



The Buncefield Incident – 7 Years on: Could It Happen Again?

Colin Howard

istech Consulting Ltd, Middlesbrough, UK
istech@colizhoward.plus.com

A trip will fail to operate; a tank will be overfilled.

T.A. Kletz¹

Most discoveries are made regularly every 15 years.

George Bernard Shaw

- Fault reporting and escalation;
- Appropriate procedure content;
- Effective proof testing;
- Contractor/supplier management;
- System documentation;
- Safety critical systems identification;
- Risk assessment;
- Leadership;
- Competences.

response to changes in the liquid level. The technology of the servo type of tank-level measurement is long established, but it does need careful maintenance to ensure that it remains serviceable and gives reliable measurements. The instrument involved incorporated meshed gear trains and bearings, which can lead to stiff or erratic operation if incorrectly aligned or worn. The wire that connects the displacer and the measuring head can fail to wind correctly onto the measuring drum.

Tank 912 had been brought back into service after maintenance little more than 3 months prior to 11 December 2005. In the period up to the incident, there were at least 14 (and possibly up to 19) occasions when the level gauge was observed to have stuck at some point ('flatlined') while the tank was being filled or emptied. There was no particular pattern or apparent cause for this sticking. On many occasions, the operating team performed a 'stow' operation on the level transmitter, causing the displacer to be raised to the top position and then returned to the liquid surface. This usually resulted in the measurement becoming live again. Service engineers from the contractor were called out on four occasions under their service contract to attend to sticking gauge head. The visit reports included references to stiffness in the main gear/idler gear train that was adjusted and to a need to change the main drum bearings, but this was not actioned. No definitive cause for the 'flatlining' was

I. Introduction

Are we nearly halfway to the next major incident after Buncefield? But then, there have been other explosions and fires overseas since Buncefield, including Silver Eagle, Utah (2009), Puerto Rico (2009), Jaipur (2009), Macondo/Deep Horizon (2010), and Venezuela (2012).

The explosion and fire at the Buncefield fuel terminal on 11 December 2005 was the result of a sequence of events and activities that had taken place in the days, weeks, months, and years prior to the incident. The primary causes were the failure of two-level instruments on the tank that overflowed; the alarm and overfill protection functions did not operate as a result. Allied to these technical failures was inadequate and poor presentation of information about the status of the plant that prevented diagnosis and recognition that a problem existed.

Underlying these technical failures was a series of failures of management to effectively address over a long time a wide range of issues including the following:

- Design and maintenance;
- Management of change;

These failures were not confined to the operator of the terminal but extended across the supply chain involved: the 'site operator', the tank-level equipment 'contractor', and the independent high-level switch 'manufacturer'. This paper outlines how some of the technical and management failures were linked so that the incident could develop. It is vital for the future that the lessons highlighted in this paper and the official reports are fully learnt and the corrective action is embedded in all organisations associated with high hazard or safety critical operations, not just those responsible for the supply and distribution of fuels.

Many of the topics included in this paper may appear individually quite small, but taken together, they demonstrate how management failures can be critical to the continued safe operation of a high-hazard process.

II. Automatic Tank Gauging Level Gauge Failure

The Automatic Tank Gauging (ATG) level gauge head was a servo-assisted device where a displacer sitting on the surface of the liquid is raised or lowered in

The Buncefield Incident – 7 Years on: Could It Happen Again?

identified, and as the gauge was working on the engineer's departure, he appeared to have resolved the problems. However, as the sticking continued after each visit, there was an underlying systematic fault with the gauge that had not been identified and addressed. No consideration appears to have been given to replacing the servo head on tank 912 with a new replacement one set up in the contractor's factory.

The records of 'flatlining' have come from shift logs and the service reports plus an analysis of the ATG records. There was no evidence of an effective fault logging system in the control room, or means to escalate a persistent problem to a more senior level at the site operator or with the ATG contractor. There was no system with the contractor where repeated faults on a specific instrument could be readily identified. A visit by more senior contractor's staff at the end of November to discuss tank dip and gauge differences, including tank 912, was a missed opportunity to investigate the continuing 'flatlining' issues.

The inability to identify the root causes of the 'flatlining', and to carry out an effective repair was an indication of a serious deficiency by both the site operator and the ATG contractor in the management systems and procedures for maintenance of the gauge.

