

Recommendations on the design and operation of fuel storage sites

Recommendations on the design and operation of fuel storage sites

© *Crown copyright* This publication may be freely reproduced, except for advertising, endorsement or commercial purposes. First published 03/07.

Contents

Introduction	1
The Board's approach	2
Scope of the recommendations	3
Status of the recommendations	3
The Baker report	5
Further work to investigate explosion mechanism	6
The recommendations	6
Systematic assessment of safety integrity level requirements	8
Recommendation 1	
Protecting against loss of primary containment using high integrity systems	10
Recommendations 2-10	
Engineering against escalation of loss of primary containment	14
Recommendations 11-16	
Engineering against loss of secondary and tertiary containment	16
Recommendations 17-18	
Operating with high reliability organisations	18
Recommendations 19-22	
Delivering high performance through culture and leadership	20
Recommendations 23-25	
Annexes	
1: Terms of reference and progress	22
2: Members of the independent Board	25
3: Rationale for Recommendation 3 – Independent and automatic storage tank overflow prevention	26
4: Background and supporting material for 'improved components and systems' (Recommendation 8)	28
5: High reliability organisations (Recommendations 19-22)	30
6: BS EN 61511 Functional safety - safety instrumented systems for the process industry sector	32
7: Examples of incidents that have involved loss of primary containment from storage tanks	34
References	36
Glossary	38
Further information	41



Figure 1 An overview of an oil storage depot on the east coast of England.

Introduction

1 This report sets out recommendations to improve safety in the design and operation of fuel storage sites. We make these recommendations as the independent Investigation Board, chaired by Lord Newton of Braintree, set up to supervise the investigation into the explosions and fires at the Buncefield oil storage and transfer depot, Hemel Hempstead, Hertfordshire on 11 December 2005. The investigation was directed by the Health and Safety Commission (HSC) using its powers under section 14(2)(a) of the Health and Safety at Work etc Act 1974.

2 Item 5 of the investigation's terms of reference requires us to 'make recommendations for future action to ensure the effective management and regulation of major accident risk at COMAH¹ sites. This should include consideration of off-site as well as on-site risks and consider prevention of incidents, preparations for response to incidents, and mitigation of their effects.'

3 Our initial report, published on 13 July 2006, identified four principal workstreams that would form the basis for our continuing work and developing recommendations. Those workstreams are:

- ▼ design and operation of storage sites;
- ▼ emergency preparedness for, and response to, incidents;
- ▼ advice to planning authorities; and
- ▼ examination of the Health and Safety Executive's (HSE's) and the Environment Agency's roles in regulating the activities on the Buncefield site.

4 This report concentrates on the first of these – design and operations. Future reports will make recommendations on other areas, though we anticipate some overlap as the workstreams are closely related. Improving control measures goes hand in hand with improving emergency arrangements and with considering the potential impacts of major incidents on local communities. This report builds on the broad conclusions set out in paragraphs 61-77 of our initial report, which in turn reflect the findings of the investigation, as summarised in the initial report and in the three progress reports preceding it. That material is referenced, but not repeated, in this report. In preparing this report we have also considered information from other sources, such as the Buncefield Standards Task Group,² the Competent Authority³ and the Baker report (see paragraph 15). Our broad aim in making these recommendations is to catalyse improvement in the fuel storage sector so that it is continually alert to the major hazard potential of its operations.

¹ The Control of Major Accident Hazards Regulations 1999. These Regulations are enforced by a joint Competent Authority comprising HSE and the Environment Agency in England and Wales and HSE and the Scottish Environment Protection Agency in Scotland.

² The joint Competent Authority/Industry Standards Task Group set up to review safety and environmental protection standards at fuel storage sites following the Buncefield incident. The Task Group published its initial recommendations on 12 October 2006.

³ See footnote 1. The Competent Authority issued Safety Alerts in February and July 2006.

The Board's approach

5 Our starting point in developing these recommendations is the importance of primary containment,⁴ as expressed in paragraph 63 of our initial report:

The occurrence of a massive fuel vapour explosion confirms the overriding need to ensure the integrity of the primary means of containment; in other words, to make sure that liquid does not escape from the vessels in which it is normally meant to be confined.

6 Recommendations 1-16 therefore emphasise the need to increase the protection provided by primary containment systems. The Buncefield incident highlighted the need for high integrity systems for this purpose. Notwithstanding the importance of primary containment, there remains a need for effective means of preventing environmental pollution in the event of a failure of primary containment. While implementing our recommendations should significantly reduce the likelihood of such a failure, the potential for failure remains. Recommendations 17-18 therefore deal with improvements to secondary and tertiary containment.⁵

7 Recommendations 1-18 essentially deal with technological matters and their management. However, paragraph 74 of our initial report noted that human and organisational factors are also important and these are covered in Recommendations 19-22. Finally, Recommendations 23-25 deal with broader strategic objectives relating to sector leadership and culture, essential to ensure that the benefits of the more detailed recommendations are fully realised.

8 In several areas work is already underway that has the potential to meet these recommendations, in response both to the Buncefield Standards Task Group report^(ref 1) and to Safety Alerts issued by the Competent Authority. We understand that the Task Group is also working on other aspects of design and operation, including aspects recommended in our initial report. We welcome the initiative of the sector and the Competent Authority in taking this forward. However, the Task Group is a temporary body set up to deliver a specific project of improvements (a so-called 'task-and-finish' group). Without implying any criticism of the Task Group, this is not a suitable arrangement for leadership of the sector. As we indicate in paragraphs 34-36 of this report, the Board believes that the sector, in consultation with the Competent Authority, needs to build on its work to put in place continuing arrangements for comparable leadership in relation to operating and safety standards on a long-term basis. In our view action to improve sector leadership will be the key to facilitate implementation of our recommendations and to provide a focus for continuous improvement.

⁴ Primary means of containment are the tanks, pipes and vessels that hold liquids and the devices fitted to them to allow them to be operated safely.

⁵ Secondary means of containment are enclosed areas around storage vessels (often called bunds), created usually by concrete or earth walls. Their purpose is to hold any escaping liquids and any water or chemicals used in firefighting. Tertiary means are features such as drains designed to limit the passage of chemicals off site, or raised kerbs to prevent liquids that have breached the bunds from escaping into the general area around the site.

Scope of the recommendations

9 As a minimum the recommendations in this report address Buncefield-type sites as defined in the Buncefield Standards Task Group report,⁶ ie depots that store and transfer petroleum products on a large scale. We use the term ‘the sector’ to denote these sites collectively, except where the context clearly indicates otherwise. Some recommendations will also apply to a wider range of fuel storage facilities. In some cases, although we have not studied the wider chemical industry, we consider that relevant lessons for fire and explosion risks can be applied beyond fuel storage and distribution. We indicate in the text some obvious areas where our recommendations may apply beyond the sector, as defined above. More generally, we encourage the chemical industry, working with the Competent Authority, to consider the broader relevance of our findings so far.

10 The recommendations are addressed to those in the sector who have the legal duties to prevent and control major accidents.⁷ Primarily this means operators of Buncefield-type sites as described in paragraph 9, but also includes designers, suppliers and contractors, as well as professional institutions or trade associations where appropriate. In practice this will require close working with the regulators (the Competent Authority), who will also need to ensure the recommendations are implemented.

Status of the recommendations

11 In making these recommendations we recognise that work continues, including the work to investigate explosion mechanisms mentioned in paragraphs 16-19 and work in the Buncefield Standards Task Group. Further recommendations will follow in relation to other areas of interest mentioned in paragraph 3.

12 We expect our recommendations to be put into practice throughout the sector. Unless the context indicates otherwise, we envisage the Competent Authority will adopt the recommendations as the minimum necessary to comply with legal requirements. For example, where the recommendations call for higher standards to be incorporated in revised guidance, those standards should be capable of being insisted upon by law. The recommendations do not specifically call for changes to the law on the assumption that the existing legal framework is sufficient to ensure that necessary improvements are put in place. However, if this proves not to be the case in any respect, HSC and the Department for Environment, Food and Rural Affairs (DEFRA) should draw up proposals for the necessary legal changes.

⁶ The Task Group initial recommendations apply to petrol stored at COMAH top and lower tier sites in vertical, cylindrical, non-refrigerated, above ground storage tanks with side walls greater than 5 metres in height and where the filling rate is greater than 100 cubic metres/hour.

⁷ COMAH requires operators of major hazard sites subject to the Regulations to take all measures necessary to prevent major accidents and limit their consequences to persons and the environment. Operators of top tier COMAH sites (like Buncefield) are also required to submit written safety reports to the Competent Authority; and to prepare emergency plans to deal with the consequences of a major accident. Operators and others (including contractors, designers, suppliers) also have relevant duties under the Health and Safety at Work etc Act 1974 and related regulations and under environmental legislation.



Figure 2 Aerial view of the Buncefield depot

13 Where the recommended improvements are self evidently necessary or where the sector is already intent on their implementation we expect the recommendations to be implemented without undue delay. Some recommendations, particularly those involving large-scale engineering improvements, will be easier to implement in new sites than in existing sites. Other recommendations, such as those needing cultural and leadership changes, should be addressed immediately, though their effects may not be apparent in the short term. It is essential to have clear timescales, understood both by the industry and the Competent Authority, against which progress can be measured and reported. We therefore ask the Competent Authority to start without delay a programme of reviews with operators of Buncefield-type sites of their response to these recommendations, leading to site-specific timed action plans.

14 Where commitments have already been made (eg through the Buncefield Standards Task Group) or the need for action is self-evident, we have not made detailed cost-benefit assessments. In most cases we consider the costs will be reasonable and the benefits, in preventing another Buncefield incident, beyond argument. We are exploring further the costs and other implications of some recommendations relative to their perceived benefits, though we expect this to confirm our belief that the improvements we recommend are affordable. In agreeing priorities for the action plans we call for in paragraph 13, the Competent Authority will need to take account of cost, as described in paragraph 31.

