Safety and environmental standards for fuel storage sites

Buncefield Standards Task Group (BSTG) Final report

Contents

Foreword

How industry responds to incidents such as Buncefield and how the regulators respond on behalf of the public is a measure of our society. A decisive and dynamic response with all parties co-operating is the product of a democratic and advanced society.

If there is a serious incident then everybody, including the public, the company directly involved and any company in the same or similar sectors, suffers consequences to a greater or lesser extent. It follows that all companies have a vested interest in ensuring that these incidents do not occur. Stakeholders have a right to expect compliance with a minimum set of standards and expectations from everybody in a particular sector and compliance with a higher set of standards for specific situations involving higher than normal risks.

Shortly after the Buncefield incident, the Buncefield Standards Task Group (BSTG) was formed consisting of representatives from the Control of Major Accident Hazards (COMAH) Competent Authority and industry, with the aim of translating the lessons from Buncefield into effective and practical guidance that industry would implement as rapidly as possible. This also facilitated a joined-up approach to managing risk across the sector by providing an authoritative benchmark for standards and practices. The intent was to ensure more consistent responses to broadly similar risks. Existing guidance was reviewed and confirmed as industry standards, with extra detail and examples added where necessary, while in other cases new standards were created to close gaps. This report contains all of the recommendations of BSTG including those previously released. A separate report will detail the progress made in complying with the initial recommendations.

In parallel with the BSTG work, the Buncefield Major Incident Investigation Board (MIIB) conducted an investigation into what happened at Buncefield. Information from the MIIB's reports and from safety alerts issued by the Competent Authority was factored into BSTG work as appropriate. In addition, BSTG also considered all the factors that need to go right to prevent such an incident, which helped define further areas for action. In March 2007, the MIIB issued a report *Recommendations on the design and operation of fuel storage sites*.[1] It sets out 25 recommendations to improve safety and environmental performance. Many of these had already been fully addressed by the BSTG's work, although others have only been partially addressed or have yet to be addressed. This lack of an identical match is due to the decision made at an early stage to balance the need for putting improvements in place rapidly with the need to await the MIIB's full recommendations. We believe that BSTG made the right decision, with significant improvements already having been achieved.

One of the guiding principles of BSTG has been that we would be judged on the delivery of improvements, not simply on an intention to deliver. We have achieved much already; however, we are not complacent and realise that much work remains to be completed. Outstanding matters will be taken forward by the Petrochemical Process Standards Leadership Group (PPSLG), which replaces BSTG, whose working life ends with the publication of this report. PPSLG will also oversee the monitoring of and reporting on compliance with all of their recommendations, as well as those of BSTG.

I believe that the way in which industry and regulator have come together to co-create and deliver action to prevent a Buncefield-type incident is a model for the future. PPSLG will continue the approach of industry and regulator being 'aligned but not joined', whereby we are committed to delivering timely and appropriate agreed action through mutual challenge and understanding of our particular perspectives. Delivery is an essential part of building trust upon which this approach depends. Critically, success requires us to 'say what we will do' and 'do what we say'.

Please read this report and turn its recommendations into action. Doing so may well prevent you and others from suffering the adverse consequences, whether to people or the environment, of an incident.

Ken Rivers
Chair
Buncefield Standards Task Group
24 July 2007

Introduction

1 The purpose of this report is to specify the minimum expected standards of control which should be in place at all establishments storing large volumes of petroleum and similar products capable of giving rise to a large flammable vapour cloud in the event of a loss of primary containment. Although in the main aimed at the operators and regulators of major fuel facilities, parts of the guidance in this report should be applied to other enterprises managing major hazards. To ensure focused and timely follow-ups we have limited our considerations to tanks containing petrol as defined in paragraph 7. It is possible that a limited number of other substances (with specific physical properties and storage arrangements) will be drawn into scope in the future.

2 This report is our final report and it is in four parts. Part 1 details the actions required of operators, including timescales, and Part 2 contains all of the detailed guidance produced by BSTG, including for completeness the guidance from our initial report. Part 3 sets out work in progress, ie work that BSTG has started but is yet to complete, and Part 4 provides a comparison with the work of BSTG and the MIIB report *Recommendations on the design and operation of fuel storage sites*.[1]

3 Our original intention was to produce this guidance in the form of a route map to existing standards relevant to risk controls at bulk fuel storage sites within scope. Wherever possible we have done this and for convenience simply provided a brief summary of that information. In other areas, where there is an absence of any pre-existing authoritative guidance, we have had to produce guidance from scratch. We have also, on occasion, produced detailed commentary on guidance where appropriate, for example, with regards to BS EN 61511:2004 *Functional safety. Safety instrumented systems for the process industry sector*.[2]

4 In its report on the design and operation of fuel storage sites, the MIIB recommended that, 'The sector, in consultation with the Competent Authority, needs to build on [the work of BSTG] 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.' It also stated that a key challenge facing the fuel sector is dealing with the issues arising from the Baker Panel Report[3] into the BP Texas City incident, where it was made clear that deficiencies in process safety culture, management and corporate oversight were not limited to BP and that all companies should thoroughly evaluate these for themselves and improve them as necessary.

5 To take forward continued improvements in industry, it is proposed to build on the model developed for BSTG – a small, focused, oversight team to lead, develop and promote improvements to safety and environmental control at fuel storage sites. This new group, the Petrochemical Process Standards Leadership Group (PPSLG), will be supported by dedicated working groups dealing with specific topics. PPSLG will be chaired by a senior member of industry and involve representatives from the United Kingdom Petroleum Industry Association (UKPIA), the Tank Storage Association (TSA), the United Kingdom Onshore Pipeline Operators' Association (UKOPA) and the Chemical Industries Association (CIA), as well as representatives from the Competent Authority. It will lead, develop and promote improvements to the safety and environmental controls and will, in particular:

- demonstrate effective leadership within the sector;
- develop organisational and technical solutions;
- share learning from incidents and good practice;

- drive forward research;
- assist in assuring the process of monitoring compliance with the MIIB's and BSTG's recommendations;
- make further recommendations; and
- take effective account of the findings of the exploration of the explosion mechanism.

6 It is anticipated that all in-scope sites will benchmark their current operation against the guidance in this report. Any gaps should be closed without undue delay. Part 1 of this report gives compliance dates that we consider achievable in most cases. Best endeavours should be made to comply with the timescales. Any site that cannot meet these compliance dates should discuss the reasons with their local Competent Authority inspector.

Scope – sites and activities covered by the guidance

7 Pending the results of work that is currently ongoing, BSTG limited its work to tanks containing material and operating under similar regimes that existed at Buncefield, namely:

- COMAH top- and lower-tier sites, storing:
- gasoline (petrol) as defined in Directive 94/63/EC [European Parliament and Council Directive 94/63/EC of 20 December 1994 on the control of volatile organic compound (VOC) emissions resulting from the storage of petrol and its distribution from terminals to service stations],[4] in:
- vertical, cylindrical, non-refrigerated, above-ground storage tanks typically designed to standards BS 2654,[5] BS EN 14015:2004,[6] API 620,[7] API 650[8] (or equivalent codes at the time of construction); with
- side walls greater than 5 metres in height; and at
- filling rates greater than 100 m^3/hour (this is approximately 75 tonnes/hour of gasoline).

8 Other materials could have the same vapour-forming attributes as gasoline defined above. A key piece of work to be pursued by PPSLG will be to consider widening the scope of materials that this report should apply to. A start has been made on this through joint work undertaken by the Health and Safety Laboratory (HSL) and Shell Global Solutions (SGS) but further work is required.

9 This guidance is issued jointly by:

- Health and Safety Executive (HSE);
- Environment Agency (EA);
- Scottish Environment Protection Agency (SEPA);
- United Kingdom Petroleum Industry Association (UKPIA);
- Tank Storage Association (TSA); and
- United Kingdom Onshore Pipeline Operators' Association (UKOPA).

Part 1: Action required to prevent a further incident – what must go right!

10 This section outlines BSTG's recommendations for action in each key area of control of primary, secondary and tertiary containment. These recommendations are set out in the form of minimum expected good practice. Compliance with these measures will meet minimum legal standards with the Control of Major Accident Hazards Regulations 1999 (COMAH). The recommendations in this report may not be the only way of achieving the minimum expected good practice. There may be other ways that provide equal or better protection. However, if you comply with the recommendations in this report you will be meeting current minimum good practice. Table 1 provides a summary of the following information:

- the BSTG initial[9] and final recommendations; and
- the target dates by which site operators should have implemented any necessary improvements.

11 Operators are expected to meet these timescales. Exceptional reasons as to why they cannot be met should be discussed with the COMAH Competent Authority (CA). The site concerned should also provide a revised time-bound action plan for the remedial work.

12 The remainder of this part sets out the BSTG recommendations in the form of minimum expected standards of good practice.

13 The initial aim of BSTG was to identify good practice as a benchmark for important aspects of risk control to be adopted at relevant sites. In this way industry will ensure that consistent controls are in place to deal with similar levels of risk. It is stressed that the standards set out in this report are considered to be controls consistent with the legal duties of operators of COMAH establishments to take all necessary measures to prevent major accidents and to limit their consequences to persons and the environment. COMAH operators are strongly encouraged to strive for even higher standards wherever possible as one way of demonstrating strong leadership and raising the reliability necessary within their organisations.