There was a 'movement' functionality installed on the ATG where the operator

could input the intended movement for a tank, and the system monitored the actual direction of movement of the tank level with facility for a discrepancy alarm. From the data obtained as part of the investigation, it appears that the movements page was not set up correctly for tank 912 on 10 and 11 December 2005, and that the operators had not been using the movement functionality as it should have been used.

III. Independent High-Level Switch Failure

When the tanks added to the Buncefield terminal in the early 1980s (including tank 912) were built, they were fitted with a non-checkable independent high-level switch, based on a sealed reed switch as the detector operated by a magnet in a carrier connected by a wire to a level-sensing element consisting of either a float or displacer (for a liquid) or a weight (for an internal floating roof). These switches were later modified onsite by the addition of a pull cord (see *Figure 3* later in the paper) to enable the magnet carrier to be pulled upwards to test the operation of the reed switch.

In 1987, TAV Engineering Ltd (TAV) produced their first range of checkable switches (*Figure 1(a)*). At the time, this was a good concept for high-level protection, with an in-built test mechanism, but it could not test for a sunken floating roof or a damaged float or displacer if this sensing option was

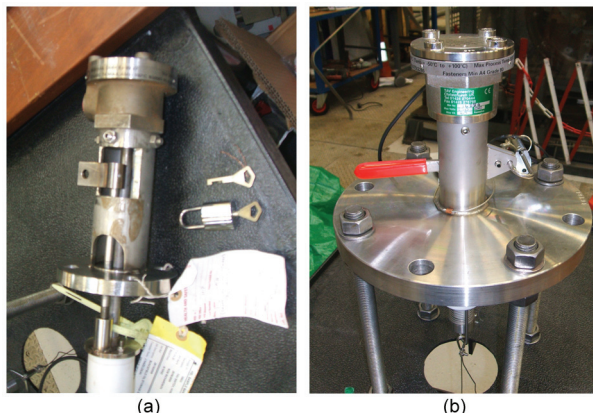
fitted. The in-tank-sensing method was broadly unchanged.

To operate the checking feature, the switches were fitted with a small plate forming a handle that could be rotated by 90° out of a rebate or detent in the switch's upstand and lifted to test the high-level switch function within the device. (Where a separate reed switch was fitted for a low-level application, the plate could be lowered to test the low-level function.) The small plate used to test the switch was provided with a padlock to lock it in its 'home' position within the rebate when the switch was in normal use; the hole was large enough to take a standard 'lock-out tag-out' padlock. As long as the plate was returned to sit in the rebate, the padlock provided additional security; it would have been difficult for the plate to have rotated out of the rebate and then moved up or down on its own. The design also provided for different cut outs in the upstand depending on whether the application was for activation on high or low level. *Figure 1(a)* shows a switch designed for a high-level application.

In 1996, TAV developed a modified design of the check mechanism by providing a larger, more easily accessible, lever mechanism (*Figure 1(b)*). A driver for this was to reduce the number of parts required and to simplify the manufacturing process. This lever was also to be locked in its normal operating position with a padlock, which could be removed to test the switch, by raising or lowering the lever, in a similar manner to that described above. This switch, however, differed from the original design in that the lever did not rest within a rebate in the upstand and was held in its normal, horizontal, operating position, at right angles to the main body of the switch, solely by use of the padlock. If the padlock was not fitted, then the lever would be readily pulled into the downward position by the effect of gravity and the attached weight of the sensing mechanism.

The fitting of, and the make and hasp size of, the padlock was critical to the correct functioning of the switch in normal operation. This essential

Figure 1. TAV checkable switch comparison: (a) original and (b) new



The Buncefield Incident – 7 Years on: Could It Happen Again?

requirement was not, however, made explicitly clear in any of the manufacturer's documentation where the padlock continued to be referred to as being for 'security' purposes. Many users interpreted this as an anti-tamper feature, and considering their installation to be on a secure site, did not fit the padlock until advised to do so in the aftermath of the Buncefield incident.

The operating and maintenance instructions available for the switches included the following instructions for the 'operation of the check facility':

- a. Unlock the padlock and remove, the check lever will now be free to move vertically.
- b. Empty tank condition. Raise the check lever, thereby lifting the magnet carrier upwards; this will allow the switch to change condition.
- c. Ensure the check lever is put back into the operating position and is relocked.
- d. Full tank condition. Push the check lever down, thereby lowering the magnet carrier downwards; this will allow the switch to change condition.
- e. Ensure that the check lever is put back into the operating position and is relocked.