The Baker report

15 We have noted with interest the recent report of the BP US Refineries Independent Safety Review Panel by James Baker's panel in the United States.^(ref 2) Some of the recommendations and findings in that report align with our thinking arising from the Buncefield investigation. In particular the Baker report's recommendations relating to process safety leadership, process safety culture, performance indicators, independent monitoring and industry leadership are relevant. The Baker panel's findings regarding the implementation of good engineering practices, safety knowledge and competence also align with our views.



Figure 3 Damage to property on the Maylands estate adjacent to Buncefield

Further work to investigate explosion mechanism

16 Current explosion models do not predict the blast damage that occurred at Buncefield. Paragraph 77 of our initial report said:

Further work is needed to research the actual mechanism for generating the unexpectedly high explosion overpressures seen at Buncefield. This is a matter of keen international interest, and participation from a broad range of experts, as well as the industry, is essential to ensure the transparency and credibility of any research programme. The Board will consider further recommendations about the nature and scope of such work.

17 Towards the end of 2006 we appointed an advisory panel to assist us in formulating proposals for a programme of work. The panel is chaired by Professor Dougal Drysdale who is a member of the Board. The panel is considering the evidence currently available in respect of potential explosion mechanisms of a flammable vapour cloud that could cause the type and extent of damage seen at Buncefield.

18 We have asked the panel to advise us whether research is justified and if so the scope of such research, likely methods of funding it, and its governance arrangements, to ensure a satisfactory outcome. We have asked the panel to present its findings to us shortly after Easter and we shall make our recommendations known soon afterwards.

19 The advisory panel experts are:

Professor Dougal Drysdale, University of Edinburgh (Chair)
Professor Derek Bradley, University of Leeds
Professor Geoffrey Chamberlain, Shell Global Solutions
Dr Laurence Cusco, Health and Safety Laboratories
Mike Johnson, Advantica
Professor Hans Michels, Imperial College London
Professor Vincent Tam, BP Exploration

The recommendations

20 Our recommendations are grouped under the following six headings:

- ▼ Systematic assessment of safety integrity level requirements (Recommendation 1)
- ▼ Protecting against loss of primary containment using high integrity systems (Recommendations 2-10)
- ▼ Engineering against escalation of loss of primary containment (Recommendations 11-16)
- ▼ Engineering against loss of secondary and tertiary containment (Recommendations 17-18)
- ▼ Operating with high reliability organisations (Recommendations 19-22)
- ▼ Delivering high performance through culture and leadership (Recommendations 23-25)

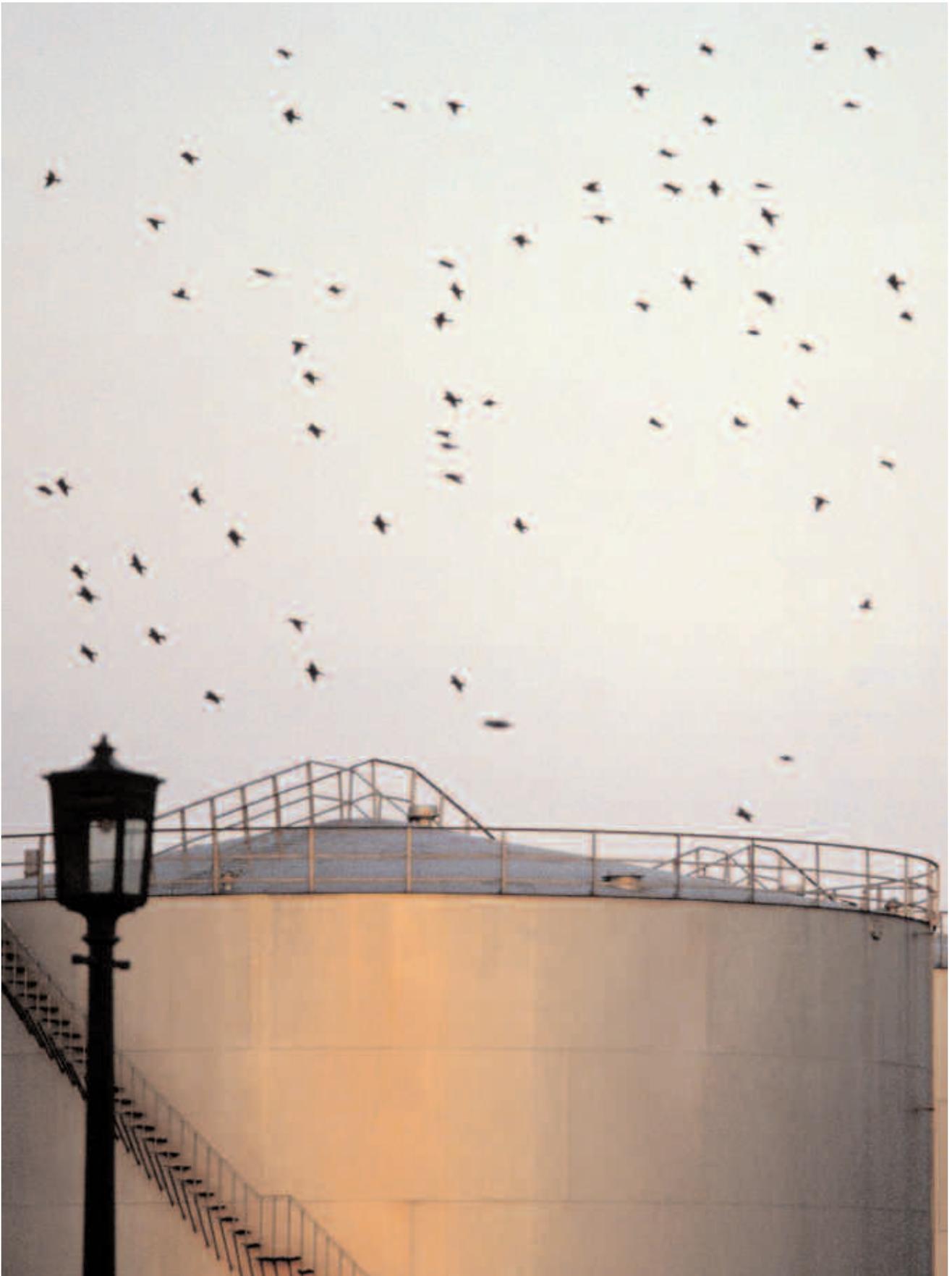


Figure 4 Tops of a tank farm in South London

Systematic assessment of safety integrity level requirements

21 The recommendations under this and the next two headings are based on the conclusions set out in paragraphs 61-77 of our initial report and on the findings of the first and third progress reports. The Buncefield incident highlighted the need for high integrity systems, which we discuss further in the next section. However, our firm belief is that before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve. The sector currently lacks a common methodology to ensure a systematic approach to this determination process. Several methodologies exist, but there is no consistency. A common methodology would provide greater assurance.

22 Recommendation 1 is in line with work now underway following the Buncefield Standards Task Group's initial recommendations relating to tank overflow protection, particularly paragraph 9, which states *'The overall systems for tank-filling control must be of high integrity – with sufficient independence to ensure timely and safe shutdown to prevent tank overflow. Site operators should meet the latest international standards.'*

Recommendation 1 The Competent Authority and operators of Buncefield-type sites should develop and agree a common methodology to determine safety integrity level (SIL)⁸ requirements for overflow prevention systems in line with the principles set out in Part 3 of BS EN 61511.^(ref 3) This methodology should take account of:

- ▼ the existence of nearby sensitive resources or populations;
- ▼ the nature and intensity of depot operations;
- ▼ realistic reliability expectations for tank gauging systems; and
- ▼ the extent/rigour of operator monitoring.

Application of the methodology should be clearly demonstrated in the COMAH safety report submitted to the Competent Authority for each applicable site. Existing safety reports will need to be reviewed to ensure this methodology is adopted.

⁸ A SIL is a measure of the safety system performance, in terms of the probability of failure on demand. There are four discrete integrity levels, SIL 1-4. The higher the SIL level, the higher the associated safety level and the lower the probability that a system will fail to perform properly.



Figure 5 General view of fuel storage tanks with associated pipework and instrumentation

Protecting against loss of primary containment using high integrity systems

23 Paragraph 21 notes that the Buncefield incident highlighted the need for high integrity systems to prevent breaches of primary containment. The background is summarised in paragraphs 61-77 of our initial report, based on the findings of the third progress report. In particular, paragraph 63 of our initial report emphasised the overriding need to ensure the integrity of the primary means of containment. The following recommendations, particularly Recommendations 2-8, are closely related and need to be considered as a whole. Our recommendations for automatic systems, that do not depend on the need for human intervention, are not intended to override the risk-based approach of Recommendation 1 but to act as a starting point.

24 Recommendations 3-5 reflect our firm view that to ensure integrity the sector must move towards installing independent overfill prevention systems at sites handling large quantities of highly flammable liquids⁹ such as petrol. We welcome indications that API Code 2350^(ref 4) is also moving in this direction. In many respects Recommendations 3-5 align with work underway to implement paragraphs 8-11 of the Buncefield Standards Task Group's initial report, except that the Task Group stopped short of recommending automatic overfill prevention systems. Annex 1 to this report sets out our arguments for installing automatic overfill prevention systems (Recommendation 3). This would be a significantly higher standard than that generally installed in this sector. These changes will need to be carefully planned to consider up-stream implications and phased in to avoid undue disruption to the UK fuel supply.

25 Recommendations 6 and 7 follow up paragraph 76 of our initial report, which referred to the need for good communication between the parties responsible for transferring fuel safely around the country. We indicated that the adequacy of existing safety arrangements for transferring fuel between sites, eg between refineries and Buncefield-type sites, may need to be reviewed. In returning to this, we firmly believe that such a review is necessary given the number of responsible parties in a typical system – refinery operator, pipeline operator, and depot operator.

