

Recurring accidents: *overfilling vessels*

Steve & Sara Emvlick



Peter Waite examines the lessons we should be learning

MUCH work has been done, and many words written, on the subject of repeated accidents. The questions that arise time and again are 'why do they recur?' and 'how can they be stopped?'

The aim of this article, the second in a series on repeated accidents, is to revisit the safety lessons we should have learned and offer practical guidance on how these can be shared interactively between management, supervisors and those directly involved in the job or process – in this case particularly the designers – in a bid to stop similar accidents in the future.

overfilling vessels

What are the consequences of overfilling vessels with dangerous liquids? Such incidents have the potential to cause major accidents wherever significant quantities of hazardous liquids may be present, including food processing (solvents) and drinks (ethanol) as well as chemicals, oil and

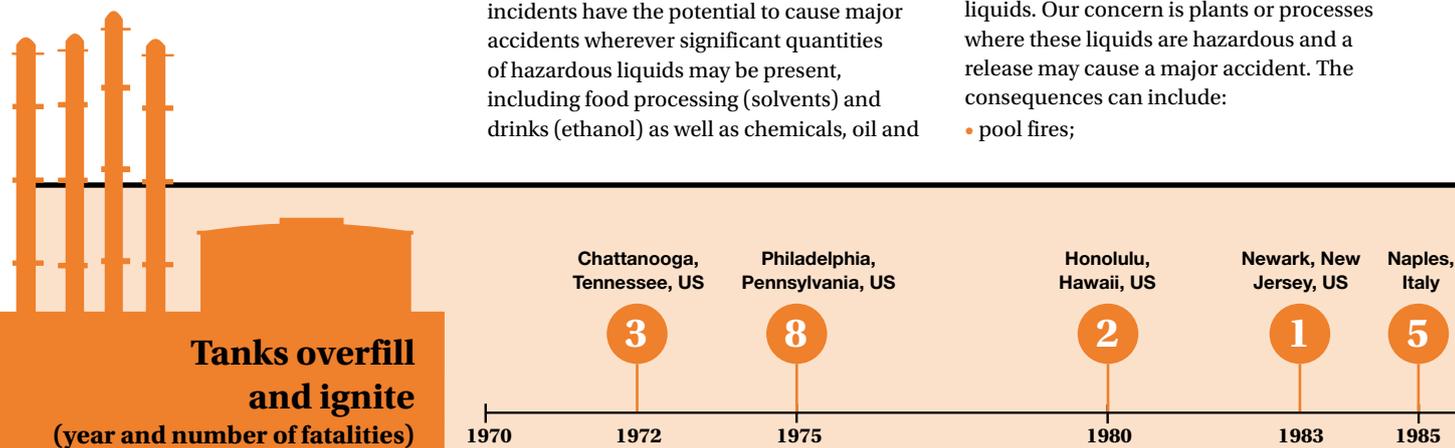
gas. The types of accident that arise due to overfilling vary widely:

- overfilled drums – immediate spillage from drums in filling area, or drums bursting during storage or transportation due to expansion of the liquid or insufficient ullage space;
- overfilled storage tanks – liquid is released through vents intended for vapour (see Accident 1) or the pressure becomes too much and the tank fails; or
- vessels intended to separate gases from liquids are overfilled and the liquid enters the outlets designed for the gas phase.

consequences of overfilling vessels

The range of scenarios shows that overfilling can occur in almost any process involving liquids. Our concern is plants or processes where these liquids are hazardous and a release may cause a major accident. The consequences can include:

- pool fires;



operator error

In a review of incidents, researchers found that 29 out of 242 storage tank accidents involved operator error, and 15 of these were overfilling. These accidents were the most serious as in most cases ignition was unavoidable; 13 of the 15 led to fires and explosions.