Despite a direct instruction to relock the check lever, there is no indication of the padlock's safety critical function. The manufacturer had carried out a number of studies to verify that the functionality of the modified checkable switch range had not changed from the original intent, but crucially, they did not do a full failure mode and effect analysis (FMEA) study and consider what would happen if the padlock was not fitted or the switch was maloperated.

Following the Buncefield investigation, the manufacturer has fitted a pin through the upstand to prevent the lever falling down, even if the padlock is not fitted.

The new switches fitted in 2004 were specified with single pole double throw (SPDT) rather than the single pole single throw (SPST) contact arrangement in the original switches. The impact of this very

simple change on the ultimate failure to operate of the switch on tank 912 was not foreseen.

It only emerged during the investigation that there was a fundamental difference in the way a SPST contact arrangement was set up when compared with a SPDT arrangement; there was nothing in the published documentation to highlight the difference. In the SPST arrangement, the magnet is directly over the reed switch, holding the contacts closed, when the level is in a normal position, and only moves away if the level switch is called upon to operate, thereby opening the contacts. The manufacturer had specifically intended this arrangement to be the one that would be used for high- or low-level alarm functions; each switch would be set up specifically for a particular service and would not be interchangeable. Raising or lowering the test lever with this configuration would generate an alarm. With the SPDT arrangement, the magnet is below the reed switch when the level is in a normal position and moves to cover the reed switch if the level switch is called upon to operate, thereby causing the contacts to change over. This provides a more flexible arrangement than the SPST configuration; the appropriate connections have to be selected when the switch is installed. This was a feature that the manufacturer considered inadvisable for the alarm function switches because of the possibility for error; it was intended for systems such as pump start applications. When the lever is raised, the magnet moves over the reed switch simulating a high level, and the contacts change over, but if the lever is left in the lowered position, the magnet carrier can never rise to cover the reed switch on rising level as the movement is restricted by internal stops (common to all the types of switch).

Enquiries during the investigation elicited a commonly held view that ran something like this

level switches are simple devices and the knowledge built up by experience is generally enough to specify and use

them without recourse to manufacturers' information, which in any case was either difficult to obtain or doesn't provide any more useful detail.

Clearly, this is not correct.

There had been neither an effective management of change process nor a thorough design review and delivery of essential manufacturer's documentation to the end users.

IV. Monitoring and Control Arrangements

The original Buncefield terminal was extended in the early 1980s by the addition of the area that included tank 912 and in the early 1990s by the termination of the FINAline pipeline from the refinery on the Humber. Until the mid-1990s, the British Pipelines Agency (BPA) facilities and the area that became the Hertfordshire Oil Storage Ltd (HOSL) facility were operated together by BPA staff. The operations team had oversight of the terminal areas, the FINAline pipeline and the United Kingdom Oil Pipelines (UKOP), and importantly, controlled the offtakes from the UKOP network. From the mid-1990s, the BPA and HOSL operations were separated, and the staff operating the HOSL facility no longer had direct oversight of what was happening on the UKOP network. Communication about operations on the UKOP network was henceforth by telephone, fax, and e-mail. Crucially, there were no facilities provided for HOSL to directly monitor the flowrate from either UKOP into the HOSL facility nor was there a hardwired emergency stop from the HOSL control room to stop transfers from BPA and UKOP.

The HOSL operations team would open up the required tankside valves in preparation to receive a fuel parcel from BPA, but the final route setting, start of the transfers, and finish of the transfers were under the control of BPA. If necessary, to accommodate large parcel transfers, the HOSL team would open up further tank(s) and close off the original, now full, tank as the transfer proceeded.

The Buncefield Incident – 7 Years on: Could It Happen Again?