14 Detailed guidance on how to meet these recommendations is given in Part 2 to this report. The information is presented in the same order as the recommendations in the MIIB report[1] on the design and operation of fuel storage sites. This will facilitate further additions to this guidance as work progresses to address the MIIB's recommendations.

15 For a number of recommendations there is a requirement to ensure that any changes are incorporated within the safety report. For lower-tier sites, demonstrating that improvements have been made will be achieved in the normal way by having systems and procedures in place at the establishment to deliver the intended outcome.

Table 1 *Summary of action required*

Topic	Completion date
Systematic assessment of safety integrity levels (SILs)	
Control and safety systems for petroleum storage tanks	INITIAL RECOMMENDATION Assessment of the safety integrity level (SIL) requirements for overfill prevention systems against BS EN 61511:2004[2] should have been completed **by the end of June 2007.** Relevant maintenance and testing regimes to meet BS EN 61511:2004[2] should be in place **by the end of November 2007.** Improvements required to achieve the required level of integrity should be in place **by the end of November 2007.**
Incorporating the findings of SIL assessments into COMAH safety reports	NEW RECOMMENDATION Existing safety reports should be reviewed to incorporate a demonstration that: ● the overall systems for tank filling control are of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow; and ● the overall systems for tank filling control meet BS EN 61511:2004[2] **by the end of December 2007**. An appropriate demonstration of compliance should be included in safety reports submitted to the Competent Authority **by the date of the next five-year periodic review of the safety report.**
Protecting against loss of primary containment using high-integrity systems	
Management systems for maintenance of equipment and systems to ensure their continuing integrity in operation	INITIAL RECOMMENDATION Inspection and maintenance systems should already be established. Changes to the testing and maintenance regime resulting from the SIL assessment should be in place **by the end of November 2007.**
Tank overfill prevention: defining tank capacity	INITIAL RECOMMENDATION The capacities of storage tanks should be clearly defined and appropriate safety margins put in place to prevent a release. This action should have been completed **by the end of January 2007.**
Fire-safe shut-off valves	INITIAL RECOMMENDATION The assessment of valves as being fire-safe should have been completed **by the end of April 2007**.
Remotely operated shut-off valves (ROSOVs)	INITIAL RECOMMENDATION The assessment (as per HSG244[10]) of the need for ROSOVs on tank outlets should have been completed **by the end of June 2007.**

Table 1 *Summary of action required (continued)*

Topic	**Completion date**
Testing of overfill protection systems	INITIAL RECOMMENDATION Inspection and maintenance systems **should already be established.** Changes to the testing and maintenance regime resulting from the SIL assessment should be in place **by the end of November 2007.**
Safe management of fuel transfer	INITIAL RECOMMENDATION Adopt the principles for safe management of fuel transfer and develop consignment transfer agreements consistent with these principles. This should have been completed **by the end of January 2007.** NEW RECOMMENDATION Ensure that suitable 'job factors' are provided to facilitate safe fuel transfer; to be reviewed **by the end of December 2007.** INITIAL RECOMMENDATION Companies involved in inter-business transfer of fuel by pipeline should have agreed on the nomenclature to be used for their product types **by the end of January 2007.** INITIAL RECOMMENDATION For ship-to-shore transfers, carry out a terminal-specific review to ensure compliance with the *International Shipping Guide for Oil Tankers and Terminals* (ISGOTT).[11] This should have been completed **by the end of January 2007.** NEW RECOMMENDATIONS Receiving sites to develop procedures for transfer planning and review them with their senders and appropriate intermediates **by the end of December 2007.** Ensure that written procedures are in place, and consistent with current good practice, for safety-critical operating activities in the transfer and storage of fuel **by the end of June 2008.**
Engineering against loss of secondary and tertiary containment	
Leak-tight bunds	NEW RECOMMENDATION Bund wall and floor construction and penetration joints should be leak-tight. **Should already be in place** as good practice.
Fire-resistant bund wall joints	INITIAL RECOMMENDATION Joints in bunds must be capable of resisting fire: improvements should have been completed **by the end of May 2007.**

Table 1 *Summary of action required (continued)*

Topic	**Completion date**
Bund capacity	NEW RECOMMENDATION Bund capacity at existing installations should be a minimum of 110% of the largest contained tank. **Should already be in place** as good practice.
Firewater management and control measures	NEW RECOMMENDATION Site-specific planning of firewater management and control measures should be undertaken with active participation of the local Fire and Rescue Service. To be completed **by the end of June 2008.**
Tertiary containment	INITIAL RECOMMENDATION Assessment of sites and action plans for improvement should have been completed **by the end of January 2007.**
High reliability organisations	
Roles, responsibilities and competence	NEW RECOMMENDATION Identification of roles and responsibilities **by the end of September 2007.** Implement a competence management system **by the end of June 2008.**
Staffing and shift work arrangements	NEW RECOMMENDATION Demonstrate adequate staffing arrangements by the end of March 2008. Ensure that shift work is adequately managed to control risks from fatigue **by the end of June 2008.**
Shift handover	INITIAL RECOMMENDATION This was a priority action that should have been completed **by the end of January 2007.**
Organisational change and management of contractors	NEW RECOMMENDATION Policies and procedures in place **by the end of December 2007.**
Performance evaluation and process safety performance measurement	NEW RECOMMENDATION Ensure suitable active monitoring programme and develop a set of leading and lagging indicators **by the end of December 2007.** Procedures for investigation of incidents and near misses and the audit and review of the control of major accident hazards **should already be in place.**

Table 1 *Summary of action required (continued)*

Topic	**Completion date**
Emergency arrangements	
Principles for emergency arrangements	NEW RECOMMENDATION Arrangements for on-site emergency response implemented **by the end of January 2008.**
On-site emergency plan	NEW RECOMMENDATION Template for the on-site emergency plan completed **by the end of January 2008.**
Firefighting planning and preparation	NEW RECOMMENDATION Firefighting planning and preparations implemented **by the end of January 2008.**

Systematic assessment of safety integrity level requirements

Control and safety systems for petroleum storage tanks

16 Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve. This report uses a layer of protection study (LOPA) to provide a more consistent approach to safety integrity level (SIL) assessment. The study included in Appendix 1 illustrates the LOPA methodology but **it does not present a model solution** that can simply be used by a site. A site-specific assessment must be conducted.

17 For each risk assessment/SIL determination study, operators must be able to justify each and every claim and data used in the risk assessment and ensure that appropriate management systems and procedures are implemented to support those claims. For COMAH top-tier sites this will form part of the demonstration required with the safety report. Of particular importance is the reliability and diversity of the independent layers of protection. To avoid common mode failures extreme care should be taken when claiming high reliability and diversity, particularly for multiple human interventions.

Minimum expected good practice

18 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.

19 Site operators should meet the latest international standards, ie BS EN 61511:2004 *Functional safety. Safety instrumented systems for the process industry sector*.[2]

Incorporating the findings of SIL assessments into COMAH safety reports

Minimum expected good practice

20 COMAH five-year periodic reviews of safety reports should incorporate a demonstration that:

- the overall systems for tank filling control are of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow; and
- the overall systems for tank filling control meet BS EN 61511:2004.[2]

21 Where the SIL assessment results in a change to the safety management system that could have significant repercussions with respect to the prevention of major accidents or the limitation of their consequences, operators of top-tier sites should review their safety reports under the provisions of COMAH regulation 8(c).[12] For the majority of sites it is not expected that a revised safety report is required to be submitted to the Competent Authority before the next five-year review.

Protecting against loss of primary containment using high-integrity systems

Management systems for maintenance of equipment and systems to ensure their continuing integrity in operation

22 The MIIB's third progress report[13] indicated that there was a problem with the tank level monitoring system at Buncefield. An examination of the records for Tank 912 from the automatic tank gauging (ATG) system suggest an anomaly in that the ATG system indicated that the level remained static while approximately 550 m^3/hr of unleaded petrol was being delivered into Tank 912. This section represents interim guidance as further work will be undertaken by PPSLG to develop more detailed guidance on inspection and maintenance of control systems.

Minimum expected good practice

23 Overfill protection systems should be tested periodically to prove that they would operate safely when required.

24 Proof testing should be end to end, incorporate elements of redundancy, and include the detector at the liquid interface and the valve closure element. The test period should be determined by calculation according to the historical failure rate for each component or the system and the probability of failure on demand required to achieve the specified SIL. Records of test results, including faults found and any repairs carried out, should be retained.

25 Procedures for implementing changes to equipment and systems should ensure any such changes do not impair the effectiveness of equipment and systems in preventing loss of containment or in providing emergency response.

Tank overfill prevention: Defining tank capacity

26 To prevent overfill, tanks must have headspace margins to ensure that the intake will be closed off in time. High level alarms and operator or automatic actions must be adequately spaced to respond to a developing overfill situation.

Minimum expected good practice

27 Operating practices, staffing levels and systems must provide effective safety margins to prevent an overfilling release.

28 Tank capacities and appropriate action levels should be set in accordance with this guidance.

29 Tanks should not be intentionally filled beyond the normal fill level.

Fire-safe shut-off valves

30 Each pipe connected to a tank is a potential source of a major leak. In the event of an emergency, it is important to be able to safely isolate the contents of the tank. Isolation valves should be fire safe, ie capable of maintaining a leak-proof seal under anticipated fire exposure.