DOI: 10.1016/j.jlp.2005.05.015



- flash fires (flammable vapour from either vapourising pools or liquefied gas releases are ignited);
- vapour cloud explosions (as happened at Buncefield¹);
- toxic vapour clouds (either the released material is toxic or its products of combustion are); and
- uncontrolled liquid spills that are dangerous to the environment, contaminating soil, ground or surface waters, and harming life. The consequences of simply overfilling a vessel are varied and tragic.

the legal section

Many countries have laws to prevent injury to workers, public and environment. In the UK the Health & Safety at Work etc Act 1974² is the primary legislation under which specific regulations are made which apply to all work places, such as Management of Health and Safety at Work Regulations, 1994³; Control of Substances Hazardous to Health Regulations 2002⁴; and Dangerous Substances and Explosive Atmospheres Regulations (2002)⁵.

For installations such as refineries, process plants and storage, the Control of Major Accident Hazards Regulations 1999⁶ (COMAH – Seveso 2 throughout Europe and shortly to be revised as Seveso 3) are the most onerous safety regulations. COMAH requires the identification of all major accident scenarios, including overfilling and demonstration that “all measures necessary” have been taken to prevent major accidents and mitigate the consequences of any that do occur.

Other jurisdictions have similar requirements. Guidance on prevention and mitigation, produced following Buncefield,

(2005) would be regarded as the minimum required. Recommendations from Texas City (2005) focus on other issues but overfilling was an immediate cause of the accident.

avoiding overfilling vessels

current issues

Recent efforts have concentrated on measures to reduce the consequences of overfill, such as the use of tertiary containment rather than preventing overspill by providing timely information to operators.

The accident at the Buncefield storage depot, UK (see Accident 2) led to emphasis on technical measures to improve the reliability of high level detection, alarms and trips together with remotely operated or automatic shut-off valves^{6,7}. Further recommendations have concentrated on mitigating the consequences of overfill using tertiary containment, and greater separation of vulnerable facilities.

There are striking similarities between tank overfilling incidents such as those at storage sites in Buncefield and Newark and accidents that have occurred at refineries and petrochemical facilities. For example, the explosions at the Pembroke refinery in 1994 (see Accident 3) and Texas City in 2005 (see Accident 4) shared common features related to the human factor angle of workers interacting with instrumentation despite the installed safety, instrumentation and control systems. Recommendations from the investigations at Texas City and Buncefield recognised the need for better process safety leadership but there is also a need for designers to recognise the needs of operators.

Texas City and Pembroke had flooded columns while Pembroke also had excess liquid in knock-out drums. At Texas City a column had been deliberately overfilled above normal operating levels (to make start-up easier). At Pembroke, operators failed to detect a blocked outlet. Knock-out drums had been overfilled due to a combination of inadequate/unavailable liquid removal capacity (as also occurred during the *Piper Alpha* incident in 1988), or failure to switch to rapid liquid removal. Level detection covering the full range of possible levels (not just normal operation conditions) could have made

accident 1: 1983

Newark, New Jersey, US: a gasoline tank overfills

A storage tank was receiving a planned shipment by pipeline but in order to accommodate the delivery, some of the existing product had to be transferred to another tank. This transfer did not take place in time.

The operators failed to gauge and monitor the tank according to procedures and arrived to discover it was overflowing. 1,300 bbl of gasoline spilled into the tank dike. A slight wind (1–5 mph) carried the developing vapour cloud about 1,000 ft to a drum reconditioning plant where it was ignited by an incinerator.

The resulting explosion killed one man, injured 23 others, and caused US\$10m of damage to the terminal and up to US\$25m in legal claims for damage to rail rolling stock and adjacent properties. Although dikes contained the burning spill, two adjoining internal floating roof tanks and a smaller transmix tank ignited and eventually were destroyed along with 120,000 bbl of product.





Royal Chiltern Air Support Unit

accident 2: 2005

Buncefield, UK: a gasoline tank overfills

Operators failed to realise that the tank was overflowing because there was inadequate level monitoring as the tank filled and the system to detect a high level and shut-off the inflow before overflow occurred was defective.

More than 250,000 l of gasoline spilled from an atmospheric pressure storage tank. It was equipped with a bund to contain the liquids but this did not stop a vapour cloud from forming, escaping and igniting.

