether the causes discussed above could arise again and whether mitigation could be provided:

- HAZOP – this is often considered to be hardware oriented and applied at various stages during design. It could therefore, capture and avoid some of the problems before hazardous materials are introduced. However HAZOP examinations may become too mechanical and when considering "Level – MORE THAN" for example may see the operational level – high level alarm and considering the headspace before a column

may be regarded as flooded think that there is adequate time for an operator response, without realising that there may be intentional overfill at start-up, for example. Startup and shutdown are often reviewed in HAZOP but the team may not explicitly consider the need for process conditions outside the range of normal operating settings of instruments. This is where the input of experienced operators is vital.

Other deviations may be relevant – for example "Composition – OTHER" which should identify any issues over lower density fluids but a HAZOP team may not always examine how instruments are being used to measure level and that deviations on level and composition may be related.

- Various forms of risk assessment, which may consider specific scenarios or a set of generic failure cases. In either case the frequency of challenges to the safety systems is assessed together with the scale of potential consequences so that the need for risk reduction measures determined. These measures may be specified in terms of levels of protection, or more recently in terms of the SIL (Safety Integrity Level) Classification as defined in IEC61511. However the assessments of the effectiveness of safety measures makes assumptions about how they will be used, the number of challenges (demands) on them and the frequency of testing and/or maintenance.
- Human Factors Assessments – will often be focussed on issues of layout and adequacy of resources, skills, experience, awareness, supervision and technical support. This latter group of issues has been addressed in methods such as the Entec Staffing Assessment (Energy Institute 2004) which considers whether the operators and their support are adequate for dealing with abnormal situations, particularly those which might lead to process accidents. The support considered will include information supplied by the instruments and control systems and the actions that these will perform for the operators (including remotely operated valves and automatic shut down mechanisms). The method includes physical assessment of scenarios where a team, including operators discuss the development and control of abnormal, high workload situations. The teams are encouraged to discuss how they identify problems, diagnose the causes and then how they would bring them under control. These scenario assessments can be used to determine whether the instruments are providing the operators with adequate information and also examine whether the operators can suffer distractions which prevent them monitoring or controlling the evolving scenario. Ultimately there may be a need to invoke the emergency shut-down system and this has to be considered in the context of whether it would operate in time for the scenario to be brought to a safe conclusion. A very important consideration is the culture of the operating teams and whether they would be "willing to initiate a shutdown," if necessary without reference to higher authority.

This type of scenario assessment can be performed outside the staffing assessment method and will serve as identification of any misunderstandings of how level measurements and alarm/trips are designed to work as well as identifying where additional information or instruments may be required. However, it is not the intention of this paper to add to the number of alarms provided on a plant but rather that safety alarms be identified separately as such and level alarms/trips set where they will act as safeguards and not as a normal operating level which may not be relevant for start-up, for example.

CONCLUSIONS

Several high profile major accidents have occurred due to high liquid levels not being recognised by operators. There are several reasons why operators may fail to recognise or act on high liquid levels, these include:

- Inaccurate measurements of level where the instrument relies on an assumed density;
- The high level has not been covered by the instrumentation scheme, which assumes normal operating conditions and that procedures will be strictly followed;
- Operators have come to rely upon alarms or trips which are intended to be used as back-up safety devices;
- Operators are distracted and not available to respond when a critical level is reached.

Therefore the designers need to have a more practical approach to how the system may be challenged and allow for deviations outside the normal operating conditions, particularly in situations where operators will be aware there is considerable additional head space that can be utilised before dangers can arise. Also operators need to be aware of how instruments are measuring level and whether they rely on parameters that can vary, such as density. They should also be aware of where the instruments can only give information over a restricted range.

Rather than wait for accidents to occur the actions of operators in response to difficulties during unusual operating conditions, either during the physical, scenarios examination in staffing assessments or by separate desktop, talk through or walk through workshops to identify how deviations from standard, defined operating procedures may lead to dangerous situations such as overfill, or flooding. Simulators may have an important role to play, particularly if they can be used to show the effects of instrument malfunctions on the operators' perception of plant status.

In this way it is hoped that potential sequences leading to accidents can be anticipated, and barriers introduced so that lessons may be learned without having accidents.

ACKNOWLEDGEMENTS

The author would like to thank the referees and colleagues who have made helpful suggestions to improve this paper. However the observations and opinions are the author's

own and do not necessarily reflect the views of Entec UK or any of its Clients.

REFERENCES

Energy Institute, 2004, Safe staffing arrangements – user guide for CRR348/2001 methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated plant and/or equipment.

Hailwood, M., 2009, Lessons from Buncefield in Loss Prevention Bulletin 206.

Health and Safety Executive, 1997, 'The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994: A report of the investigation by the Health and Safety Executive into the explosion and fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 July 1994', ISBN 0 7176 1413 1.

Kletz, T. A., 2001, An Engineer's View of Human Error 3rd ed IChemE, ISBN 0-85295-430-1.

Mogford J., December 9th 2005, Isomerization Unit Explosion March 23, 2005 Final Report Texas City, Texas, USA.

Newton, Lord, Drysdale, D., Baxter, P., Powell, T., Leinster. P. and Ashton D., 2008, The Buncefield Incident 11 December 2005. The final report of the Major Incident Investigation Board ISBN 978-0-7176-6270-8.