Minimum expected good practice

31 Fire-safe shut-off valves must be fitted close to the tank on both inlet and outlet pipes. Valves must either conform to an appropriate standard (BS 6755-2 or BS EN ISO 10497),[14] equivalent international standards or be of an intrinsically fire-safe design, ie have metal-to-metal seats (secondary metal seats on soft-seated valves are acceptable), not be constructed of cast iron and not be wafer bolted.

Remotely operated shut-off valves (ROSOVs)

32 In an emergency, rapid isolation of vessels or process plant is one of the most effective means of preventing loss of containment, or limiting its size. A ROSOV is a valve designed, installed and maintained for the primary purpose of achieving rapid isolation of plant items containing hazardous substances in the event of a failure of the primary containment system (including, but not limited to, leaks from pipework, flanges, and pump seals). Valve closure can be initiated from a point remote from the valve itself. The valve should be capable of closing and maintaining tight shut off under foreseeable conditions following such a failure (which may include fire).

33 *Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice* HSG244[10] provides guidance on how to assess the need to provide ROSOVs for emergency isolation.

Minimum expected good practice

34 ROSOVs for the emergency isolation of hazardous substances should be fitted to the outlet pipe tanks in scope where an assessment under HSG244 indicates that such valves should be fitted. ROSOVs for the emergency isolation of hazardous substances should fail safe.

35 Operators of existing sites should review their risk assessments to ensure that an effective assessment has been undertaken following the key stages in HSG244.

Testing overfill protection systems

36 Overfill protection alarms or shutdown systems using high level switches or other two-state detectors may be inactive for long periods and may develop unrevealed faults. Such faults cause the system to fail to danger when required to operate.

Minimum expected good practice

37 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.

Safe management of fuel transfer

38 The initial report of the Buncefield Major Incident Investigation Board[15] identified an issue with regard to safety arrangements, including communications, for fuel transfer. No existing authoritative guidance was found that adequately described this and so a set of principles for safe management of fuel transfer, which includes the adoption of principles for consignment transfer agreements has been developed.

Minimum expected good practice

39 Companies involved in the transfer of fuel by pipeline should:

- adopt the principles for safe management of fuel transfer;
- where one party controls the supply, and another controls the receiving tanks, develop consignment transfer agreements consistent with those principles;
- ensure that suitable 'job factors' are provided to facilitate safe fuel transfer;
- for inter-business transfers, agree on the nomenclature to be used for their product types;
- for ship-to-shore transfers, carry out a terminal-specific review to ensure compliance with the *International Shipping Guide for Oil Tankers and Terminals* (ISGOTT);[11]
- for receiving sites, develop procedures for transfer planning and review them with their senders and appropriate intermediates;
- ensure that written procedures are in place and consistent with current good practice for safety-critical operating activities in the transfer and storage of fuel.

Engineering against loss of secondary and tertiary containment

40 This section represents interim guidance, as PPSLG will undertake further work to develop more detailed guidance on secondary and tertiary containment.

41 While priority 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. The failure of secondary and tertiary containment at Buncefield contributed significantly to the failure to prevent a major accident to the environment (MATTE).

Minimum expected good practice

Bund integrity (leak-tightness)

42 Bund wall and floor construction and penetration joints should be leak-tight. Surfaces should be free from any cracks, discontinuities and joint failures that may allow relatively unhindered liquid trans-boundary migration. As a priority, existing bunds should be checked and any damage or disrepair, which may render the structure less than leak-tight, should be remedied.

Fire-resistant bund joints

43 Joints in concrete or masonry bund walls must be capable of resisting fire. Existing bunds should be modified to meet this requirement. In addition to repairing any defects in bund joints, steel plates should be fitted across the inner surface of bund joints, and/or fire-resistant sealants should be used to replace or augment non-fire-resistant materials.

Bund capacity

44 The minimum capacity for bunds containing tanks in scope at existing installations is 110% of the largest tank.

Tertiary containment

45 Installations where bunds contain tanks within scope are required to assess the requirement for tertiary containment on the basis of environmental risk and to make site action plans for improvement.

Firewater management and control measures

46 Site-specific planning of firewater management and control measures should be undertaken with active participation of the local Fire and Rescue Service, and should include consideration of:

- bund design factors, such as firewater removal pipework, aqueous layer controlled overflow to remote secondary or tertiary containment (for immiscible flammable hydrocarbons);
- recommended firewater/foam additive application rates and firewater flows and volumes at worst-case credible scenarios;
- controlled burn options appraisal; and
- planning/media implications.

High reliability organisations

47 The need for high reliability organisations follows from the 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.

Roles, responsibilities and competence

Minimum expected good practice

48 Operators should ensure that they have:

- clearly identified the roles and responsibilities of all those involved in managing, performing or verifying work in the management of major hazards, including contractors; and
- implemented a competence management system, linked to major accident risk assessment, to ensure that anyone whose work impacts on the control of major accident hazards is competent to do so.

Staffing and shift work arrangements

Minimum expected good practice

49 Operators should ensure:

- they can demonstrate that staffing arrangements are adequate to detect, diagnose and recover any reasonably foreseeable hazardous scenario; and
- that shift work is adequately managed to control risks arising from fatigue.

Shift handover

Minimum expected good practice

50 Operators should set and implement a standard for effective and safe communication at shift and crew change handover in relation to fuel transfer and storage. For top-tier COMAH sites, a summary of the standard should be included in the next revision of the safety report.

Organisational change and management of contractors

Minimum expected good practice

51 Site operating companies should ensure that:

- there is a suitable policy and procedure for managing organisational changes that impact on the safe transfer and storage of fuel, and for retention of corporate memory;
- the policy and procedures ensure that the company retains adequate technical competence and 'intelligent customer' capability when work impacting on the control of fuel transfer and storage is outsourced or contractorised; and
- suitable arrangements are in place for management and monitoring contractor activities.

Performance evaluation and process safety measurement

52 To maintain and improve an effective complex process safety management system relating to fuel transfer and storage, managers must periodically evaluate the system's performance and address any identified deficiencies or opportunities for improvement.[16]

Measuring process safety performance

53 Measuring performance to assess how effectively risks associated with fuel transfer and storage are being controlled is an essential part of a health and safety management system.[12,17] Active monitoring provides feedback on performance before an accident or incident, whereas reactive monitoring involves identifying and reporting on incidents to check the controls are in place, identify weaknesses and learn from mistakes.

Minimum expected good practice

54 Operators should:

- ensure that they have a suitable active monitoring programme in place for those systems and procedures that are key to the control of fuel transfer and storage; and
- develop an integrated set of leading and lagging performance indicators for effective monitoring of process safety performance.

Investigation of incidents and near misses

Minimum expected good practice

55 Operators should ensure they have suitable procedures for:

- identifying incident/near miss potential;
- investigating according to the identified potential;
- identifying and addressing both immediate and underlying causes;
- sharing lessons learnt; and
- tracking remedial actions.

Audit and review

Minimum expected good practice

56 Operators should adopt and implement audit plans defining:

- the areas and activities to be audited, with a particular focus on process safety/control of fuel transfer and storage;
- the frequency of audits for each area covered;
- the responsibility for each audit;
- the resources and personnel required for each audit;
- the audit protocols to be used;
- the procedures for reporting audit findings; and
- the follow-up procedures, including responsibilities.

57 Operators should ensure that they have implemented suitable arrangements for a formal review of arrangements for controlling fuel transfer and storage, including:

- the areas and activities to be reviewed, with a particular focus on process safety/control of major accident hazards;
- the frequency of review (at various levels of the organisation);
- responsibility for the reviews;
- the resources and personnel required for each review; and
- procedures for reporting the review findings.

Emergency arrangements

58 Operators should be aware that the event that they should plan for, with respect to emergency arrangements, is that of a multiple tank fire following an explosion. The emergency systems will need to be capable of operating effectively following such an event.

Principles

Minimum expected good practice

59 Operators should ensure that their arrangements for on-site emergency response and firefighting planning and preparations are drawn up in accordance with the principles for emergency arrangements detailed in the guidance part of this report.

On-site emergency plan template

Minimum expected good practice

60 Operators should ensure that the template for the on-site emergency plan is completed with respect to their site. See ww.hse.gov.uk/comah/buncefield/final.htm.

Firefighting planning and preparation

Minimum expected good practice

61 Operators should ensure that the firefighting planning and preparations are in accordance with the measures detailed in the guidance part of this report.

Part 2: Detailed guidance on standards for the transfer and storage of fuel

62 This part contains detailed guidance on standards that should be applied to all fuel storage sites within scope. These standards should be met within the timescales set out in Part 1 and complied with in full to meet good practice. Compliance with these measures will meet minimum legal standards within the Control of Major Accident Hazards Regulations 1999 (COMAH).[12] The recommendations in this report may not be the only way of achieving the minimum expected good practice. There may be other ways that provide equal or better protection. However, if you comply with the recommendations in this report you will be meeting minimum good practice.

63 Where the MIIB has made additional recommendations on the design and operation of fuel storage sites[1] which have not been fully addressed by BSTG, eg the recommendation for fully automated overfill protection systems, these will form part of the work of PPSLG, which replaces BSTG. A clear indication is given at the start of each section wherever it is envisaged that additional guidance will be provided in future on an issue covered in this Part of the report. Part 3 of this report contains some initial guidance on a number of these additional recommendations, but at this stage it should be considered as work in progress.