The pipeline was delivering to two tanks at the beginning of the transfer operation, but when the delivery to one tank was complete the rate of filling to the other was roughly doubled. The level monitoring instrument malfunctioned and gave the operators misleading information. They did not recognise the implication of this or were not aware of the increased filling rate. The independent high level switch had been set up incorrectly and was not functioning; it should have signalled a remotely-operated shutoff valve to close. As a result, there were now no barriers remaining to prevent the overflow occurring. The local operators did not have direct control over all the pipelines feeding the site so were unable to plan receipts and check volumes of available storage in advance. There was no independent high-level alarm which could have activated before the overflow occurred. There was no means for the operators to monitor the volume of liquid in the tank after the single level monitor failed and no opportunity to calculate the expected time when the tank would be full. A high-level alarm should have been available to give sufficient warning to the operators so that inflow could be stopped in a controlled manner.

The vapour cloud exploded with a force measuring 2.4 on the Richter scale and was heard as far away as continental Europe. Fortunately, it was a weekend so the site was largely empty and no one died. Forty-three people were injured, houses and local businesses were destroyed, and the groundwater was polluted.

the outlet valve was closed. Designers should consider whether level instrumentation is adequate and how operators will manage levels in practice.

In other cases (Buncefield) operators failed to monitor increasing levels and did not estimate when the tank would be full. They relied on alarms and trips which were the final layers of protection to backup level monitoring. Thus levels of protection were eroded and a single failure of the alarm/trip system led to overflow.

In some cases the level is deduced from pressure (or mass), sometimes misleadingly called liquid head, and assumed constant density. If overflow occurs with lighter than normal liquids (eg during blow-down - Pembroke) then these measurements cannot be trusted and are dangerous.

Operators form a mental model of the process. When faced with conflicting indications between accurate and misleading instruments they will accept readings that reinforce their preconceptions that levels are within safe limits.

potential for improvements

There are several approaches which may identify whether the causes discussed above could arise and whether protection is needed:

- **HAZOP** -when considering 'Level - more than' examine the difference between normal maximum and overflow level. Will operators seek to use this volume during start-up?

Also consider other deviations - for example 'Composition - other' which should identify issues over lower density fluids.

- **Risk assessment using LOPA and SIL, to consider specific scenarios or a set of generic failure cases** - the scale of potential consequences together with the frequency of challenges to the safety systems is used to determine the need for risk reduction measures. These are specified as the number of independent protection measures, or the SIL (safety integrity level) classification (IEC61511). The assessment of the effectiveness of the safety measures makes assumptions about operator response, the number of demands and the frequency of testing.

- **Human factors assessments** - used to focus on equipment layout but over the last 15 years has been extended to consider the adequacy of resources, skills, experience, awareness, supervision and technical support. The latter issues are covered in the Entec Staffing Assessment (Energy Institute) which considers whether the operators and their support are adequate for dealing with precursors to process accidents. This also considers the instruments and control systems supporting the operators including remotely-operated valves and automatic

Operators form a mental model of the process. When faced with conflicting indications between accurate and misleading instruments they will accept readings that reinforce their preconceptions that levels are within safe limits.



operators aware of the developing danger and helped to avoid these disasters.

common themes

At Texas City the operators did not follow formal procedures. It became accepted practice to utilise the capacity above normal operating level, but left operators with no means of monitoring when a release was inevitable.

At Pembroke the operators did not recognise liquid accumulation as there was a false positive outflow being recorded; the level instruments were not clear and a flow meter on the liquid outflow from the fractionation unit gave a credible outflow rate even though

Wrexham, UK, 2001

A process feedstock tank overfilled, spilling 13.8 t of toxic liquid phenol into a bunded area. The phenol solidified and low ambient temperatures and had to be chiselled out by staff wearing full personal protective equipment. The cost of material losses, cleanup and lost production amounted to £39,800.



shutdown mechanisms. The method encourages discussion of how operators identify problems, diagnose the causes and then recover the situation. Scenario assessments are used to determine whether instruments provide operators with adequate information. An important consideration is whether operators are "willing to initiate a shutdown," when necessary.