At the time of the Buncefield incident, the key features of the monitoring and control arrangements for the HOSL facility in relation to the tanks primarily involved (tanks 912 and 915) are shown in *Figure 2*. The things to note are the following:

- Four Visual Display Unit (VDU) screens for monitoring and control of the FINALine.
- Full control by the HOSL operators of the FINALine, all the way from the refinery.
- Direct measurement of the flow being received by HOSL from the FINALine.
- Only one VDU screen for monitoring the tank ATG system (20+ tanks) (if display of more than one individual tank was required, it would be 'nested' on the screen).
- Output of the independent high-level switches from the alarm panel routes through supervisory control and data acquisition (SCADA) system controlled by the programmable logic controller (PLC) to remote-operated shut-off valves in the pipeline, rather than being directly hardwired.
- Emergency stop in the control room only operates on the FINALine.
- UKOP remote isolation valve is upstream of the offtakes to other terminal users (BPA and British

Petroleum (BP)) who may not be affected by a requirement to shutdown initiated from the HOSL site, for example, a spurious trip initiation. Similar shutdown arrangements for the UKOP North line are not shown in the diagram.

- Emergency shutdown of the flow from the UKOP lines from the HOSL control room initiated by telephone call to the BPA Kingsbury terminal in the midlands.
- No direct flow measurement of the flow received from BPA.

The flowrates from UKOP were typically significantly higher than those from the FINALine; on 11 December, gasoline was being received from the UKOP line (into tank 912) at a flowrate in excess of 500 m³/h, whereas the flow from the FINALine (into tank 915) was between 140 and 240 m³/h. HOSL had direct control of the flowrates from the FINALine, but only indirect control, by request, over the flowrates from the UKOP lines. Commercial pressures were to accept whatever flowrate was set by the UKOP system and make any adjustments necessary on the FINALine.

There is no evidence that the changes to the control room arrangements in the mid-1990s had been subject to a formal review or management of change

process to ensure that the HOSL operator had appropriate information and full direct control over the fuels they were receiving. A Buncefield Standards Task Group (BSTG) and Process Safety Leadership Group (PSLG) action has addressed this issue.^{2,3}

Over the years, and particularly since the Shell part of the Buncefield terminal closed in 2003, the workload of the HOSL operators had significantly increased. The throughput of road tankers had increased with the consequent increase in throughput from the pipelines to the tanks. Available tank capacity had become a constraint. Parcel sizes from the pipelines often exceeded the available capacity in a single tank, particularly for the high-throughput fuels such as gasoline. Again there was no evidence of a formal review of the implications on the operational capability of the terminal and the workload for the operations team.

Both the examples above demonstrate how 'mission creep' can affect operations and build up into bigger issues over time, often bypassing formal change control processes.

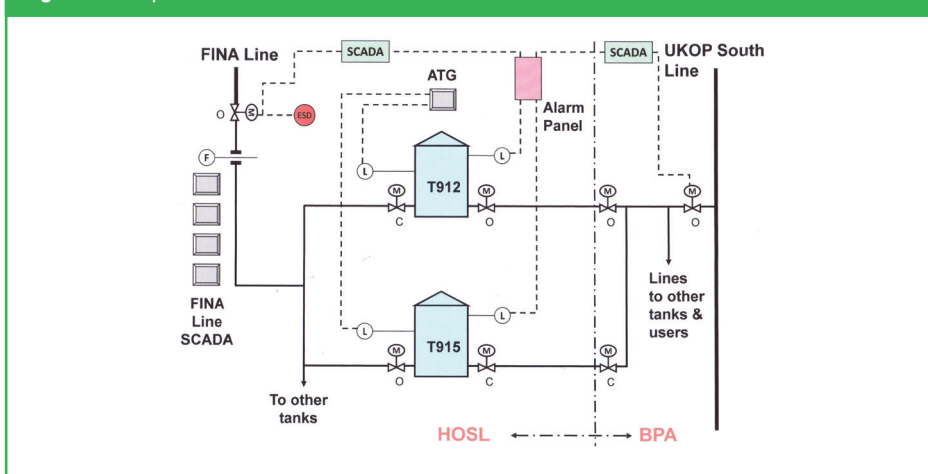
V. Management of Change

The process of replacing the failed independent high-level switches on tanks 911 and 912 in 2004 was treated as a 'like for like' replacement. In practice, this was not the case, and a number of opportunities were missed to ensure that the changes necessary with the new TAV checkable switch had been properly reviewed and understood.

The request from the site operator was to replace the failed switches, but there was no evidence that any original design information or definitive technical data for the required instruments was made available by them to the contractor. In turn, the contractor referred to their internal records and previous purchases of switches from the manufacturer (not solely for the site operator) to prepare an enquiry. There was no evidence of any checks on what was currently fitted onsite.