Systematic assessment of safety integrity level requirements

Control and safety systems for petroleum storage tanks

64 All overfill prevention systems, including instrumentation, devices, alarm annunciators, valves and components comprising the shutdown system, should be assessed using BS EN 61511:2004,[2] which sets a minimum performance for safety integrity levels (SILs). This includes the following considerations:

- design, installation, operation, maintenance and testing of equipment;
- management systems;
- redundancy level, diversity, independence and separation;
- fail safe, proof test coverage/frequency; and
- consideration of common causes of failures.

65 Systems for a SIL requirement less than 1 are not in scope of BS EN 61511. They may, however, still provide a safety function and a risk reduction of up to a factor of 10 and hence are safety systems and can be a layer of protection. Such systems should comply with good practice in design and maintenance so far as is reasonably practicable.

66 Shut down of product flow to prevent an overfilling should not depend solely upon systems or operators at a remote location. The receiving site must have ultimate control of tank filling by local systems and valves.

67 The normal fill level, high alarm level and high-high alarm/trip level should be set in compliance with the guidance on designating tank capacities and operating levels.

68 Tank level instrumentation and information display systems should be of sufficient accuracy and clarity to ensure safe planning and control of product transfer into tanks.

Operator responsibilities and human factors

69 Monitoring and control of levels, and protection against overfill, may depend on operators taking the correct actions at a number of stages in the filling procedure. These actions may include:

- calculation of spare capacity;
- correct valve line up;
- cross-checks of valve line up;
- manual dipping of tank to check ATG calibration;
- confirmation that the correct tank is receiving the transfer;
- monitoring level increase in the correct tank during filling;
- checks for no increase in level in static tanks;
- closing a valve at the end of a transfer;
- response to level alarm high; and
- response to level alarm high-high.

70 Some of these actions are checks and hence improve safety; some however are actions critical to safety. The probability of human error increases in proportion to the number of critical actions required and hence the human factors associated with operator responsibilities need careful consideration. A useful guide is *Reducing error and influencing behaviour* HSG48.[16] In addition, refer to Appendix 1, the layer of protection analysis worked example included in this guidance.

Risk assessment and SIL determination

71 The operator of a COMAH installation has a duty to review the risk assessment for the installation periodically and take into account new knowledge concerning hazards and developments in standards. Any improvements required by standards such as BS EN 61511 should be implemented so far as is reasonably practicable.

72 Layer of protection analysis (LOPA) is one of several methods of risk assessment and SIL determination; BS EN 61511 Part 3 provides a summary of the method. A LOPA analysis is used in the example in Appendix 1. Other methods described in BS EN 61508[18]/BS EN 61511,[2] eg risk graphs, are equally acceptable for the determination of the system SIL. For a detailed guide on LOPA studies, refer to *Layer of protection analysis*, Centre for Chemical Process Safety of the American Institute of Chemical Engineers.[19]

73 The rules for LOPA studies, in particular, the tests for independence between protection layers and between protection layers and initiating events, should be carefully observed for the analysis to be valid.

Layer of protection analysis (LOPA) methodology

74 The method comprises the following key stages:

- identify the event sequences and failures that can lead to an overfill and estimate the frequency of each initiating event (IE);
- identify the protection layers provided that are capable of independently preventing each IE and derive a probability of failure on demand for each layer;
- apply the appropriate conditional modifiers such as probability of ignition, occupancy and fatality;

- calculate the mitigated overfill event likelihood and compare with the risk tolerability criteria (RTC) for the site; and
- if the calculated event likelihood is greater than the RTC, further risk reduction measures need to be considered as part of a demonstration that the risks have been reduced as low as reasonably practicable (ALARP).

75 Once the LOPA study is completed operators must be able to justify each and every claim and data used in the risk assessment and ensure that appropriate management systems and procedures are implemented to support those claims. For COMAH top-tier sites this will form part of the demonstration required with the safety report. A worked example of a LOPA study can be found at Appendix 1. This illustrates the LOPA methodology but **it does not present a model solution** that can simply be used by a site. A site-specific assessment must be conducted. Of particular importance is the reliability and diversity of the independent layers of protection; to avoid common mode failures extreme care should be taken when claiming high reliability and diversity for multiple human interventions.

Incorporating the findings of SIL assessments into COMAH safety reports

76 The findings of the SIL assessment, using the common methodology, should be included in the COMAH safety report for the site. This should provide sufficient detail to demonstrate that:

- the overall systems for tank filling control are of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow; and
- safety instrumented systems and management systems meet BS EN 61511:2004.

77 The SIL assessment of any control system that relies wholly or in part on any off-site capability to function effectively must demonstrate that the operation of the off-site capability meets the appropriate level of integrity.

Protecting against loss of primary containment using high-integrity systems

Management systems for maintenance of equipment and systems to ensure their continuing integrity in operation

Future work: this section represents interim guidance as further work will be undertaken by PPSLG to develop more detailed guidance on inspection and maintenance of control systems.

78 The MIIB's third progress report[13] indicated that there was a problem with the tank level monitoring system at Buncefield. An examination of the records for Tank 912 from the ATG system suggest an anomaly in that the ATG system indicated that the level remained static while approximately 550 m3/hr of unleaded petrol was being delivered into Tank 912.

79 Overfill protection alarms or shutdown systems using high level switches or other two-state detectors may be inactive for long periods and may develop unrevealed faults. Such faults cause the system to fail to danger when required to operate. Hence overfill protection systems should be tested periodically to prove that they would operate safely when required.

80 Proof testing should be end to end, incorporate elements of redundancy, and include the detector at the liquid interface and the valve closure element. The test period should be determined by calculation according to the historical failure rate for each component or the system and the probability of failure on demand required to achieve the specified SIL. Records of test results, including faults found and any repairs carried out, should be retained.

Management of change

81 The procedures for implementing changes to equipment and systems should ensure any such changes do not impair the effectiveness of equipment and systems in preventing loss of containment or in providing emergency response.

High-integrity, automatic operating overfill prevention systems

Future work: the sector and the Competent Authority plan to address the issue of high-integrity, automatic overfill prevention systems and to issue more detailed guidance on this recommendation. In the meantime, as well as the guidance on SIL assessments, we have developed guidance on defining tank capacities as to assist in the prevention of an overfilling.

Tank overfill prevention: Defining tank capacity

82 To prevent overfill, tanks must have headspace margins that enable the filling line to be closed off in time. High level alarms and operator or automatic actions must be adequately spaced to deal with a developing overfill situation.

Overfill level (maximum capacity)

83 A vital element of any system to prevent overfilling of a storage tank is a clear definition of the maximum capacity of the vessel. This is the maximum level consistent with avoiding loss of containment (overfilling or overflow) or damage to the tank structure (eg due to collision between an internal floating roof and other structures within the tank, or for some fluids, overstressing due to hydrostatic loading).

Tank rated capacity

84 Having established the overfill level (maximum capacity), it is then necessary to specify a level below this that will allow time for any action necessary to prevent the maximum level being reached/exceeded. This is termed the ‘tank rated capacity’, which will be lower than the actual physical maximum.

85 The required separation between the maximum capacity and the tank rated capacity is a function of the time needed to detect and respond to an unintended increase in level beyond the tank rated capacity. The response in this case may require the use of alternative controls, eg manual valves, which are less accessible or otherwise require longer time to operate than the normal method of isolation.

86 In some cases, it will be necessary to terminate the transfer in a more gradual fashion, eg by limiting the closure rate of the isolation valve, to avoid damaging pressure surges in upstream pipelines. Due allowance should be made for the delay in stopping the transfer when establishing the tank rated capacity. For some fluids, the tank rated capacity may also serve to provide an allowance for thermal expansion of the fluid, which may raise the level after the initial filling operation has been completed.

High-high level shutdown

87 The high-high level device provides an independent means of determining the level in the tank and is part of the overfilling protection system. It provides a warning that the tank rated capacity has been (or is about to be) reached/exceeded and triggers a response:

- the high-high level should be set at or below the tank rated capacity;
- the function of the high-high level (level alarm high-high (LAHH)) is to initiate a shutdown;
- the outcome of LAHH activation may be limited to a visible/audible alarm to alert a human operator to take the required action. The actions required by the operator to a high-high level warning should be clearly specified and documented; and
- the response may be fully automatic, via an instrumented protective system including a trip function that acts to close valves, stop pumps etc to prevent further material entering the tank. The trip function should include an audible/visual alarm to prompt a check that the trip function has been successful. Different devices can be employed to provide the trip function; these may range from a simple level switch (level switch high-high (LSHH)) to more sophisticated arrangements including duplicate level instrumentation.

Level alarm high (LAH)

88 Providing an additional means of warning that the intended level has been exceeded can reduce the demand on the high-high device. It is anticipated that the LAH will be derived from the system used for determining the contents of the tank ATG:

- the position of the LAH should allow sufficient time for a response following activation that will prevent the level rising to the tank rated capacity (or the high-high level activation point if this is set lower); and
- it is very important that the LAH is **NOT** used to control routine filling (filling should stop before the alarm sounds).

Normal fill level (normal capacity)

89 This level may be defined as the level to which the tank will intentionally be filled on a routine basis, using the normal process control system. The normal fill level will be dependent on the preceding levels and should be sufficiently far below the LAH to avoid spurious activation, eg due to level surges during filling or thermal expansion of the contents.