26 The safety report for any given depot or refinery (gasoline pipelines are not currently subject to COMAH, though we may return to this in our next report) does not deal specifically with the relationship between the transmitter and the receiver of hazardous products. Therefore we welcome the recommendation at paragraph 7 in the Buncefield Standards Task Group's first report relating to improving the communications between site operators and operators of pipeline transfers. This does not, however, go so far as to require site operators to have ultimate control to stop receiving fuel into tanks to prevent an overfill. We believe it is essential for such a hierarchy of control to be established, at the same time dealing with any upstream consequences.

⁹ A liquid fuel is classified under the Planning (Control of Major Accident Hazards) Regulations 1999 according to its flashpoint, defined as *'The minimum temperature at which a liquid, under specific test conditions, gives off sufficient flammable vapour to ignite momentarily on the application of an ignition source'*. A highly flammable liquid is defined as one with the flashpoint below 21°C. As petrol has a flashpoint in the region of c -40°C, it is therefore classified as a highly flammable liquid.

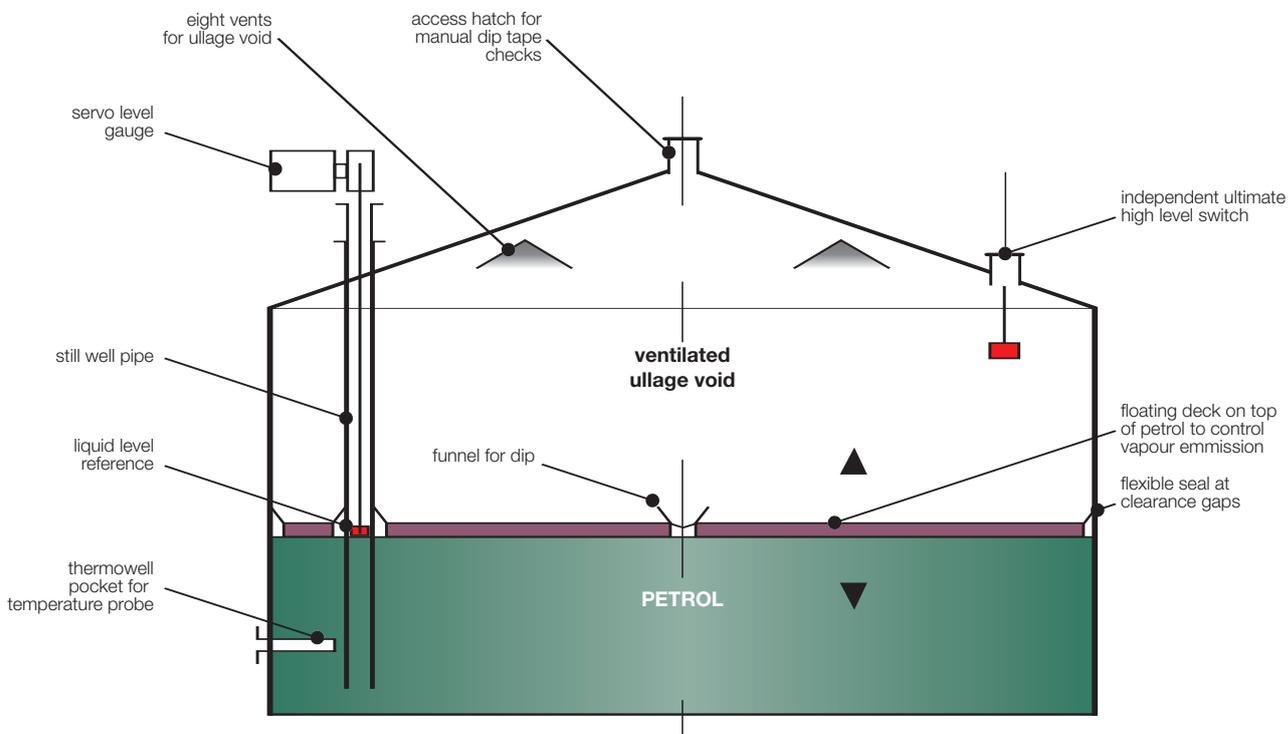


Figure 6 General schematic of a typical internal floating roof tank

27 Annex 2 to this report sets out our arguments for developing improved components and systems (Recommendation 8). Recommendations 9 and 10 are needed to help monitor and review the effectiveness of improved control measures.

Recommendation 2 Operators of Buncefield-type sites should, as a priority, review and amend as necessary their management systems for maintenance of equipment and systems to ensure their continuing integrity in operation. This should include, but not be limited to reviews of the following:

- ▼ the arrangements and procedures for periodic proof testing of storage tank overfill prevention systems to minimise the likelihood of any failure that could result in loss of containment; any revisions identified pursuant to this review should be put into immediate effect;
- ▼ the procedures for implementing changes to equipment and systems to ensure any such changes do not impair the effectiveness of equipment and systems in preventing loss of containment or in providing emergency response.

Recommendation 3 Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a high integrity, automatic operating overfill prevention system¹⁰ (or a number of such systems, as appropriate) that is physically and electrically separate and independent from the tank gauging system.

Such systems should meet the requirements of Part 1 of BS EN 61511 for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1). Where independent automatic overfill prevention systems are already provided, their efficacy and reliability should be reappraised in line with the principles of Part 1 of BS EN 61511 and for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1).

¹⁰ The factors that determine the type of independent automatic system required will include the effects on the upstream system, for example if filling from a refinery process, a ship or a railway vessel. For all systems the outcome required is the same, ie automatically stopping supply to the dangerously full tank by means that are fully independent of the tank gauging system.

Recommendation 4 The overfill prevention system (comprising means of level detection, logic/control equipment and independent means of flow control) should be engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity in accordance with the requirements of the recognised industry standard for ‘safety instrumented systems’, Part 1 of BS EN 61511.

Recommendation 5 All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure the specified safety integrity level is maintained in practice in accordance with the requirements of Part 1 of BS EN 61511.

Recommendation 6 The sector should put in place arrangements to ensure the receiving site (as opposed to the transmitting location) has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) without depending on the actions of a remote third party, or on the availability of communications to a remote location. These arrangements will need to consider upstream implications for the pipeline network, other facilities on the system and refineries.



Recommendation 7 In conjunction with Recommendation 6, the sector and the Competent Authority should undertake a review of the adequacy of existing safety arrangements, including communications, employed by those responsible for pipeline transfers of fuel. This work should be aligned with implementing Recommendations 19 and 20 on high reliability organisations to ensure major hazard risk controls address the management of critical organisational interfaces.

Recommendation 8 The sector, including its supply chain of equipment manufacturers and suppliers, should review and report without delay on the scope to develop improved components and systems, including but not limited to the following:

- ▼ alternative means of ultimate high¹¹ level detection for overfill prevention that do not rely on components internal to the storage tank, with the emphasis on ease of inspection, testing, reliability and maintenance;
- ▼ increased dependability of tank level gauging systems through improved validation of measurements and trends, allowing warning of faults and through using modern sensors with increased diagnostic capability; and
- ▼ systems to control and log override actions.

Recommendation 9 Operators of Buncefield-type sites should introduce arrangements for the systematic maintenance of records to allow a review of all product movements together with the operation of the overfill prevention systems and any associated facilities. The arrangements should be fit for their design purpose and include, but not be limited to, the following factors:

- ▼ the records should be in a form that is readily accessible by third parties without the need for specialist assistance;
- ▼ the records should be available both on site and at a different location;
- ▼ the records should be available to allow periodic review of the effectiveness of control measures by the operator and the Competent Authority, as well as for root cause analysis should there be an incident;
- ▼ a minimum period of retention of one year.

Recommendation 10 The sector should agree with the Competent Authority on a system of leading and lagging performance indicators for process safety performance. This system should be in line with HSE's recently published guidance on *Developing process safety indicators* HSG254.^(ref 5)

¹¹ Also commonly known as 'high high' level alarms.

Engineering against escalation of loss of primary containment

28 The recommendations under this heading follow on from our earlier arguments about the importance of primary containment – see paragraph 23 above. The Buncefield incident demonstrated the potential for a vapour cloud to form from a loss of primary containment of a highly flammable liquid such as petrol. We have adopted a precautionary approach in drawing up these recommendations as we believe they are appropriate in the light of the Buncefield incident, notwithstanding that the investigation into the severity of the explosion continues. Recommendation 12, in particular, anticipates our coming recommendations on emergency response arrangements.

Recommendation 11 Operators of Buncefield-type sites should review the classification of places within COMAH sites where explosive atmospheres may occur and their selection of equipment and protective systems (as required by the Dangerous Substances and Explosive Atmospheres Regulations 2002^(ref 6)). This review should take into account the likelihood of undetected loss of containment and the possible extent of an explosive atmosphere following such an undetected loss of containment. Operators in the wider fuel and chemicals industries should also consider such a review, to take account of events at Buncefield.

Recommendation 12 Following on from Recommendation 11, operators of Buncefield-type sites should evaluate the siting and/or suitable protection of emergency response facilities such as firefighting pumps, lagoons or manual emergency switches.

Recommendation 13 Operators of Buncefield-type sites should employ measures to detect hazardous conditions arising from loss of primary containment, including the presence of high levels of flammable vapours in secondary containment. Operators should without delay undertake an evaluation to identify suitable and appropriate measures. This evaluation should include, but not be limited to, consideration of the following:

- ▼ installing flammable gas detection in bunds containing vessels or tanks into which large quantities of highly flammable liquids or vapour may be released;
- ▼ the relationship between the gas detection system and the overfill prevention system. Detecting high levels of vapour in secondary containment is an early indication of loss of containment and so should initiate action, for example through the overfill prevention system, to limit the extent of any further loss;
- ▼ installing CCTV equipment to assist operators with early detection of abnormal conditions. Operators cannot routinely monitor large numbers of passive screens, but equipment is available that detects and responds to changes in conditions and alerts operators to these changes.