The key features of the order that was placed with the manufacturer were for a

Figure 2. Simplified overview of fuel transfer



SCADA: supervisory control and data acquisition; BPA: British Pipelines Agency; UKOP: United Kingdom Oil Pipelines; HOSL: Hertfordshire Oil Storage Ltd; ATG: Automatic Tank Gauging.

The Buncefield Incident – 7 Years on: Could It Happen Again?

weight-operated, checkable switch with a change-over SPDT contact arrangement and Exd certification. In all these areas, the ordered switch differed from that initially installed on the tanks: displacer operated, non-checkable (later modified onsite with a form of check facility), SPST contact and Exi certification. The manufacturer did not challenge the details of the order, but in turn, the manufacturer was not provided with full details of the application. An outcome from the criminal court case was that both the manufacturer and the contractor as suppliers of safety critical equipment should have been more inquisitive about the intended use of the level switches and should have been prepared to challenge the proposals.

A final opportunity to identify that the replacement was not 'like for like' came with the actual installation (*Figure 3*). The switch removed from tank 912 was clearly different from the one to be fitted, most notably in the large displacer rather than the small weight and the different checking mechanism. At some stage during the installation process, the padlock was removed from the new switch and not replaced; its vital importance to the safe operation of the new switch was not recognised.

During the investigation, the isolator units to interface the independent high-level switches with the alarm panel were found to be different from those shown on the circuit diagram. A newer type of

intrinsically safe certified galvanic isolator had replaced the original design. In doing so, the originally fitted line break and short circuit protection features had been compromised. There was no evidence that change control procedures had been applied to this modification. Nor were there any documents to support the changes to Exd certified switches where the original circuits had been designed as Exi.

VI. Operating and Proof Testing Procedures

At first sight, there was a range of operating procedures and proof testing arrangements in place. Detailed examination of the documents demonstrated that they were of limited use, although their existence had satisfied an external safety audit. Many of the procedure documents obtained were less than a page long with the majority of the requirements relating to 'health and safety' topics rather than the actual task to be done.

There was no standardised procedure for filling a tank. Each operator had his own approach, and there was evidence that often through constraints on available ullage, reliance would be placed on the high-level alarms to warn of the need to take action and, for example, to change over to a new tank. The use of an alarm clock was one approach used by some operators to provide an action

trigger. The availability and use of the 'movement' functionality on the ATG was an example of something not included in any procedure.

In the commercial court, Mr Justice David Steel commented,

– I unhesitatingly accept the need for written instructions, but there were in fact no written instructions for tank filling activity (leaving aside WI 10 & WI 11 which were irrelevant), let alone any compliant with API 2350.⁴

– A near miss in August 2003 was justifiably described ... as a dress rehearsal for the incident in December 2005 ... (it is) legitimately suggested ... that the only explanation of the incident is that there was no monitoring of the Motherwell screens. The supervisors were simply waiting for the alarms to sound.

– ... my own view is that routine operations are often those in which lax habits are most likely to develop.

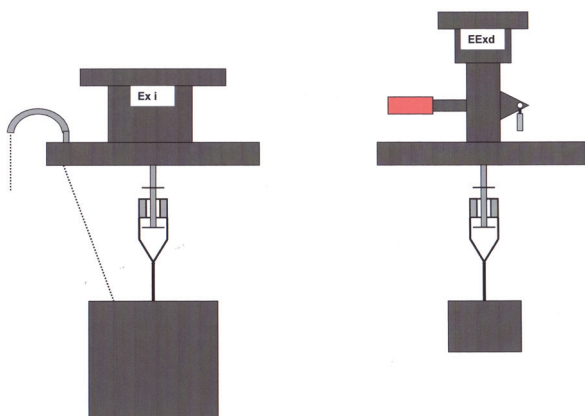
There was a test procedure and record sheet for the independent high-level switches to be completed monthly for the alarms and annually for a shutdown initiated from one tank only.

The documentation referred to the switches as 'Cobham', much in the same way as 'Hoover' is used when referring to a vacuum cleaner; there were switches manufactured under the Cobham name on the terminal, but they were not on storage tank-independent high-level duty.