Other applications

90 In other applications, the primary means of determining the level may not involve an automatic gauging system. Depending on the detailed circumstances, the LAH may be a separate device, eg a switch.

Operator notifications

91 Some ATG systems include the facility for the operator to set system prompts to notify them when a particular level has been reached or exceeded. As the same level instrument typically drives these prompts and the LAH, they do not add significantly to the overall integrity of the system.

Determining action levels

92 Having defined generically the minimum set of action levels in the preceding section, it is necessary to consider the factors that determine the spacing between action levels in particular cases. In all cases, the spacing should be directly related to the response time required to detect, diagnose and act to stop an unintentional and potentially hazardous increase in level.

Response times

93 Care is needed when estimating the likely time for operators to respond to an incident. Consideration should be given to the detection, diagnosis, and action stages of response.

94 Detection covers how an operator will become aware that a problem exists. Assessment of alarm priorities and frequencies, the characteristics of the operator, and console displays, as well as operators' past experience of similar problems on sites, are all useful aspects to review. Plant problems that appear over a period of time and where the information available to the operators can be uncertain are particularly difficult to detect. When control rooms are not continually staffed, the reliable detection of plant problems needs careful consideration.

95 Diagnosis refers to how an operator will determine what action, if any, is required to respond to the problem. Relevant factors to think about include training and competence assurance, the availability of clear operating procedures and other job aids, and level of supervision. The existence of more than one problem can make diagnosis more difficult.

96 Action covers how a timely response is carried out. Key aspects include: the availability of a reliable means of communicating with other plant operators, the time needed to locate and operate a control (close a valve, stop a pump), the need to don personal protective equipment (PPE), the ease of operating the control while wearing PPE, and how feedback is given to operators that the control has operated correctly. Occasionally there may be circumstances where operators may hesitate if shutting down an operation might lead to later criticism.

97 A 'walk-through' of the physical aspects of the task with operators can provide useful information on the minimum time needed to detect and respond to an overfilling incident. However due allowance needs to be made for additional delays due to uncertainty, hesitation or communications problems. This will need to be added to the minimum time to produce a realistic estimate of the time to respond.

98 Figure 1 summarises this guidance. The spacing between levels in the diagram is not to scale and it is possible that the greatest response time, and hence the largest separation in level, will be between the LAHH and the overfill level. This is because the response is likely to involve equipment that is more remote and for which the location and method of operation is less familiar. An exception to this would be if the high-high level device included a trip function, when a shorter response time might be anticipated.

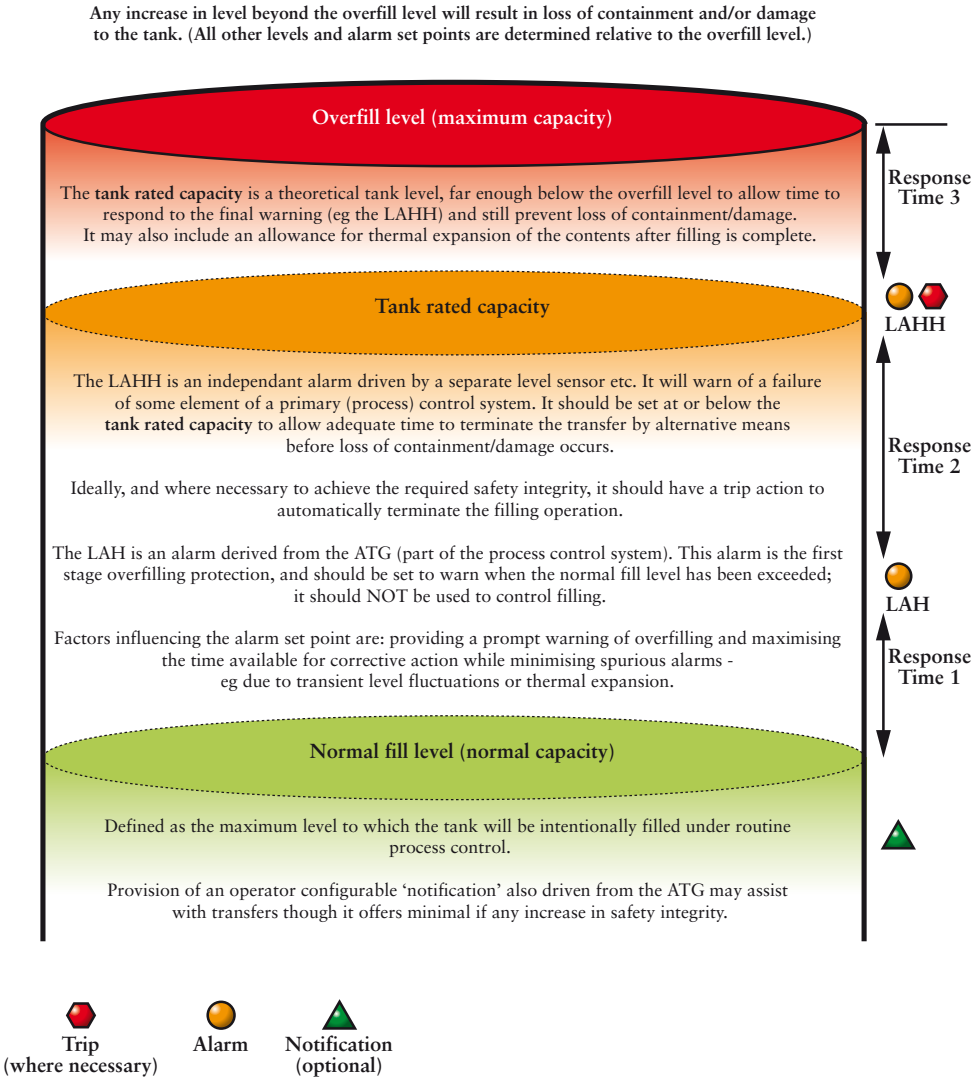


Figure 1 *Overfilling protection: Tank levels (based on API2350)*

Response time 3: LAHH to overfill/damage level (maximum capacity)

99 This is the response time between the LAHH and the overfill level (or maximum capacity – at which loss of containment or damage results). It should be assumed that the action taken to respond to the LAH has not been successful, eg the valve did not close or the wrong valve closed, and so corrective or alternative contingency action is now urgently required.

100 The response time to do this is identified as the worst combination[note1] of filling rate and time taken to travel from the control room to the tank and positively[note3] close the valve. This may be an alternative valve and may need additional time to identify and close it if not regularly used.

101 This could be done per tank, or more conservatively, standardised at the longest margin time for a group of or all tanks. In all cases, however, it must be recorded in writing.

Response time 2: LAH to LAHH

102 The response time between the high level alarm (LAH) and the independent high-high level (LAHH) should again be defined based on the worst combination[note1] of filling rate and time taken to activate and close a remotely operated valve if installed, or to get from the control room to the tank manual valve if not.[note2]

103 Again, this could be done per tank, or more conservatively, standardised at the longest margin time for a group of or all tanks. In all cases, however, it must be recorded in writing.

Response time 1: Normal fill level to LAH

104 The normal fill level should be close enough to the LAH to enable overfilling to be rapidly detected (and to maximise the usable capacity of the tank), but should be set an adequate margin below the LAH to prevent spurious operation of the alarm, eg due to liquid surge or thermal expansion at the end of an otherwise correctly conducted transfer.

105 Separation between the normal fill level and the LAH may also help to discourage inappropriate use of the LAH to control the filling operation.

Notes:

1 The tank with the highest fill rate might have a remotely operated valve (ROV) operated conveniently from the control room, allowing for very rapid shutdown, whereas a slower filled (and/or smaller diameter) tank that required a long journey to get to a local manual valve may in fact result in a lengthy time before the fill is stopped.

2 It is essential to take into account all of the organisational and human factors relevant to the site, eg failure of remote operation, loss of communications etc.

3 The remote and automatic systems must now be assumed to have failed – even if they appear to be working – and positive human action is now required to prevent overfill.

Appendix 2 contains worked examples of the application of this guidance for setting tank capacities.

Fire-safe shut-off valves

106 Each pipe connected to a tank is a potential source of a major leak. In the event of an emergency it is important to be able to safely isolate the contents of the tank. Isolation valves should be fire-safe, ie capable of maintaining a leak-proof seal under anticipated fire exposure.

Fire-safe criteria

107 Fire-safe shut-off valves must be fitted close to the tank on both inlet and outlet pipes. Valves must either conform to an appropriate standard (BS 6755-2 or BS EN ISO 10497),[14] equivalent international standards or be of an intrinsically fire-safe design, ie have metal-to-metal seats (secondary metal seats on soft-seated valves are acceptable), not be constructed of cast iron and not be wafer bolted.

Remotely operated shut-off valves (ROSOVs)

Future work: This section addresses the provision of ROSOVs on tank outlet lines. Broader issues relating to automated shutdown systems using ROSOVs on tank inlet lines will be covered in future work of PPSLG.

108 In an emergency, rapid isolation of vessels or process plant is one of the most effective means of preventing loss of containment, or limiting its size. A ROSOV is a valve designed, installed and maintained for the **primary purpose of achieving rapid isolation of plant items containing hazardous substances in the event of a failure of the primary containment system** (including, but not limited to, leaks from pipework, flanges and pump seals). Valve closure can be initiated from a point remote from the valve itself. The valve should be capable of closing and maintaining tight shut off under foreseeable conditions following such a failure (which may include fire).