Recommendation 14 Operators of new Buncefield-type sites or those making major modifications to existing sites (such as installing a new storage tank) should introduce further measures including, but not limited to, preventing the formation of flammable vapour in the event of tank overflow. Consideration should be given to modifications of tank top design and to the safe re-routing of overflowing liquids.

Recommendation 15 The sector should begin to develop guidance without delay to incorporate the latest knowledge on preventing loss of primary containment and on inhibiting escalation if loss occurs. This is likely to require the sector to collaborate with the professional institutions and trade associations.

Recommendation 16 Operators of existing sites, if their risk assessments show it is not practicable to introduce measures to the same extent as for new ones, should introduce measures as close to those recommended by Recommendation 14 as is reasonably practicable. The outcomes of the assessment should be incorporated into the safety report submitted to the Competent Authority.



Figure 8 View of fuel tank set in earth bund

Engineering against loss of secondary and tertiary containment

29 While we emphasise the priority that should be given to preventing a loss of primary containment, adequate secondary and tertiary containment remains necessary for environmental protection in the event of a loss of primary containment of hazardous substances. Paragraphs 66 and 73 of our initial report and, in particular, the second progress report, described the failure of secondary and tertiary containment at Buncefield to prevent a major accident to the environment (MATTE).

30 Significant improvements to primary containment¹² will have implications for environmental protection systems. A fundamental review of the whole system of containment, taking account of site-specific conditions, will provide the greatest assurance for the safety and environmental protection of the site and its neighbourhood. As well as Buncefield-type incidents, other causes of primary containment failure such as sudden or undetected creeping loss of tank or pipework integrity can give rise to serious environmental consequences. This underlines the importance of maintaining high bunding standards.

31 Though there is a need for an integrated approach to containment, the recommendations below are segmented for convenience. Operators should adopt a risk-based approach and draw up plans for phased investment and improvement. They should be able to demonstrate to the Competent Authority why it is not practicable to meet fully improved standards, if that is so. We stress that the overflow of highly flammable liquid which led to the Buncefield explosions is only one foreseeable cause of a MATTE. Industry should therefore include improvements against those other foreseeable events in its remedial programme to secondary and tertiary containment, taking the same risk-based and phased approach.

¹² For example, in preventing tank overfilling, structural failure and loss of integrity (eg gasket failure) of pipework and valve joints.

Recommendation 17 The Competent Authority and the sector should jointly review existing standards for secondary and tertiary containment with a view to the Competent Authority producing revised guidance by the end of 2007.

The review should include, but not be limited to the following:

- ▼ developing a minimum level of performance specification of secondary containment (typically this will be bunding);
- ▼ developing suitable means for assessing risk so as to prioritise the programme of engineering work in response to the new specification;
- ▼ formally specifying standards to be achieved so that they may be insisted upon in the event of lack of progress with improvements;
- ▼ improving firewater management and the installed capability to transfer contaminated liquids to a place where they present no environmental risk in the event of loss of secondary containment and fires;
- ▼ providing greater assurance of tertiary containment measures to prevent escape of liquids from site and threatening a major accident to the environment.

Recommendation 18 Revised standards should be applied in full to new build sites and to new partial installations. On existing sites, it may not be practicable to fully upgrade bunding and site drainage. Where this is so operators should develop and agree with the Competent Authority risk-based plans for phased upgrading as close to new plant standards as is reasonably practicable.



Figure 9 A modern process control room

Operating with high reliability organisations

32 The need for high reliability organisations¹³ was not addressed directly in our initial report or in the Buncefield Standards Task Group's interim recommendations, though many of the issues below are being considered in the Task Group's continuing work. The need follows from the preceding recommendations relating to technological improvements in hardware. Such improvements are vital in improving process safety and environmental protection, but achieving their full benefit depends on human and organisational factors such as the roles of operators, supervisors and managers. Paragraph 74 of our initial report indicated our interest in this area.

33 The recommendations are more broadly applicable than Buncefield-type sites, but are intended to apply to those sites as a minimum.

Recommendation 19 The sector should work with the Competent Authority to prepare guidance and/or standards on how to achieve a high reliability industry through placing emphasis on the assurance of human and organisational factors in design, operation, maintenance, and testing. Of particular importance are:

- ▼ understanding and defining the role and responsibilities of the control room operators (including in automated systems) in ensuring safe transfer processes;
- ▼ providing suitable information and system interfaces for front line staff to enable them to reliably detect, diagnose and respond to potential incidents;
- ▼ training, experience and competence assurance of staff for safety critical and environmental protection activities;
- ▼ defining appropriate workload, staffing levels and working conditions for front line personnel;
- ▼ ensuring robust communications management within and between sites and contractors and with operators of distribution systems and transmitting sites (such as refineries);
- ▼ prequalification auditing and operational monitoring of contractors' capabilities to supply, support and maintain high integrity equipment;
- ▼ providing effective standardised procedures for key activities in maintenance, testing, and operations;
- ▼ clarifying arrangements for monitoring and supervision of control room staff; and
- ▼ effectively managing changes that impact on people, processes and equipment.

¹³ That is, robust organisations with a strong safety culture that have a high probability of achieving safe and reliable performance. More detail is given in Annex 5.

Recommendation 20 The sector should ensure that the resulting guidance and/or standards is/are implemented fully throughout the sector, including where necessary with the refining and distribution sectors. The Competent Authority should check that this is done.

Recommendation 21 The sector should put in place arrangements to ensure that good practice in these areas, incorporating experience from other high hazard sectors, is shared openly between organisations.

Recommendation 22 The Competent Authority should ensure that safety reports submitted under the COMAH Regulations contain information to demonstrate that good practice in human and organisational design, operation, maintenance and testing is implemented as rigorously as for control and environmental protection engineering systems.



Figure 10 Maintenance worker inspecting a tank top

Delivering high performance through culture and leadership

34 Culture and leadership were not addressed directly in our initial report or in the Buncefield Standards Task Group's first report, but are necessary prerequisites to achieving full compliance with the preceding recommendations. We have set the sector several tasks which we acknowledge to be very challenging:

- ▼ to substantially strengthen safety standards at Buncefield-type sites;
- ▼ to identify analogous sites where the same high level of engineered safety is necessary and to install it;
- ▼ to continue with and extend a programme of revision of guidance and standards to ensure more consistent responses to broadly similar risks than are the case today; and
- ▼ to bring about a wide range of cultural and behavioural changes.

35 Implementing our recommendations will require the sector to show clear leadership in setting high standards of process safety and environmental protection and in pursuing excellence in operations. At paragraph 8 we indicated our support for the work done thus far by the Buncefield Standards Task Group. We see the Task Group as continuing to play a key role. However, the scale of the improvements that we believe the sector needs to make can only come about through sector leadership at the highest level. We welcome the sector's acknowledgement of the need for more consistent responses to broadly similar risks. However, some fifteen months have passed since Buncefield, and we believe that the sector will face deserved criticism if clear and energetic progress is not now made on our recommendations.

36 The recommendations below require collaboration across the sector, as will several of our earlier recommendations in practice (eg Recommendation 19). Collaboration in turn requires leadership and vision. We make no specific recommendations about the form of leadership structures or the precise arrangements for taking forward implementation. These are matters for the sector to determine if it is to embrace the arrangements fully. They could build on existing arrangements, but need to engage and motivate all parts of the sector, including the workforce. Leadership should also embrace the important relationship between site operators and the surrounding communities, businesses and the local authorities.¹⁴ This needs to be characterised by openness and transparency. The recommendations can also be applied to other sectors. The Competent Authority should actively encourage and support the development of robust arrangements for continuing leadership in the sector, and other sectors as necessary.

¹⁴ We intend to return to this point in our recommendations for emergency preparedness and response.

Recommendation 23 The sector should set up arrangements to collate incident data on high potential incidents including overfilling, equipment failure, spills and alarm system defects, evaluate trends, and communicate information on risks, their related solutions and control measures to the industry.

Recommendation 24 The arrangements set up to meet Recommendation 23 should include, but not be limited to, the following:

- ▼ thorough investigation of root causes of failures and malfunctions of safety and environmental protection critical elements during testing or maintenance, or in service;
- ▼ developing incident databases that can be shared across the entire sector, subject to data protection and other legal requirements. Examples¹⁵ exist of effective voluntary systems that could provide suitable models;
- ▼ collaboration between the workforce and its representatives, dutyholders and regulators to ensure lessons are learned from incidents, and best practices are shared.

Recommendation 25 In particular, the sector should draw together current knowledge of major hazard events, failure histories of safety and environmental protection critical elements, and developments in new knowledge and innovation to continuously improve the control of risks. This should take advantage of the experience of other high hazard sectors such as chemical processing, offshore oil and gas operations, nuclear processing and railways.

¹⁵ Such as HSE's Offshore Hydrocarbon Releases Database and the Rail Safety and Standards Board's National Incident Reporting System, NIR-Online.

Annex 1

Terms of reference and progress

This annex sets out the eight terms of reference for the Investigation and explains the progress that is being made towards accomplishment of each of them.

1 To ensure the thorough investigation of the incident, the factors leading up to it, its impact both on and off site, and to establish its causation including root causes

The Board has published three progress reports from the Investigation Manager. This was followed by the Board's initial report on 13 July 2006, which summarised the three preceding reports and set out the Board's four main areas of concern. These have revealed the main facts of the incident, but have not speculated on why control of the fuel was lost. The explosion mechanism, ie the means by which unexpectedly high overpressures were generated, is subject to significant further investigation. Wider expert consultation has been undertaken on whether and what further research may be required and this is explained in this report.

The criminal investigation is pursuing all reasonable lines of inquiry into the facts and causes of the incident to enable the Competent Authority (HSE and the Environment Agency) to take a view on legal proceedings.