Parts of the assessment can be performed separately and could identify problems with level measurements and initiation of the alarm/trips as well as the need for additional information or instruments. However, additional alarms are not encouraged but safety alarms should be identified separately as such distinguished from normal operating level controls (which may be bypassed during startup).

so why do accidents recur?

Safety guru Trevor Kletz has examined this subject in detail and provides a number of reasons. Principal amongst these, to which I've added some comments of my own, are:

- organisations fail to record and circulate the lessons learned from past accidents, and fail to encourage a search for past relevant accidents either for design purposes or for operator training;
- experience and skills are lost when staffing is reduced, long-term employees retain memories of abnormal plant behaviour, near misses and, most importantly, why modifications were made;
- hazards are not reassessed often enough. What was safe in the past is not necessarily safe now. Plant modifications may have affected the plant capacity to handle excursions safely;
- supervisors are overloaded. They are the interface between management and workforce, ensuring that work flows smoothly. They should not be distracted with unnecessary tasks and detail, diverting attention away from safety;
- change of design can lead to fatal conditions. There should be a formal system for assessment of proposed changes to plant and they should only be implemented after they have met the appropriate criteria. This should

accident 3: 1994

Pembroke refinery, UK: a column is overfilled

A blocked outlet in the debutaniser column led to an accumulation of liquid. It was not possible for the operators to see the actual liquid level either by sight glass or using instruments as they measured the levels indirectly using pressure. There was no high-level alarm in place above the normal maximum operating levels. Liquid accumulated in a compressor suction knock-out drum where the high levels of liquid tripped the compressor. As the debutaniser outlet flow meter was recording a false positive the supervisor believed the suction drum could be drained back to the process using an unauthorised temporary connection and the compressor could then be restarted.

Also, when process fluids vented to flare, liquid was collected in the flare knock-out drum. But as the cracker unit was operating in an unusual condition, the liquids were lighter than expected. Therefore instruments using pressure to measure levels gave erroneous readings. Operators could not establish the actual level because it was outside the range covered by the sight glass. So operators wrongly assumed that the level was low and falling and the compressor could be restarted to remove liquid accumulations elsewhere. Shortly after the compressor was re-started the suction drum level again tripped the compressor and vented the process to flare, resulting in liquid filling the flare drum and slugs entered and ruptured the flare line.

The initial high level in the knock-out drum should have resulted in the manual activation of rapid liquid dumping to a slops tank. This procedure was introduced following a modification to reduce waste and emissions, however this change did not go through a full management of change process, being beneath the cost threshold at the time. The modification and necessary change in procedures had not been formally communicated. Some 20 t of hydrocarbons escaped and exploded, killing no-one but injuring 26.

Following the accident, a highly reliable automatic system to remove liquid was installed.

be enforced for field modifications; and

- taking short cuts is a readily recognisable human behaviour but will result in unsafe working.

easy steps to help avoid repetitions

To prevent repetitions, consider the following:

- describe accidents in safety bulletins, emphasising reasons why they happened;
- follow up accident recommendations to ensure that they have been put into effect;
- never change a procedure until the reason for it is fully approved and understood;
- learn from accidents in other organisations, particularly those with similar processes;
- emphasise the importance of risk assessments and make sure that they are carried out;
- put this into effective practice using techniques such as safety information notes and emails; committee meetings; on- and off-the-job training courses; formal apprenticeships; computerised learning modules; and toolbox talks. Designers should be included in these communications.

the design and simulation challenge

Several high-profile major accidents have occurred due to high liquid levels not being



Organisations fail to record and circulate the lessons learned from past accidents, and fail to encourage a search for past relevant accidents either for design purposes or for operator training.

Naples, Italy, 1985

During a filling operation, fuel overflowed through the roof of a tank for almost 90 minutes. An estimated 700 t of fuel escaped into the secondary containment.