109 *Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice* HSG244[10] provides guidance on how to assess the need to provide ROSOVs for emergency isolation. It has been written for a wide range of circumstances and as a result the section dealing with ROSOV failure modes requires additional interpretation.

110 A BSTG review of HSG244 ROSOV assessments was conducted and showed that several assessments did not fully address the risks in the structured manner required by HSG244, but rather simply asserted that the provision of ROSOVs was not reasonably practicable. Others did not fully apply the primary and secondary selection criteria and of those that did properly follow the steps in HSG244. It was concluded that:

- where the case-specific risk assessment indicated a ROSOV was required where currently only manual valves existed, then there was a worthwhile improvement to be gained by fitting a ROSOV;
- where the case-specific risk assessment indicated a ROSOV should be provided where currently a remotely operated valve (ROV) which would not fail safe existed, it was not reasonably practical to upgrade to a fail-safe device. But additional risk reduction could be achieved by ensuring that the cables were fire protected, and a rigorous regime was in place for inspection and testing the operation of the valves and control systems.

111 For tanks within scope, the expectation is that primary and secondary criteria in HSG244 would **not normally eliminate the need for a ROSOV** to the outlet pipe and as such a case-specific assessment as set out in Appendix 1 of HSG244 should be undertaken. For existing sites, the case-specific assessment must fully consider:

- whether fitting a ROSOV, where none is currently provided, is reasonably practicable;
- where a ROV is provided but it does not normally fail safe, whether upgrading to fail-safe valve is reasonably practicable; and
- where an existing ROV does not fail safe and it is not considered reasonably practicable to upgrade it, what additional measures should be provided to protect against failure, eg providing fire protection to the cabling and increasing the frequency of inspection and testing of the valve and associated cabling and energy supply.

Configuration

112 Bulk storage tanks can have their import and export lines arranged in a variety of configurations. These have a bearing on the necessary arrangements for isolating the tank inlets/outlets. Some tanks will have separate, dedicated import and export lines. Within this group, some will fill from the top and export from the base; some will both fill and export from either the top or the base. Others will have a single common import/export line, commonly connected at the base of the tank.

Dedicated import line

113 Tanks with dedicated import lines, whether these enter at the top or the base can be protected against backflow from the tank by the provision of non-return valves. Lines that enter at the top of the tank and deliver via a dip leg may in some cases be adequately protected by the provision of a siphon break to prevent the tank contents flowing back out via the feed line.

114 The provision of either or both of these features may affect the conclusion of any assessment of the need to provide a ROSOV for the purpose of emergency isolation of the tank against loss of the contents. These factors need to be considered when determining the appropriate failure mode for the valve or whether motorised 'fail in place'-type valves are acceptable.

Dedicated export line

115 Dedicated export lines on bulk tanks containing petrol should ideally be fitted with fire-safe, fail-closed ROSOVs; this would be the minimum expectation for a new tank installation. For existing installations, the need to provide ROSOVs retrospectively should be subject to an assessment according to the principles in HSG244. This assessment will need to include consideration of an individual having to enter a hazardous location to manually operate a valve for emergency isolation.

Common import/export lines

116 These lines cannot be provided with a non-return valve and it appears most appropriate to assess the ROSOV requirement, including the failure mode of the valve, based on the export function.

Testing overfill protection systems

117 Overfill protection alarms or shutdown systems using high level switches or other two-state detectors may be inactive for long periods and may develop unrevealed faults. Such faults cause the system to fail to danger when required to operate.

Proof testing

118 All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures frequently enough to ensure the specified safety integrity level is maintained in practice.

119 Proof testing should be end to end so far as is reasonably practicable including the detector at the liquid interface and the valve closure element. The test period should be determined by calculation according to the historical failure rate for each component or the system and the probability of failure on demand required to achieve the specified SIL. Records of test results, including faults found and any repairs carried out, should be kept. Part 1 of BS EN 61511[2] provides appropriate guidance on this issue.

Safe management of fuel transfer

120 BSTG recognised at an early point an issue with regard to safety arrangements, including communications, for fuel transfer. No existing authoritative guidance was found that adequately described this and so a set of principles for safe management of fuel transfer has been developed.

121 Companies involved in the transfer of fuel by pipeline should:

- adopt the principles for safe management of fuel transfer;
- where more than one party is involved in the transfer operation develop consignment transfer agreements consistent with those principles;
- ensure that suitable 'job factors' are considered and incorporated into systems and procedures to facilitate safe fuel transfer;
- for inter-business transfers, agree on the nomenclature to be used for their product types;
- for ship transfers, carry out a terminal-specific review to ensure compliance with the *International Shipping Guide for Oil Tankers and Terminals* (ISGOTT);[11]
- for receiving sites, develop procedures for transfer planning and review them with their senders and appropriate intermediates; and
- ensure that written procedures are in place and consistent with current good practice for safety-critical operating activities in the transfer and storage of fuel.

Principles for safe management of fuel transfer

122 To ensure that at all times, fuel transfer operations are carried out safely, operators and other organisations involved in fuel transfer should adopt the following guiding principles and implement specific procedures and protocols that meet those principles. All parties involved in the transfer of fuel must ensure that:

- responsibility for the management of the safe transfer of fuel is clearly delineated;
- there are suitable systems and controls in place to adequately manage the safe transfer of fuel commensurate with the frequency and complexity of the operation;
- there is clear accountability and understanding of all tasks necessary for the transfer operation;
- there are sufficient, adequately rested, competent persons to safely execute all stages of the operation;
- shift handover procedures comply with latest available industry guidance;
- receiving site operators:
  - positively confirm that they can safely receive the fuel before transfer commences; and
  - positively confirm that they are able to initiate emergency shutdown of the fuel transfer;
- there is clear understanding of what events will initiate an emergency shutdown of the fuel transfer operation;
- as a minimum, the following information is communicated between all relevant parties before commencing fuel transfer:
  - grade/type;
  - consignment size (including common understanding of units used);
  - flow rate profiles (significant[note1] unplanned changes in flow rate during the transfer should be communicated);
  - start time;
  - estimated completion time; and
  - any critical operations/periods when transfer could adversely affect other operations;[note2]
- there is an appropriate degree of integrity in the method of communication[note3] with positive confirmation of all critical exchanges;
- there is an agreed process to communicate changes to the plan in a timely manner;
- there is clearly understood nomenclature; and
- key performance indicators are in place to monitor and review performance.

Notes:

1 All parties to agree what constitutes a 'significant' change for their operation.

2 For instance, slow load requirements, roof on legs.

3 For instance, telephone, radio, facsimile, e-mail, common server.

123 Appendix 3 contains an aide memoire for job factors governing management of the safe transfer of fuel.

Consignment transfer agreements

124 Companies involved in the transfer of fuel by pipeline should develop and work within formal consignment transfer agreements consistent with the guiding principles for safe fuel transfer and incorporating the relevant job factors.

125 This guidance applies where one party controls the supply, and another controls the receiving tanks. This includes, for example, transfers between sites belonging to one business.

126 It does not apply to transfers where a single person or team controls both 'ends' of the transfer, although an equivalent standard of control is necessary. For the purposes of these agreements the sender is the party primarily responsible for the final transfer of fuel to the receiving terminal.

127 For transfers from ships into tanks, the current edition of the *International Shipping Guide for Oil Tankers and Terminals* (ISGOTT)[11] is considered to be the appropriate standard.

128 A consignment agreement involves three stages:

- **Stage 1:** a shared written initial consignment agreement describing what is to be transferred.
- **Stage 2:** a direct verbal confirmation, to a specified protocol or procedure, of:
  - the key details of the transfer taken from the written initial consignment agreement; and
  - confirmation of clearance to start the transfer given by the receiver.
- **Stage 3:** a procedure for handling significant change during a transfer.

Stage 1: Initial consignment agreement – written description of the transfer

129 The initial consignment agreement should form a description of the transfer, be agreed in writing, between sender and receiver, and be exchanged between all parties as close as practicable to Stage 2 (for example, during the current or previous shift).

130 The initial consignment agreement should be concise (not generally including product quality data) and should include information on:

- the nominated batch number (schedules/sequential);
- the product grade/type (in agreed terms);
- the product density (if required to enable conversion of volume to weight and vice versa);
- the amount to be transferred, stating units;
- the expected rate of transfer, including initial rate, steady cruise rate, and changes during plan;
- the date and expected time of start (this should include the need to agree these verbally);
- the estimated completion time;
- any relevant information regarding abnormal conditions that may affect product transfer, and mitigations in place, including risk assessment;
- the name of the sender (named individual);
- the name of the receiver (named individual);

- details of other responsibilities for involvement in the transfer and receipt process, as agreed locally;
- the arrangements for receiving terminal to stop the flow in the event of an emergency; and
- the target tank(s) for receipt.

131 The receiving terminal must sign the initial consignment agreement (after considering any abnormal conditions) and return it to the sending terminal to confirm that product can be safely received.

***Stage 2:** Final verbal confirmation and decision to receive*

132 Following the exchange of the initial consignment agreement, verbal confirmation of the details on the consignment note should be made. This includes the receiver giving permission to start the product transfer and confirmation of:

- the batch number(s) of the products ready to be transferred;
- the product grade/type and quantity, including a check of units to be transferred;
- that there are no significant changes from the written agreement that may affect the safe receipt of the product; and
- that the receiving party is ready to receive the product.