2 To identify and transmit without delay to dutyholders and other appropriate recipients any information requiring immediate action to further safety and/or environmental protection in relation to storage and distribution of hydrocarbon fuels

The Competent Authority issued a Safety Alert to around 1100 COMAH dutyholders on 21 February 2006. Special attention was paid to 108 fuel depot owners storing COMAH quantities of fuel in Great Britain, seeking a review of arrangements for detecting and dealing with conditions affecting containment of fuel. Most dutyholders responded to the alert by the Easter deadline. Meanwhile, the Competent Authority visited all 108 depots to follow up the alert. An interim report was published on 13 June 2006 and is available at www.hse.gov.uk/comah/alert.htm.

The Environment Agency issued further advice to its inspectors to investigate secondary (bundling) and tertiary (drains and barriers) containment at depots in England and Wales in response to the Second progress report. The Environment Agency continues to monitor the effects of Buncefield on the surrounding environment and to issue updates on its website, www.environmentagency.gov.uk. The initiative is being handled separately for Scotland by the Scottish Environment Protection Agency, with joint inspections undertaken with HSE covering primary, secondary and tertiary containment, and management systems. However, it is understood that an overall view of the situation in Britain will be available following the publication of this report by the Buncefield Board.

On 16 June 2006 investigators served two Improvement Notices on the manufacturers of the high level alarm switch installed on Tank 912, having identified a potential problem at other sites related to the setting of the switch for normal operations following testing. This was followed up by a Safety Alert from HSE on 4 July 2006 alerting operators relying on such switches of the potential problem.

The Chairman of the Buncefield Board wrote to the Chief Executive of the Health Protection Agency on 3 July 2006 enquiring into progress with informing regional resilience groups of early lessons learned from Buncefield, focusing on public health issues in the immediate aftermath of a major airborne incident, following up with a meeting December 2006. HPA is assisting the Board with its recommendations for improving emergency preparedness and response to major incidents which is likely to be the subject of the next report from the Board.

3 To examine the Health and Safety Executive's and the Environment Agency's role in regulating the activities on this site under the COMAH Regulations, considering relevant policy guidance and intervention activity

Work is progressing steadily on both parts of the review, concerning respectively HSE's and the Environment Agency's prior regulatory activities at Buncefield. The full findings of the review will be incorporated into the Board's final report (see term of reference 8). Immediate important lessons from the examination of the Competent Authority's prior role will be incorporated as appropriate into the lessons learned programme under term of reference 5.

4 To work closely with all relevant stakeholders, both to keep them informed of progress with the Investigation and to contribute relevant expertise to other inquiries that may be established

The ongoing impact on residents and businesses of the Buncefield incident has been reported in the three progress reports and in the initial report in which, in Part 2, the Board set out its main areas of concern. The Board has maintained an active interest in releasing as much new information as possible to the community and its representatives, such as the local MP Mike Penning, to assist in understanding the events of 11 December 2005, and to maintain public confidence that progress is being made with the Investigation. As has been reported previously, residents and businesses continue to show remarkable resilience in the difficult aftermath to the Buncefield incident. Dacorum Borough Council in particular, but also St Albans and Hertfordshire Councils, have performed extremely effectively in very difficult circumstances, and have supported the Board in its engagement with residents and businesses, as has Mike Penning MP.

The Board has also kept key Government stakeholders informed of the Investigation's progress, and has maintained its interest in developments that have taken place since Buncefield to help manage the aftermath and support a return to normality for residents and businesses.

The Board has engaged with all the public sector agencies involved in the emergency response to Buncefield and has met with a number of the key agencies, particularly the Category 1 (Gold) responders. This is not an issue in which the Board has primary responsibility but, as reported in this Initial Report, the Board is giving further consideration to emergency response and emergency preparedness issues, and will say more on this in its report on emergency preparedness and response.

The Buncefield Major Incident Investigation made presentations to two multiagency debriefing sessions on 21 and 28 June 2006 to inform regional resilience groups around Britain of the response to the Buncefield incident.

5 To make recommendations for future action to ensure the effective management and regulation of major accident risk at COMAH sites. This should include consideration of off-site as well as on-site risks and consider prevention of incidents, preparations for response to incidents, and mitigation of their effects

Staff seconded from HSE, the Environment Agency and the Health Protection Agency are assisting the Investigation Manager and the Board to make sensible, practical and affordable recommendations for improvements in the light of the Buncefield incident. Key workstreams are in environmental protection; land use planning; fire and explosion mechanisms; control and instrumentation; human and organisational factors; health; emergency response and preparedness; and regulatory impact.

This report, making recommendations for the design and operation of Buncefield-type sites, is the first report under this term of reference. HSE has convened an industry chaired task group (the Buncefield Standards Task Group) that includes the Environment Agency and the Scottish Environment Protection Agency, to also consider design and operation issues in parallel with the Board's work. This initiative has been welcomed by the Board in this report.

Work is advanced in producing recommendations on emergency preparation for, and response to, extreme events such as Buncefield. This work is supported by an immense amount of work undertaken by other agencies such as Hertfordshire Resilience, Hertfordshire Fire and Rescue Service, and the Health Protection Agency. The Board intends to join together the many strands of this subject, including issues concerning support to communities and businesses in the aftermath of an extreme incident.

The Board is close to recommending suitable arrangements for further research and modelling of explosion mechanisms in flammable vapour clouds.

HSE has completed its initial work on changes to land use planning advice and has issued a public consultation document seeking views by 22 May 2007 (see <http://hse.gov.uk/consult/condocs/cd211.htm>). The Board will be setting out its own views to the consultation document in due course. HSE is also working closely with a Cabinet Office led team on applying new knowledge of risks to society in the planning system. The Health Protection Agency is consulting key agencies to improve public health advice and support during significant pollution events.

6 To produce an initial report for the Health and Safety Commission and the Environment Agency as soon as the main facts have been established. Subject to legal considerations, this report will be made public

This element is discharged by the publication of the Board's initial report on 13 July 2006.

7 To ensure that the relevant notifications are made to the European Commission

A report from the Environment Agency and HSE was made to the European Commission on 10 March 2006. Subsequently, the Environment Agency declared Buncefield a major accident to the environment (MATTE), and the Competent Authority has recently reported this to the European Commission.

8 To make the final report public

The timing for the publication of the final report remains uncertain and is of course linked to progress on the main terms of reference and to any decision on any criminal proceedings that might be considered. The possibilities include a further interim report or reports; decisions must necessarily depend on the timing of developments and consideration of the public interest.

Annex 2

Members of the independent Board

The Rt. Hon. Lord Newton of Braintree has been a life peer since 1997 after spending 23 years as a Conservative Member of Parliament for Braintree, Essex. From 1982 to 1988 he held ministerial positions at the Department of Health and Social Security. In 1988 he joined the Cabinet as Chancellor of the Duchy of Lancaster and Minister at the DTI. He then held the post of Secretary of State for Social Security from 1989 to 1992 when he was appointed Leader of the House of Commons, which he held until 1997. In 2002 he chaired the Committee that reviewed the operation of the Anti-Terrorism, Crime and Security Act 2001.

Professor Dougal Drysdale is one of the leading international authorities in Fire Safety Engineering. He was the Chairman of the International Association of Fire Safety Science until September 2005 and is currently the editor of the leading scientific journal in the field, Fire Safety Journal. His wide range of research interests includes the ignition characteristics of combustible materials, flame spread and various aspects of fire dynamics. He is a Fellow of the Royal Society of Edinburgh and a Fellow of both the Institution of Fire Engineers and the Society of Fire Protection Engineers.

Dr Peter Baxter is a Consultant Physician in Occupational and Environmental Medicine at Cambridge University and Addenbrooke's Hospital, Cambridge. In the past he has advised the Government on the impacts on public health relating to air quality standards, major chemical incidents, natural disasters and climate change.

Taf Powell is Director of HSE's Offshore Division. He graduated in Geology and Chemistry from Nottingham University. His oil field career has been split between working in the UK and abroad in offshore exploration and development and regulation of the sector in licensing, well operations, policy and safety regulation. In 1991 he joined HSE's Offshore Division from BP and started work to develop the new offshore regulatory framework, one of Lord Cullen's recommendations following his inquiry into the Piper Alpha disaster. As HSE's Operations Manager, based in Aberdeen, he then led inspection teams and well engineering specialists responsible for enforcing the new regulations until 2000 when he took up his current role.

Dr Paul Leinster is Director of Operations at the Environment Agency. Up until March 2004 he was the Director of Environmental Protection, having joined the Agency in 1998. Prior to this he was the Director of Environmental Services with SmithKline Beecham. Previous employers also include BP International, Schering Agrochemicals and the consultancy firm Thomson-MTS where he was Managing Director. Paul has a degree in Chemistry, a PhD in Environmental Engineering from Imperial College and an MBA from the Cranfield School of Management. Paul has worked for 30 years in the health and safety and environmental field.

David Ashton is Director of HSE's Field Operations North-West and Headquarters Division. He joined HSE in 1977 as an inspector in the west of Scotland where he dealt with a wide range of manufacturing and service industries, including construction, engineering and the health services. In 1986 he joined Field Operations HQ to deal with machinery safety. He then held the post of Principal Inspector of manufacturing in Preston for two years, before being appointed as a management systems auditor to examine offshore safety cases in the newly formed Offshore Division. In 1993 he became Head of HSE's Accident Prevention Advisory Unit, looking at the management of health and safety in organisations. Between 1998 and 2003 David was HSE's Director of Personnel, before being appointed to his current position.

Annex 3

Rationale for Recommendation 3 – Independent and automatic storage tank overflow prevention

1 It is common practice to employ an ultimate high level detection system to detect when the liquid in a storage tank has reached a level beyond which any further filling is likely to result in an overspill of liquid unless suitable averting action is taken. The benefit of such a system being independent of the tank gauging system is recognised in the current standards and guidance for storage tank operations.^(refs 4,7,8) However, the current standards and guidance (other than in the case of reference 2 for unattended facilities only) do not require the overflow prevention system to be automatic.