The pool of liquid covered the bund area of the tank and the adjacent pumping area, which was connected through a drain duct. A vapour cloud formed rapidly and ignited. The explosion killed five, injured 170 and destroyed 24 tanks and the main fire-fighting control centre. The fire lasted for seven days.



recognised by operators during safety critical operations. There are several reasons why operators may fail to recognise or act on high liquid levels, including inaccurate measurements of level; a high level not detected because instruments are designed to manage normal operating conditions; operators relying upon alarms or trips which are intended to be used as backup safety devices; and operators are distracted and not available to respond when a critical level is reached.

Therefore designers need to have a more practical approach to design of instruments and controls allowing for how the system may be challenged; in particular for deviations outside the normal operating conditions. Also operators need to be aware of how instruments are measuring levels 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.

Evaluation of scenarios such as perturbations at startup, or utility system failures can give a clear understanding of how operators will respond. Desktop or talk-/walk-through workshops can identify how deviations from standard, defined operating procedures may lead to dangerous situations such as overflow, 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 based on the experience of operations as well as past accidents. **tce**

Peter Waite (peter@astriduk.co.uk) is an independent safety consultant with over

accident 4: 2005

Texas City refinery, US: a column is overfilled

During startup of the isomerisation unit an explosion and fire occurred which killed 15 people and injured 170.

It began when a night shift operator brought in cold feed to the splitter; the level indicator's high-level alarm activated and remained on until after the incident, 11 hours later. The redundant hard-wired high-level alarm did not operate. The indicated level continued to rise. The feed to the splitter was closed to leave the remainder of the startup to the day shift. The night shift did not report the faulty hard-wired high level alarm.

The day shift recommenced feed, the level transmitter (designed to operate with a liquid gas interface) was fully submerged and displayed a signal slowly drifting downwards to 80% before any liquid was removed. While the startup procedure specified the level control should be set at 50% (in automatic mode), it was in manual.

With a higher-than-specified level in the column to begin with, operating out of the control range, an additional 2,500 bbl was added with no outflow. The liquid reached 137 ft vs normal operating level of 6–7 ft. Under these circumstances the high bottoms temperature caused vapourisation at the bottom of the tower, lifting the liquid level higher, but lower than the overhead line at the top of the tower. The cold liquid higher up the tower quenched these vapours and prevented them from distilling overhead. Two witnesses saw vapours and liquid emerging approximately 20 ft above the top of the stack "like a geyser" and running down and pooling around the base of the blowdown drum and stack.

The release ignited, possibly on an (unauthorised) vehicle exhaust and the resultant fire and explosion resulted in 15 fatalities and over 170 injuries to those in and around the temporary offices (trailers) on the adjacent unit.

30 years' experience of major accident risk assessments and investigations; formerly of Cremer & Warner/Entec, he is now also head of risk services at Altor Risk Group

further reading

1. www.buncefieldinvestigation.gov.uk/
2. Health and Safety at Work etc Act 1974 (1974 c 37)
3. Management of health and safety at work. Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and guidance L21 (Second edition) HSE Books 2000 ISBN 978 0 7176 2488 1
4. The Control of Substances Hazardous to Health Regulations 2002 (as amended) Approved Code of Practice and guidance L5 (Fifth Edition 2008)
5. Dangerous substances and explosive atmospheres Regulations 2002. Approved Code of Practice and guidance L138 HSE Books 2003 ISBN 978 0 7176 2203 0
6. *Overflow protection for storage tanks in petroleum facilities* API RP 2350 (Third edition) American Petroleum Institute 2005
7. *Recommendations on the design and operation of fuel storage sites*, HSE 2007 www.buncefieldinvestigation.gov.uk
8. Hailwood, M, 'Lessons from Buncefield', *Loss Prevention Bulletin* 206

Free to share

IN the spirit of this series, you are permitted to print, photocopy and redistribute this article as many times as you like. Feel free to share it with your boss, colleagues and reports.

Together we can help to reduce the number of workplace accidents.