***Stage 3:** Procedure for handling significant change*

133 Significant changes should be communicated between sender and receiver, and recorded in writing by both parties. Each party should also record the actions taken.

Operational planning for fuel transfer by pipeline

134 Operational planning takes into account all stages of the plan development and approval, up to the stage of implementation via the consignment note.

135 The planning process should include:

- the contract strategy for deliveries (long-term planning process);
- development and agreement of monthly movement plans;
- amendments to monthly plans;
- development of weekly and daily operational plans;
- amendments to weekly and daily operational plans; and
- 'in line' amendments.

Procedures for control and monitoring of fuel transfer and storage

136 Fit-for-purpose procedures are essential for the safe management of fuel transfer and storage to minimise errors and to protect against loss of operating knowledge (eg when experienced personnel leave). Maintaining an appropriate SIL level for overfilling protection systems will often require detailed supporting procedures to ensure that safety-critical actions are undertaken consistently and with sufficient rigour.

137 Procedures are agreed safe ways of doing things. Written procedures usually consist of step-by-step instructions, and related information, to help carry out tasks safely. They may include checklists, decision aids, diagrams, flow charts and other types of job aids. They are not always paper documents, and may appear as 'on screen' help in control system displays.

138 *Revitalising procedures*[20] provides guidance on how to develop procedures that are appropriate, fit-for-purpose, accurate, 'owned' by the workforce and, most of all, useful. It covers:

- the links between procedural problems and major accidents;
- what procedures are, and why they are needed;
- procedural violations, and why people do not always follow them;
- how to encourage compliance with procedures;
- different types of procedures;
- involvement of procedure users;
- where procedures fit into risk control;
- links between training, competency and procedures;
- a three-step approach to improving procedures;
- review of procedures; and
- presentation – formatting and layout (including use of warnings to explain what happens in the event of an abnormal situation).

Procedures

139 Procedures should be consistent with the principles for safe management of fuel transfer and consignment transfer agreements and incorporate appropriate controls specified in the SIL assessment. Ensuring that robust systems and procedures are in place to maintain the designed safety integrity level of overfill protection measures is of vital importance.

140 The **sender's** procedures should specify:

- the minimum communications required, including:
  - confirmation of the start of product transfer; and
  - information on any deviations from the original plan;
- the correct sequence of operations to avoid overpressure or surge;
- the arrangements to monitor the flow (based on risk assessment); and
- any circumstances where transfer must stop, eg:
  - no confirmation of tank changeover is received when expected; and
  - when the agreed parcel has been sent.

141 The **receiver's** written instructions should cover all key phases of its operations, including:

- preparation and start-up;
- monitoring the transfer and stock reconciliation, including response to alarms if required;
- tank changeover;
- closing/shutting down;
- routine checks; and
- contingencies for abnormal occurrences.

142 Further details of the requirements for each phase are given in paragraphs 143–157.

Preparation and start-up

143 This requires an effective means of communication between sender and receiver, which should be achieved by means of a consignment transfer agreement.

144 In addition, the receiver should have written procedures in place to ensure that the necessary preparatory checks and line setting are carried out effectively.

These procedures should specify clearly defined routings for all standard transfers, including alignment of valves etc, except where a documented risk assessment determines that this is not necessary, taking consideration of the complexity, frequency and criticality of the task.

145 If a non-standard routing is to be used, there should be a clear, detailed specification of the required route.

Monitoring and reconciliation, including response to alarms

146 These arrangements must conform to the control measures set out in the SIL assessment. Procedures for monitoring and reconciliation should include initial verification that the fuel movement phase is as expected, by initial dip/telemetry as appropriate, after around 15–20 minutes (determined by transfer speed and capacity, etc). If 'Yes' this should be confirmed to the consignor/sender.

147 If 'No' it should be treated as an abnormal situation and contingency arrangements should be specified. Robust arrangements, based on a risk assessment of local circumstances, must be made to identify 'unauthorised' movements.

148 There should be continuous verification at **set periods** (within defined tolerances) through manual checks or automated systems as appropriate. Checking at set periods is necessary to check that the 'mental model' is correct or if there has been an unexpected change (eg an unexpected process change, or a measurement error due to a stuck instrument). The set periods and tolerances should be defined and clear to operators, and be derived from risk assessment, taking account of:

- fill and offtake rates;
- capacity;
- degree of automated control of movement;
- potential speed of response;
- planned staffing cover arrangements (if a problem); and
- anticipated completion time.

149 Communication requirements must be specified, including the need for the receiver to contact the sender when critical steps are approaching, such as 'running' tank changes or when there are abnormal circumstances or trips.

150 Procedures should specify that all filling operations must be terminated at or before the normal fill level, which should be set sufficiently far below the level alarm high (LAH) to avoid spurious activation of the alarm. (In this context alarms do not include alerts for process information.)

151 Procedures should also be clear about the response required on LAH and level alarm high-high (LAHH). If the LAH is reached, then appropriate action should be taken to reduce the level to below the alarm setting in a controlled and timely manner. If the LAHH is reached, immediate action must be taken to terminate the transfer operation and reduce the level to, or below, the normal fill level.

Tank changeover

152 There may well be a plan to change tanks during the transfer. In this situation there should be clear designated routings for the changeover. Procedures must detail arrangements for verification and communication in the period up to an anticipated tank change, again clearly based upon risk assessments of local circumstances. The receiver retains primacy in a decision to cease the transfer at any time.

153 Unless a process risk assessment shows it to be unnecessary, operational procedures should require the receiver to communicate with the sender:

- when changeover is imminent; and
- when the changeover has been completed; then
- go to the monitoring and reconciliation procedure.

Closing/shutting down

154 Procedures should detail the actions to take to ensure safe isolation and to prevent damage to plant and equipment after completion of the transfer. They should require the receiver to confirm to the sender that movement has stopped.

Routine plant checks

155 Operators should ensure that there is a physical site check, to defined routes or activities, which can pick up sounds, smells etc that may indicate a problem. All parts of the tank farm should be inspected at an adequate interval (for instance, four times in a 24-hour period), with guidance on what to look for (eg source of ignition, breaches in containment, leaks, unattended machinery, security breaches etc). This, together with any anomalies found and actions taken, should be recorded.

Contingencies for abnormal occurrences

156 For each phase of the operation, foreseeable abnormal occurrences should be identified, such as:

- loss of critical equipment;
- inability to use receipt tank, or swing tank, valves;
- incapacity or unavailability of staff; and
- inability to contact key personnel etc.

157 Written instructions, based on an assessment of risks, should give clear guidance for staff on the action to take to mitigate such occurrences. These actions should be included in emergency plans and emergency response exercises.

Engineering against loss of secondary and tertiary containment

This section represents interim guidance, as PPSLG will undertake further work to develop more detailed guidance on secondary and tertiary containment.

158 While priority 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. The failure of secondary and tertiary containment at Buncefield contributed significantly to the failure to prevent a major accident to the environment (MATTE).

Bund integrity (leak-tightness)

159 Bund wall and floor construction and penetration joints should be leak-tight. Surfaces should be free from any cracks, discontinuities and joint failures that may

allow relatively unhindered liquid trans-boundary migration. As a priority, existing bunds should be checked and any damage or disrepair, which may render the structure less than leak-tight, should be remedied.

160 Bund walls should be leak-tight. As a priority, existing bund walls should be checked and any damage or disrepair, which may render the wall less than leak-tight, should be remedied.

Fire-resistant bund joints

161 This guidance does not address the fire-resistance of the main material of construction for existing bunds, because:

- this was not believed to be a significant factor in the Buncefield incident, except insofar as:
  - the contraction on cooling of concrete walls may have caused the opening up of wall joints and consequent integrity failure; and
  - the reason for concrete floor heave and associated loss of integrity and the comparative performance of earth/clay, is not known to BSTG;
- further information from the Buncefield investigation and additional civil engineering studies will be needed to properly consider the comparative impact of fire on earth/clay bund walls and floors compared to reinforced concrete.

162 Joints in concrete or masonry bunds walls should be capable of resisting fire. Existing bunds should be modified to meet this requirement. In addition to repairing any defects in bund joints, steel plates should be fitted across the inner surface of bund joints, and/or fire-resistant sealants should be used to replace or augment non-fire-resistant materials.

163 The current good practice standard for the construction of reinforced concrete bunds is BS 8007:1987 *Code of practice for design of concrete structures for retaining aqueous liquids*.[21] Bund joints are currently required to be rendered leak-tight by the adoption of flexible barriers such as waterstops and sealants, bonded into or onto the concrete joint surface.

164 BS 8007 does not address the retention of non-aqueous liquids or of liquids above 35º C, or the construction of bund joints at pipework and other penetrating structures. CIRIA reports 163[22] and 164[23] address bund design and construction issues in detail. The CIRIA/Environment Agency joint guidance[24] referring to CIRIA report 163 is also relevant to the design and construction of smaller reinforced concrete bunds.

165 To achieve bund joints capable of resisting fire, improvements may be required to the fire resistance of:

- the main material(s) of construction (not addressed in this guidance);
- the waterstops and flexible sealant(s) used to make joints leak-tight; and
- joints to wall and floor penetrations such as pipework. It may also be necessary to provide additional fire protection to joints by fitting a 'fire-proof' barrier such as steel plate.