2 Nevertheless, the benefit of an automatic overflow prevention system is recognised by the Energy Institute^(ref 7) which says that ‘where tank filling operations are complex, such as with tanks fed by cross-country pipelines, consideration should be given to the fitting of high level alarms and devices for automatically cutting off the supply. Ideally automatic cut-off devices should be high integrity and independent of any normal measuring alarm or system.’ We also note that a draft revision to API Code 2350 considers requiring automatic independent shutdown systems to control filling of tanks at Buncefield type sites.

3 The benefit of an automatic overflow prevention system stems from the diversity that such a system provides in combination with the tank gauging system. Without such diversity the combination of the systems is vulnerable to common cause failures as they would both rely on human operators. For example, abnormal events may distract or disable the operators such that they fail to properly control the tank gauging system and then also fail to respond to the ultimate high liquid level alarm in time to prevent overfilling. Such common cause failures can significantly degrade the overall integrity of the gauging and overflow prevention systems such that the likelihood of an overspill is much higher than would be evaluated by considering the systems as being independent.

4 It is our considered view, having consulted with experts in the industry, that the assurance for the overall integrity of containment provided by the diversity of manual and automatic systems justifies overflow prevention systems being automatic in Buncefield like sites. This is particularly so given the potentially high consequences for both safety and the environment, together with the associated societal concern, that may result from a substantial overspill of petrol or similar substance in such sites.

5 We consider that a further benefit of an automated overflow prevention system stems from the greater confidence in testing, inspection, verification and auditing that competently engineered arrangements allow for, compared with that afforded by manually operated systems.

6 However, even with such an approach it remains vital that both the gauging system and the overflow prevention systems are maintained in effective working order. It also remains important to properly evaluate the required safety integrity level (SIL) for the automated overflow prevention system, taking into account the associated risks in line with Recommendation 1 of this report. This will ensure a low enough level of residual risk taking into account a realistic view of the reliability of the systems.

7 We consider that the preferred way of achieving automated overfill prevention will include the use of positively isolating valves such as remotely operated shut-off valves (ROSOVs) or emergency shutdown valves (ESDVs).^(ref 9) Such valves are designed to achieve and maintain rapid isolation of plant items and thereby prevent further movement of liquid that could result in overfilling of a tank. However, we recognise that the use of ROSOVs or ESDVs may not be appropriate in some applications, such as filling from a ship or train, or from a refinery process. In such applications it may be more appropriate to employ other or additional control arrangements such as automatic diversion of flow and/or shutdown of a pump. Whatever system is selected, the safety integrity level required for that site must not be compromised.

8 In all applications, the desired outcome must be the same. Namely, if petrol (or similar flammable substance) filling at a Buncefield-type site continues after the system has warned operators to take action, but action has not been taken or is not effective, then means that require no further human intervention (ie automatic) should safely stop the tank filling before overflow occurs.

9 We further recognise that certain applications may require the industry, working with the joint Competent Authority, to resolve some practical and technical considerations to achieve what we have stipulated.

Annex 4

Background and supporting material for ‘improved components and systems’ (Recommendation 8)

Alternative means of ultimate high level detection

1 The detection of ultimate high liquid level in storage tanks often relies on a switch mounted on the roof of the tank (or on the uppermost level of the tank wall). This is commonplace within the industry. For example it is illustrated in API RP 2350.^(ref 4) However, the arrangement suffers from a number of disadvantages with regard to safety, namely:

- ▼ the operation of the switch cannot be tested fully in situ other than by raising the liquid level in the tank to the ultimate high level. Any other means of testing will leave a number of potential failure modes uncovered and so leave the switch in a faulty state unbeknown to the operator or maintenance staff. However, such testing itself introduces the possibility of overfilling so must be undertaken under strict supervision. There is often a reluctance to undertake such testing;
- ▼ simple switches do not benefit from ‘on line’ diagnostics. More advanced sensors (such as those based on tuning fork or thermocouple technology) incorporate diagnostics so that all foreseeable failure modes are detected as they occur.

2 The recommendation is intended to encourage the industry to move away from the use of simple level switches for ultimate high level indication and towards the use of more advanced sensors that incorporate ‘on line’ diagnostics and can therefore be considered to be ‘fail safe’. Such sensors are in widespread use and a number are available that have been certified for use in SIL2/3 applications in accordance with BS EN 61511.

3 The second part of this recommendation is that the means of ultimate high level detection should not rely on components ‘internal to the storage tank’. Reliance on such internal components will always be problematic from a safety viewpoint as access to the inside of the tank for inspection and maintenance will be very limited. It also means that a ‘wet test’ of the switch can only be carried out by filling the tank to the ultimate high level. While such a test could possibly be carried out safely under controlled conditions, there would be significant difficulties in ensuring safety at all times with such an approach.

4 A reasonably practicable alternative solution may be the use of a small external tank tapped into the main tank through a small bore pipe at the ultimate high level. The ultimate high level sensor would be fitted to this external tank such that the ‘overspill’ from the main tank is sensed. Initial considerations suggest that such an approach is feasible. It appears to offer a number of significant benefits. The setting of the ultimate high level would be determined by the physical position of the tapping. This would not be vulnerable to unintended changes. Access to the tank, especially if fitted adjacent to the existing stairway, would be relatively easy and wet testing of the level sensor would be possible without the need to overfill the main tank. These are significant benefits and worthy of further consideration. The practicalities of fitting such an external tank and the associated instrumentation and cabling will also need to be considered. It may be that the

tapping could be made without the need to empty the main tank, although this would need to be confirmed. This would significantly reduce the installation costs. The potential benefits on the face of it justify a recommendation to encourage the industry to explore this approach further.

Increased dependability of tank level gauging systems

5 Tank gauging systems often employ mechanical servo gauges to sense the liquid level. However, such gauges appear to be vulnerable to a number of potential failure modes.

6 This recommendation is intended to encourage the industry to make effective use of the facilities provided in state-of-the-art tank gauging systems to reconcile the indications of product level in tanks with all available information such as product movement requests, pipeline flow measurements, temperature, etc. In this way it may be arranged that the failure of a single element of the system, such as a servo gauge, is detected and the operators alerted before a hazardous situation develops or before a demand is placed on the overfill prevention system.

7 A further contribution to enhanced dependability may result from the use of modern electronic gauge sensors, for example based on radar technology. Electro-mechanical servo gauges are intricate devices vulnerable to many failure modes. Electronic sensors eliminate the failure modes associated with mechanical components and may offer a higher reliability alternative. Such devices are readily available.

Annex 5

High reliability organisations (Recommendations 19-22)

1 A ‘high reliability organisation’ (HRO) is a robust organisation with a strong safety culture that has a high probability of achieving safe, reliable and quality performance over a long period of time.

Background

2 Since the early 1980s studies have been made of organisations that operate ‘high-hazard, low-risk’ technologies at very high levels of reliability,^(refs 10-13) examples are in the air traffic control sector, and on aircraft carriers. The manufacturing and banking sectors also contain examples of companies that have elected to build HROs that are significantly in advance of their peer groups. The studies show that safe operation is not just a matter of compliance with various regulations, codes and standards, but also crucially depends on organisational design and culture. HROs have developed a culture of reliability to drive the business (including high productivity), without sacrificing the drive for improvement or the capability to change.

Culture

3 The ethos of a HRO is based on the prevention of unplanned events (including accidents) through good organisational design and management. The culture of a HRO is one that expects its organisation and sub-systems to fail and works very hard to avoid failure and to minimise its impact. This preoccupation with the possibility of failure leads to a continual state of ‘mindfulness’ combined with a strong desire to be a ‘learning organisation’. High reliability organisations actively seek to know what they do not know, design systems to make all knowledge relating to a problem available to everyone in the organisation, learn quickly and efficiently, train staff to recognise and respond to system abnormalities, empower staff to act, and design redundant systems to catch problems early. Maintenance and proof testing are optimised to increase knowledge and to raise productivity to very high levels through avoidance of unplanned interruptions of which major accidents are the extreme examples.

Characteristics

4 Frequently cited characteristics of high reliability organisations include:

- ▼ **Extensive process auditing.** The organisation will have an established system for monitoring compliance with procedures, and also the efficacy of the procedures themselves. Audits will be designed to identify both expected and unexpected safety problems. There will be robust follow up on actions and problems identified in earlier audits. Regular safety drills and equipment testing will be part of the process auditing system.
- ▼ **Reward and recognition.** Organisational reward systems have powerful influences on the behaviour of individuals in them. HROs will have reward systems that drive the desired behaviours and value the contribution of all in the organisation. For instance full and accurate reporting of incidents, and exemplary care of work equipment will be valued more than ‘zero reported lost time incidents’ (which can encourage competitive under-reporting). They will also be aware that punitive measures may reward behaviour that hides results or redirects blame.

- ▼ **Higher quality standards.** HROs will maintain high quality standards and avoid quality degradation as core values. This will involve regular evaluation of the organisation's performance, capabilities and goals.
- ▼ **Perception of risk.** The HRO will be aware of all risks and, importantly, the significance of each key risk and suitable (but not excessive) control measures will be in place.
- ▼ Command and control systems that will include:
 - *Delegated decision-making.* Relevant competent staff will be integrated into the decision-making process.
 - *Redundancy.* Critical protection systems, process technology and personnel responsibilities are protected against predicted failure that can cause process interruptions and hazardous outcomes.
 - *Senior management involvement.* Top managers will be expected to understand and communicate the 'big picture' rather than being involved too much in the detail and 'micromanaging'.
 - *Formal rules and procedures.* Standard operating procedures (SOPs) will be set out and their implementation will be monitored. The SOPs will deal with all main processes, including response to hazards to personnel, the environment and capital assets. SOPs are updated as lessons are learned from abnormal events and systems failures.
 - *Competency.* Particular emphasis will be given to training in safety critical tasks and in continuous improvement in process efficacy.
 - *Needs of front line staff.* Operator training will incorporate hands-on simulation. Communications will be geared to awareness of adverse situations that can arise, and how to deal with them. Positive behaviours are encouraged. Unwanted behaviours are challenged.