Again the detail was lacking in these procedures, the different test method required for the new level switches was not reflected in a revised procedure. There was no requirement to be sure to fit the padlock with the lever in the horizontal position at the end of a test.

The conduct of the routine proof tests was unsatisfactory in a number of respects, particularly the recording of test results, completion of tests to time, responsibilities for their completion and whether all the in-service tanks were tested. The timing of the tests was

Figure 3. Like for like replacements?



The Buncefield Incident – 7 Years on: Could It Happen Again?

apparently based on the requirements to do month-end dipping of the tanks, so that the two tasks could be done concurrently. It appears that the month-end dipping of tanks had a higher priority.

There was no evidence that the site operator had applied the baseline good practice guidance contained in the Institute of Petroleum (IP) document 'Inspection and Testing of Protective Instrumented Systems'⁵ dating from 1980 that was available prior to 1999 (guidance that has been absorbed into BS EN 61511⁶).

As far back as March 2003, there was evidence that the end-of-month proof tests had not been done on the independent high-level switches on tanks 911 and 912 due to failure of the pull cord that provides the (then) checking mechanism (see *Figure 3*). Although there was a repair to the pull cord on the switch on tank 912, the switch on tank 911 was reported in September 2003 to be 'U/S' and to need replacing. From then though to February 2004, some tests were reported as 'X' (presumably satisfactory) and others as 'U/S' until a decision was taken in March 2004 to replace both switches. The new switches were ordered in April and received at the end of May 2004 and fitted at the beginning of July 2004. There was no evidence of a proof test having been done immediately following installation of the new switches; the first record of a satisfactory test was at the normal end-of-month test scheduled for the end of July and completed in August.

In the extended period (over 6 months) when the independent high-level switches on tanks 911 and 912 were out of service, there was no evidence of any special procedures having been put in place to provide an alternative method of preventing the tanks from overfilling. Reliance on the ATG alarms remained as the prime (only?) method of warning in case of a potential overfill.

VII. Identification of Safety Critical Equipment and Risk Assessments

The HOSL Engineering Co-ordinator had been tasked with producing a list of

safety critical items on the facility. He had been progressing this over 2 years, but it was not complete. He was overloaded and needed assistance from others, which was not forthcoming despite requests. The importance of the independent high-level switches as a safety critical item was not recognised. There was no recognition among the operating team that overfill protection was safety critical. Overfilling of a tank was not identified as a principal accident hazard scenario for the Control of Major Accident Hazards (COMAH) submission; it was included as a contributor to a scenario of rupture of a tank and loss of the tank contents to the bund.⁷

BS EN 61511⁶ had been published in 2003, but there was no evidence that any action had been taken by the site operator to review the requirements of BS EN 61511⁶ (or BS EN 61508)⁸ against current activities on-site, and to generate an action plan to resolve any identified gaps. A start had been made by a consultant with a risk assessment for tank overfill as part of the COMAH submission based on the risk graph approach in part 5 of BS EN 61508.⁸ The output from the risk graph for a safety integrated level (SIL) 1 requirement was inconsistent with the input information. There was no explanation for how the final results have been derived, and variations from the risk graph output agreed. A handwritten risk assessment for overfill of tank 912 contained flawed calculations. The assessment included the definition of the servo gauge and ATG system as a SIL 1 protective system. This was inappropriate; this equipment provided the basic process control system (BPCS) as defined in IEC 61511.⁶

There was no evidence of how the proof test intervals of 1 month for the offline test of the switches and annually for the live shutdown test had been derived or validated, nor was their evidence to show that the ultimate overfill protection system met any defined performance standard, whether expressed as a SIL or as a probability of failure on demand (pfd).

VIII. Relationships with Suppliers

The relationship with the company supplying tank-level measurement expertise had developed over many years starting from the original supply of the tank float gauges through to the conversion to an ATG system and the provision of a service contract for routine and call out maintenance. The inclusion of the tank high-level switches was a relatively recent addition to the service contract. This company had gone through a number of reorganisations until a management buyout in 2003 that formed the contractor company. The site operator placed high reliance on the technical competence of the contractor and their capabilities to maintain the ATG system, level gauges, and switches, but there was no evidence that this reliance was discussed with or agreed by the contractor in particular in relation to the requirements for a high-hazard site. Rather, the contractor considered that their relationship with the site operator was a normal commercial one and that there was no guarantee that the site operator would not go elsewhere for their level instrumentation-related services once the current contracts had been completed.

There was no evidence that the role and contribution of key contractors, in relation to compliance with the COMAH regulations, had ever been discussed at senior level or with the contractors' employees who visited the site.

There was no evidence of any recent auditing of the performance of the contractor and delivery of their technical expertise. The audits that had been done concentrated on contractor health and safety performance; there was only one question related to technical aspects, and this was superficial. As a company, the contractor in their current form had only been in existence for 2 years; a review of their competence and capability should have been available.

Similarly, the relationship between the contractor and the manufacturer was a straightforward commercial one; there was no evidence of any

The Buncefield Incident – 7 Years on: Could It Happen Again?

discussions to examine the safety critical aspects of the equipment and applications or the implementation of the standards BS EN 61508⁸ and BS EN 61511.⁶ Measures to ensure that the checkable features of the independent high-level switches and the importance of the padlock were fully understood were not in evidence.

Equipment suppliers and contractors serving COMAH sites in particular need to ensure that they adopt an ‘intelligent client’ approach, ensuring that they understand the control of process risks where their equipment or service may be a contributory part. Information sharing and performance monitoring are a vital part of being an intelligent client.

IX. Leadership and Competence

Throughout the investigation, examples were found where the necessary leadership and competence, for the effective operation of safety critical systems, and in potentially high-hazard environments had been in short supply. The high levels of overtime and staff turnover at the operating site contributed to these issues. Understanding of the requirements for operating in a high-hazard arena to comply with the COMAH regulations and related standards such as BS EN 61511,⁶ and deliver an exemplary safety and environmental performance requires dedication and considerable effort. Companies supplying equipment and services into this arena

also need to have a thorough understanding of their obligations and create the necessary dialogue with their suppliers and clients. Achieving this requires that the following aspects are correctly implemented:

- Process safety leadership;
- Roles and responsibilities;
- People selection;
- Competencies;
- Culture and awareness;
- Risk assessment;
- Safety critical process control;
- Systems and procedures;
- Information and documentation;
- Management of change;
- Equipment and suppliers.

X. Conclusion

‘This case has a more to do with slackness, inefficiency and a more or less complacent approach to matters of safety (*than an element of cost cutting at the expense of safety*)’ (Mr Justice Calvert Smith presiding at St Albans Crown Court for the Buncefield criminal case).

Is your corporate memory suitably non-volatile, or can it be erased over time? Is experience valued, updated as necessary, and passed on effectively?

When incidents occur, we investigate, discover the causes, and introduce specific improvement measures to prevent them from happening again. Then, over time, experienced individuals leave the organisation taking their

knowledge with them, other requirements overlay the experiences, the organisation as a whole forgets, and before long, conditions become ripe for another incident.

What has happened before will happen again. What has been done before (or not done) will be done again. There is nothing new in the whole world. (Ecclesiastes 1:9)

The Buncefield incident – could it happen again? The answer is in your hands.

References

- 1 Kletz TA. *Lessons from Disaster – How Organisations Have No Memory*. 1993.
- 2 The Process Safety Leadership Group (PSLG). *Safety and environmental standards for fuel storage sites*. PSLG final report, 11 December 2009. Bootle: HSE.
- 3 Buncefield Standards Task Group (BSTG). *Safety and environmental standards for fuel storage sites*. BSTG final report, 24 July 2007. Bootle: HSE.
- 4 API RP 2350. *Overfill Protection for Storage Tanks in Petroleum Facilities*. 4th ed. API, 2012.
- 5 *Inspection and Testing of Protective Instrumented Systems: Part 14 of the IP Model Code of Safe Practice in the Petroleum Industry*. Institute of Petroleum, 1980.
- 6 BS EN IEC 61511:2003. *Functional safety – Safety instrumented systems for the process industry sector (Three parts)* BSI.
- 7 Control of Major Accidents (COMAH) Competent Authority Investigation Team. *Buncefield: Why did it happen?* COMAH final report, 16 February 2011. Bootle: HSE.
- 8 BS EN IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety related systems (Seven parts)* BSI.
- 9 Major Incident Investigation Board (MIIB). *The final report of the Major Incident Investigation Board*, Volumes 1 & 2, 11 December 2008. Bootle: HSE.