Annex 6

BS EN 61511 Functional safety – Safety instrumented systems for the process industry sector

Background

1 BS EN 61511^(refs 14,15,16) is the process industry standard for ‘safety instrumented systems’. Such systems are widely used in the chemical and petrochemical process industries to measure and control process variables (such as liquid levels and temperatures or gas pressures) so as to ensure that the safe working limits of plant items are not exceeded and thereby avoid hazardous events such as loss of containment of flammable or toxic materials. Other common terms for safety instrumented systems (SIS) are ‘emergency shutdown (ESD) systems’, ‘trip systems’, ‘safety interlock systems’ or ‘safety shutdown systems (SSD)’.

2 The standard (comprising three parts) was first published by the International Electrotechnical Commission (IEC) as IEC 61511 in 2003. It was developed by an international working group comprising experts from the chemical and petrochemical industries. As such it represents the worldwide consensus view on how such systems should be engineered to ensure safety. It covers all aspects of the lifecycle of a system from initial specification and design through to installation, operation, maintenance and eventual decommissioning.

3 Member countries of the IEC agree to adopt IEC standards as national standards. IEC 61511 as adopted as the national standard for the UK when it was published by the British Standards Institution (BSI) as BS IEC 61511 in 2003. Subsequently, the standard was adopted by the European standardisation body for Electrotechnical matters, CENELEC, and is now published by BSI as BS EN 61511. The standard has similarly been adopted by all member countries of the IEC. For example, in the USA it is published as ANSI/ISA-84.00.01-2004.

Principles of BS EN 61511

4 The principles of BS EN 61511 were established by the generic standard for functional safety, BS EN 61508.^(ref 17) The overall aim is to ensure that the performance of a safety instrumented system, in terms of both the functions it provides and their integrity, is adequate to ensure safety. It defines four levels of safety integrity, SIL1, SIL2, SIL3 and SIL4. The higher the SIL level the higher the associated safety level and the lower the probability that the system will fail to perform properly. The required SIL is determined by a hazard and risk assessment taking into account any measures that reduce the risks associated with the hazard under consideration and the tolerable risk target for the specific application. Generally it is preferred to avoid sole reliance on SIS, particularly in high hazard applications. Consequently, most SIS in the chemical and petrochemical process industries in the UK are specified as SIL1 or SIL2.

Application of BS EN 61511 to overfill protection systems

5 BS EN 61511 has no specific requirements for storage tank overfill prevention systems. However, the principles of the standard are directly relevant and can be readily applied to such systems. Application of the standard will provide a risk-based design target for the SIL of an overfill protection system. It will ensure that the design and installation is adequate to achieve the required SIL and that sufficiently frequent periodic testing of the system is carried out to reduce, so far as is reasonably practicable, the risks of tank overfilling.

6 While the application of BS EN 61511 provides a risk-based target for the integrity of an overfill protection system (recommendation 1), and hence for the reliability of the constituent components, it does not require such systems to be automatic in operation. However, if the overfill protection system relies on human operation, the possibility of human failure remains resulting in common cause failure of both a tank gauging system and its overfill protection system. This possibility is very difficult to quantify but is likely to be a critical factor in determining the likelihood of overfilling. For this reason it is felt necessary to make the additional recommendation (recommendation 3) that overfill protection systems should be automated.

Annex 7

Examples of incidents that have involved loss of primary containment from storage tanks

Records of incidents of this type are held by the companies involved for purposes of monitoring the effectiveness of their health and safety policy. The following table gives some examples of such incidents to illustrate the fact that they should not be considered as ‘rare events’. Data have been compiled by a reputable operator in the USA that indicate that overfilling occurs once in every 3300 filling operations.

Location	Date	Fuel released	Consequence
Jacksonville, Florida, UK	1993	Unleaded petrol/gasoline	190 m ³ released. The spill ignited, leading to a major explosion and fire.
Coryton, UK	1997	Unleaded petrol/gasoline	81 m ³ released. Spill contained within bund – no ignition.
Belgium	2001	Hexene	Approx 90 m ³ released. Spill contained within bund – no ignition.
Sour Lake, Texas, USA	2003	Crude oil	80 m ³ released. Spill contained within bund – no ignition.
Torrance, California, USA	2004	Jet fuel	Approx 10 m ³ released. Contained in bund – no fire or explosion.
Bayonne, New Jersey, USA	2004	Fuel oil	825 m ³ released. Oil ‘contained on tank farm’ – no fire or explosion.
Casper, Wyoming, USA	2004	Unleaded petrol/gasoline	Up to 1270 m ³ released. Spill contained within bund – no ignition.
Rensselaer, NY, USA	2005	Unleaded petrol/gasoline	0.4–4 m ³ released. Spill contained within bund – no ignition.

Table 1 Examples of loss of primary containment from fuel storage tanks

Table 2 contains examples of situations in which the loss of primary containment created circumstances (actual or potential) for environmental damage.

Location	Date	Fuel released	Cause	Consequence
Fawley	1999	Crude oil (400 tonnes)	Corrosion of tank base.	No injuries or off-site effects. All of the oil was recovered from primary containment. ECRA* (major loss of inventory).
Milford Haven	2005	Kerosene (653 tonnes)	Leak from damaged sump escaped through permeable floor of bund.	No injuries, but nearby gardens, farmland, and stream contaminated. All wildlife killed in stream. ECRA (contamination of groundwater).
Antwerp, Belgium	2005	Crude oil (26 000 tonnes)	Catastrophic failure of storage tank as a result of corrosion.	Overtopping of bund wall occurred due to sudden release. No injuries. ECRA (major loss of inventory).
Plymouth Harbour	2005	Kerosene (tonnage uncertain)	Corrosion of the tank base and a permeable bund base.	No injuries. Kerosene entered into the ground.
Coryton	2006	Gas oil (121 tonnes)	Tank overfilled, oil escaped from bund by defective drain valve.	No injuries or harm to the environment.
Poole Harbour	2006	Diesel oil (19 tonnes)	Diesel escaped through damaged base plate and through cracks in concrete bund floor.	No injuries. Pollution of ground but not of the harbour.

* ECRA – European Commission Reportable Accident

Table 2 Loss of primary containment from fuel storage tanks, some with environmental consequences

References

- 1 Buncefield Standards Task Group – Initial Report 2006
(www.hse.gov.uk/comah/buncefield/bstg1.htm)
- 2 *Safety Review Panel ('The Baker Report')* BP US Refineries Independent Safety Review Panel 2007
- 3 BS EN 61511: 2004 *Functional safety. Safety instrumented systems for the process industry sector* British Standards Institution
- 4 API RP 2350 *Overfill protection for storage tanks in petroleum facilities* (Third edition) January 2005
- 5 *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries* HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0
- 6 *Dangerous Substances and Explosive Atmospheres Regulations 2002* SI 2002/2776 The Stationery Office 2002 ISBN 978 0 11 042957 1
- 7 *Model Code of Safe Practice in the Petroleum Industry, Part 2, Design, Construction and Operation of Petroleum Distribution Installations* (Third edition) Energy Institute September 2005
- 8 *The storage of flammable liquids in tanks* HSG176 HSE Books 1998 ISBN 978 0 7176 1470 7
- 9 *Remotely operated shutoff valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice* HSG244 HSE Books 2004 ISBN 978 0 7176 2803 2
- 10 Hofmann D, Jacobs R and Landy F 'High reliability process industries: Individual, micro, and macro organisational influences on safety performance' *Journal of Safety Research* 1995 **26** (3) 131-149
- 11 Reason J *Managing the Risks of organisational accidents* Aldershot, Ashgate 1997 ISBN 978 1 84014 105 4
- 12 Roberts K *New challenges to understanding organisations* Macmillan, New York 1993 ISBN 978 0 02 402052 9
- 13 Weick K and Sutcliffe K *Managing the unexpected: Assuring high performance in an age of complexity* Jossey-Bass, San Francisco 2001
- 14 BS EN 61511-1: 2004 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements* British Standards Institution
- 15 BS EN 61511-2: 2004 *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of BS EN 61511-1* British Standards Institution

16 BS EN 61511-3: 2004 *Functional safety – Safety instrumented systems for the process industry sector – Part 3: guidance for the determination of the required safety integrity levels* British Standards Institution

17 BS EN 61508-1: 2002 *Functional safety of electrical/electronic/programmable electronic safety-related systems* British Standards Institution

Glossary

API American Petroleum Institute. It is the American national trade association for the petroleum industry, but it has an increasingly collaborative stance with other bodies such as BSI. API produces a number of guides to standards and recommended practices. Of interest is API Recommended Practice 2350 *Overfill protection for storage tanks in petroleum facilities* which is currently being reviewed

BSI Formerly British Standards Institution, now the BSI Group, it was founded in 1901 as the Engineering Standards Committee, it is now diversified into making standards, certifying management systems, product testing and other engineering services related to quality

bund An enclosure designed to contain fluids should they escape from the tank or vessel inside the bund, as well as any additional materials added to the container area such as firefighting water and foam, etc

Buncefield Standards Task Group The joint Competent Authority/industry standards working group set up to review safety and environmental protection standards at fuel storage sites following the Buncefield incident. The Task Group published its initial recommendations on 12 October 2006

CENELEC European Committee for Electrotechnical Standardisation

COMAH See Control of Major Accident Hazards Regulations 1999

COMAH site A site to which the Control of Major Accident Hazards Regulations 1999 apply

Competent Authority The Control of Major Accident Hazards Regulations (COMAH) are enforced by a joint Competent Authority comprising the Health and Safety Executive (HSE and the Environment Agency in England and Wales, and HSE and the Scottish Environment Protection Agency in Scotland

Control of Major Accident Hazards Regulations 1999 The main aim of these Regulations is to prevent and mitigate the effects of those major accidents involving dangerous substances, such as chlorine, liquefied petroleum gas, and explosives which can cause serious damage/harm to people and/or the environment. The Regulations treat risks to the environment as seriously as those to people. They apply where threshold quantities of dangerous substances identified in the Regulations are kept or used

dutyholder In the context of this report, any person or organisation holding a legal duty – in particular those placed by the Health and Safety at Work etc Act, the Management of Health and Safety at Work Regulations, and the COMAH Regulations

Environment Agency The Environment Agency is the lead regulator in England and Wales with responsibility for protecting and enhancing the environment. It was set up by the Environment Act 1995 and is a non-departmental public body, largely sponsored by the Department for Environment, Food and Rural Affairs and the National Assembly for Wales

firefighting pumps The pumping equipment, normally permanently installed in a pumphouse to move water around the site during fire fighting operations

firewater Water stored for use during, and used during, firefighting operations

firewater lagoon An artificial pond that principally stores water intended for firefighting operations

flashpoint The lowest temperature at which a liquid gives off sufficient vapour to form a flammable mixture

hazard Anything with the potential to cause harm

Health and Safety Commission The Health and Safety Commission is a statutory body, established under the Health and Safety at Work etc Act 1974, responsible for health and safety regulation in Great Britain

Health and Safety Executive The Health and Safety Executive is a statutory body, established under the Health and Safety at Work etc Act 1974. It is an enforcing authority working in support of HSC. Local authorities are also enforcing authorities under the Health and Safety at Work etc Act 1974

high reliability organisations Robust organisations with a strong safety culture that have a high probability of achieving safe and reliable performance. More detail is given in Annex 5

high integrity systems Systems that are designed and maintained so that they have a high probability of carrying out their intended function. Safety instrumented systems having safety integrity levels in the range SIL1 to SIL4 are regarded as high integrity systems

HSC See Health and Safety Commission

HSE See Health and Safety Executive

IEC International Electrotechnical Commission

independent overflow protection system A system that detects when the liquid in a storage tank has reached a level where continued further filling will result in loss of containment and acts to prevent further filling in time to prevent such loss of containment. Where such systems are automatic they do not rely on any human operator action

kiloPascal Pascals (Pa) are the unit of pressure in the International System of Units (SI). A kiloPascal (kPa) is equal to 1000 Pa. Although bar are not units within SI, they are sometimes used as units to measure atmospheric pressure. 1 kPa = 10 bar

major accident to the environment DEFRA has established threshold criteria defining a 'major accident to the environment' (MATTE), based on Schedule 7 (part 1) of the Control of Major Accident Hazards Regulations 1999. The Environment Agency, using these criteria, has determined that the Buncefield incident is a MATTE, and the Competent Authority has recently reported this to the European Commission

manual emergency switches Simple and robust push switches that will initiate emergency action such as shutting down pumps or interrupting process operations, and which are located at strategic and accessible locations around the site

MATTE See major accident to the environment

overpressure For a pressure pulse (or blast wave), the pressure developed above atmospheric pressure

primary containment The tanks, pipes and vessels that normally hold liquids, and the devices fitted to them to allow them to be safely operated

pumphouse In the context of this report, the structure enclosing the pumping equipment used to move water around the Buncefield site prior to the incident. It principally stored water intended for firefighting operations

risk The likelihood that a hazard will cause a specified harm to someone or something

Safety Alert Where the Competent Authority considers that an issue poses significant risk, it can choose to issue a Safety Alert to operators of COMAH sites informing them of the issue and possibly requiring them to undertake certain activity

safety integrity level (SIL) A safety integrity level (SIL) is a measure of safety system performance, in terms of the probability of failure on demand. There are four discrete integrity levels, SIL 1-4. The higher the SIL level, the higher the associated safety level and the lower the probability that a system will fail to perform properly

Scottish Environment Protection Agency The public body that is responsible for the protection of the environment in Scotland

secondary containment Enclosed areas around storage vessels (often called bunds), created usually by concrete or earth walls. Their purpose is to hold any escaping liquids and any water or chemicals used in firefighting

SEPA See Scottish Environment Protection Agency

tertiary containment The site surface and associated drainage, boundary walls, roads, containment kerbs and any features such as road humps that can provide some retention of liquids. Proper design of drainage systems will limit loss of product out of the site and prevent lost product permeating into the ground with the potential risk that it can migrate to groundwater, or contaminate surface waters and land

ultimate high level switch Part of the system to prevent overflowing of the tank, the ultimate high level switch is an independent mechanism which should be triggered when the 'ultimate high level' (ie the specified maximum capacity) is reached in a tank to which it is fitted, both causing an alarm to sound and shutting down the supply of fuel to the tank

Further information

Useful links

Buncefield Major Incident Investigation

Marlowe Room, Rose Court 2 Southwark Bridge London, SE1 9HS

Tel: 020 7717 6909 Fax: 020 7717 6082

E-mail: buncefield.inforequest@hse.gsi.gov.uk

Web: www.buncefieldinvestigation.gov.uk

Community/Business support

Dacorum Business Contact Centre Tel: 01442 867 805

Business Link Helpline Tel: 01727 813 813

Hertfordshire Chamber of Commerce Tel: 01727 813 680

Dacorum Community Trust Mayor's Fund

To apply, call the freephone helpline on 0800 131 3351. Lines are open 9.30 am to 4.30 pm, Monday to Friday

Dacorum Borough Council Tel: 01442 228 000

Web: www.dacorum.gov.uk

Hemel Hempstead Citizens Advice Bureau

19 Hillfield Road, Hemel Hempstead HP2 4AA

Tel: 01442 213368

Local authorities and emergency services

Dacorum Borough Council Tel: 01442 228 000

Web: www.dacorum.gov.uk

(Dacorum Borough Council Digest newsletter, available monthly Dacorum Borough Council Buncefield Update Newsletter)

St Albans District Council Tel: 01727 866 100

Web: www.stalbans.gov.uk

Hertfordshire County Council Tel: 01483 737 555

Web: www.hertsdirect.org

Hertfordshire Fire and Rescue Service

Web: www.hertsdirect.org/yrccouncil/hcc/fire/buncefield

Hertfordshire Constabulary

Web: www.herts.police.uk/news/buncefield/main.htm

Hertfordshire Chamber of Commerce Tel: 01727 813 680

Web: www.hertschamber.com

Government links

Department for Communities and Local Government
Fire and Resilience Directorate
Web: www.communities.gov.uk

Government Office for the East of England
Web: www.goeast.gov.uk

Environment Agency
Web: www.environmentagency.gov.uk

Department of Trade and Industry
Oil and Gas Directorate
Web: www.og.dti.gov.uk

Health and Safety Executive
Hazardous Installations Directorate
Web: www.hse.gov.uk/hid

Control of Major Accident Hazards
Web: www.hse.gov.uk/comah

Department for the Environment, Food and Rural Affairs
Web: www.defra.gov.uk

Health Protection Agency
Web: www.hpa.org.uk

Food Standards Agency
Web: www.food.gov.uk

Drinking Water Inspectorate
Web: www.dwi.gov.uk

Scottish Environment Protection Agency
Web: www.sepa.ork.uk

Buncefields Standards Task Group (BSTG)
Chair: Ken Rivers Tel: 0151 951 4078

Industry links

United Kingdom Petroleum Industry Association (UKPIA)
Tel: 020 7240 0289 Web: www.ukpia.com

Chemical Industries Association
Tel: 020 7834 3399 Web: www.cia.org.uk

Three Valleys Water
Tel: 0845 782 3333 Web: www.3valleys.co.uk

United Kingdom Onshore Pipeline Operators' Association (UKOPA)
Tel: 01773 852003 Web: www.ukopa.co.uk

Tank Storage Association
Tel: 01244 335627 Web: www.tankstorage.org.uk

Investigation reports

Buncefield Major Incident Investigation:

- ▼ Progress Report, published 21 February 2006
- ▼ Second Progress Report, published 11 April 2006
- ▼ Third Progress Report, published 9 May 2006
- ▼ Initial Report, published 13 July 2006

Available from www.buncefieldinvestigation.gov.uk

DEFRA: *Initial review of Air Quality aspects of the Buncefield Oil Depot Explosion*
www.defra.gov.uk/environment/airquality/buncefield/buncefieldreport.pdf

Buncefield: Hertfordshire Fire and Rescue Service's review of the fire response
Hertfordshire Fire and Rescue Service November 2006 ISBN 978 0 11 703716 8

Angus Fire, Buncefield Oil Terminal Incident December 2005: Review of part played by Angus Fire and lessons learned www.angusfire.co.uk

Other related reports/information

East of England Development Agency – report by SQW, Economic Developments Consultants on: *The Buncefield Oil Depot Incident: Economic and Business Confidence Impact Study*, June 2006 www.eeda.org.uk

Swiss Fire Service: *Quick Look Report – Buncefield Fire 11 December 2005*

Buncefield social impact report Decorum Borough Council January 2007
www.decorum.gov.uk/default.aspx?page=4191

Contract research reports for HSE

WS Atkins Science and Technology: *Derivation of fatality probability functions for occupants of buildings subject to blast loads Phases 1, 2, & 3 147/1997 and Phase 4 151/1997*

Biomedical Sciences Chemical and Biological Defence Sector Defence Evaluation and Research Agency: *Review of blast injury data and models 192/1998*

Available from: www.hsebooks.com

Government Advisory Bodies

Committee on mutagenicity of chemicals in food, consumer products and the environment (COM)

Committee on carcinogenicity of chemicals in food, consumer products and the environment (COC)

Committee on toxicity of chemicals in food, consumer products and the environment (COT)

www.advisorybodies.doh.gov.uk/coc/