Masonry (brickwork and block-work) bund walls

166 On older sites masonry bund walls are still in use. Vertical expansion and contraction joints and penetration joints rely on sealants to keep the bund watertight. These may require improvement to fire resistance. In addition, where significant cracks in masonry joints have been repaired with flexible sealant, these may also require improvement.

Earth/clay bunds

167 Earth/clay are in very common use, often as floors of bunds with concrete or masonry walls. In such floors there are normally no construction joints, but penetrating drains or other pipework result in points of weakness and potential failure.

168 The following modification options for improving fire resistance should be assessed for practicability and likely effectiveness.

Flexible sealants

169 Sealants are now available for which enhanced resistance to fire is claimed. The only fire-resistance standards that are quoted on these products are BS 476-20:1987 and BS 476-22:1987.[25] The maximum fire resistance quoted to BS 476 is four hours. The relationship of performance to this standard to actual performance in a bund-joint application is yet to be determined. In considering the use of fire-resistant sealants, due regard should also be given to the suitability and compatibility of candidate products (eg hydrocarbon and water resistance) in the specific application.

170 While fire-resistant sealants represent a significant improvement over non-fire-resistant sealants, a very severe pool fire, such as seen at Buncefield, is still likely to result in failure of joints. The prolonged pool fire scenarios at Buncefield are thought to have resulted in considerable longitudinal expansion of wall sections, and consequent compression of wall joints, resulting in extrusion of sealant from joints and the burning out of the extruded sealant. When walls cooled and contracted after the fire was extinguished, it is thought that joints opened up and, with sealant burnt out, loss of integrity and containment resulted. This potential mode of failure emphasises the need to consider suitable tertiary as well as secondary containment provision.

Steel protection plates

171 Steel plates, observed in some locations at the Buncefield incident site, are thought to have provided significant additional protection to bund joints. It is believed that these plates were not, however, designed for fire protection purposes. Nevertheless, the relevant joints appeared to withstand a severe pool fire without losing integrity. **It therefore appears that where it is practicable to fit them, suitably designed protective steel plates may provide more effective fire resistance than fire-resistant sealants.**

172 Detailed information is not currently available for the design of steel plate fire protection, and operators should design for specific applications. However, the following general guidance is useful:

- material of construction: stainless steel;
- width: minimum 20 cm;
- thickness: minimum 6 mm;
- fixings to bund walls: stainless steel bolts through oversized slotted holes, minimum 30 cm intervals; and
- additional protective features to be considered:
  - fireproof backing material such as cement board; and/or
  - fire-resistant coating such as intumescent material to the front face.

Note: in designing protection plates, consideration should be given to avoiding weakening the wall structure in relation to resistance to fire, hydrostatic and hydrodynamic forces. Numerous practicable designs for existing installations have now been developed and implemented.

Recommended improvements

Existing bunds

173 Improvements should be made to the fire-resistance of bund joints by suitable protection (eg metal plate covering) and/or by the use of fire-resistant sealants. Problems experienced in sourcing compatible sealants in suitable packaging for this application, together with uncertainties in actual joint fire resistance performance or requirements, unavoidably result in a range of ad-hoc improvement solutions.

174 This 'best-endeavours' design approach constitutes a reasonably practicable approach for existing installations and current designs for new build. The PPSLG will work to resolve the outstanding technical issues to produce new standards for application to reinforced concrete bund construction and penetration joints. This is likely to be based on the existing standards BS 8007,[21] BS 8110,[26] BS 6213[27] and BS 476,[25] and to be specified to achieve an adequate duration of fire resistance taking into account the post-Buncefield learning on high-integrity primary containment and firefighting response factors, and the potential for tertiary containment.

175 **Bund wall penetration joints:** For penetrations of concrete and masonry, the first option should be to consider re-routing pipework or other penetrating structures to eliminate the need for the joint. Where this is not practicable, or planned removal is significantly delayed for operational reasons, the fire-resistance of the joint must be improved. The fitting of steel collars, bellows or similar to improve fire resistance at pipework penetrations may introduce local corrosion initiation sites in the pipework, and is therefore not recommended where this may be likely. In such cases joints should be improved by replacing existing sealants with fire-resistant sealants. For penetration of earth bund walls, these joints may be inherently less vulnerable because of the greater joint thickness. However, insufficient information has been considered to allow reliable guidance to be produced for this case. Joints should be assessed on a site-specific basis.

176 **Bund floor construction joints:** For concrete bund floors, vulnerability to fire should be capable of being reduced by managed emergency response measures such as maintaining an insulating water layer on the bund floor. Removal of existing flexible sealant for replacement with fire-resistant alternatives may result in reduced performance with regard to water tightness. Floor joints nevertheless remain potential weaknesses for loss of integrity in a severe pool fire. A case-by-case assessment of floor joint fire-resistance improvement options should be made.

177 **Bund floor penetration joints:** Bund floor penetration joints are points of inherent weakness where any failure of integrity is very difficult to detect and may continue unnoticed for some time. Consequently, existing bund floor penetrations should be eliminated wherever practicable. Where flexible sealants are used in floor penetration joints, these should be removed and replaced with fire-resistant sealants.

178 **Cracks in concrete and masonry bund walls and floors:** Repaired cracks in existing bund surfaces must be assessed for significance with regard to the potential to fail in a fire scenario, resulting in loss of secondary containment. Where cracks are superficial, improvement may not be required, but where cracks are significant, the flexible sealant used must be replaced by fire-resistant sealants.

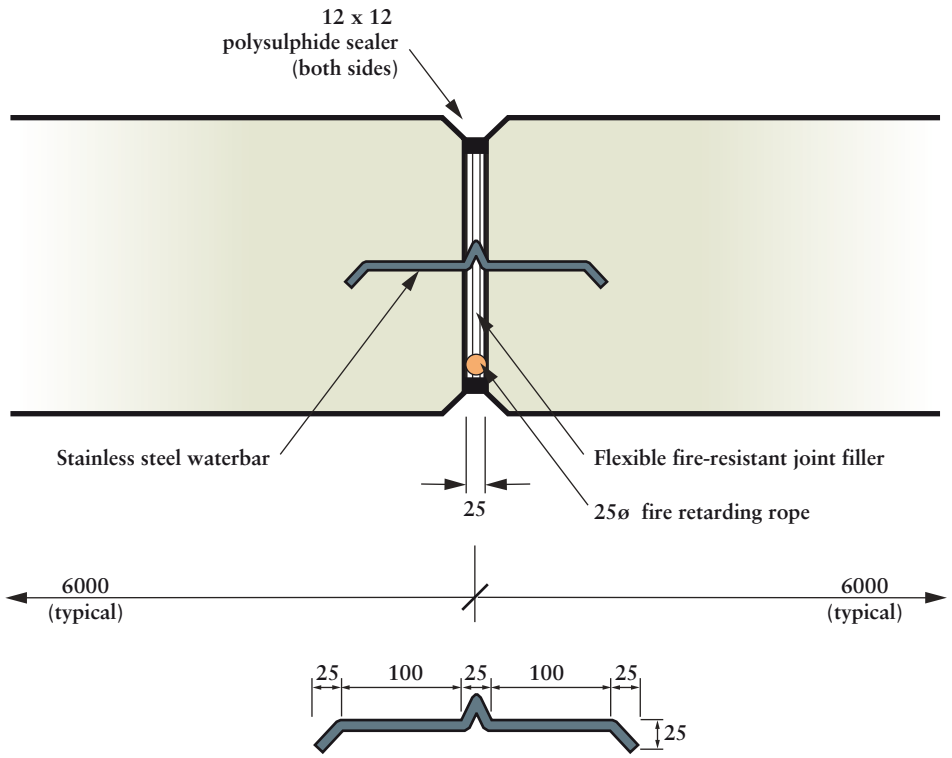
New bunds

179 For new bunds, to achieve the maximum practicable fire resistance for bund joints the following additional measures should be taken:

- **Bund wall and floor construction joints:** Joints should be designed to be fire resistant. Consideration should be given to incorporating stainless steel waterstops and expansion joints bonded into the structure, in combination with fire-resistant sealant.
- **Bund wall penetration joints:** Wall penetrations should not be incorporated into new bunds unless alternative over-wall routings are impracticable. Where wall penetrations are unavoidable, joints should be designed to be fire resistant. Consideration should be given to incorporating puddle flanges cast into the concrete structure.
- **Bund floor penetration joints:** Floor penetrations should not be incorporated into new bunds.

Stainless steel waterstop designs

180 New designs are available incorporating stainless steel waterstops into bund walls. A drawing of an example system is shown in Figure 2.



Notes: **1:** Fire retarding rope to be placed on both sides of an internal bund wall and on internal side only of an external wall
2: Waterbar, rope and polysulphide sealant to be omitted in bundwalls footings
3: Stainless steel for waterbar to be grade 316 and 1.0 mm thick

All measurements are in millimetres

Bund wall expansion joint detail (1/10)

Figure 2 *Bund wall expansion joint showing stainless steel waterstop (detail)*

Fire-resistant wall penetration joints

181 Figure 3 shows an example puddle flange cast into a bund wall – a 200 NB pipe in a 250 NB sleeve passing through a bund wall.

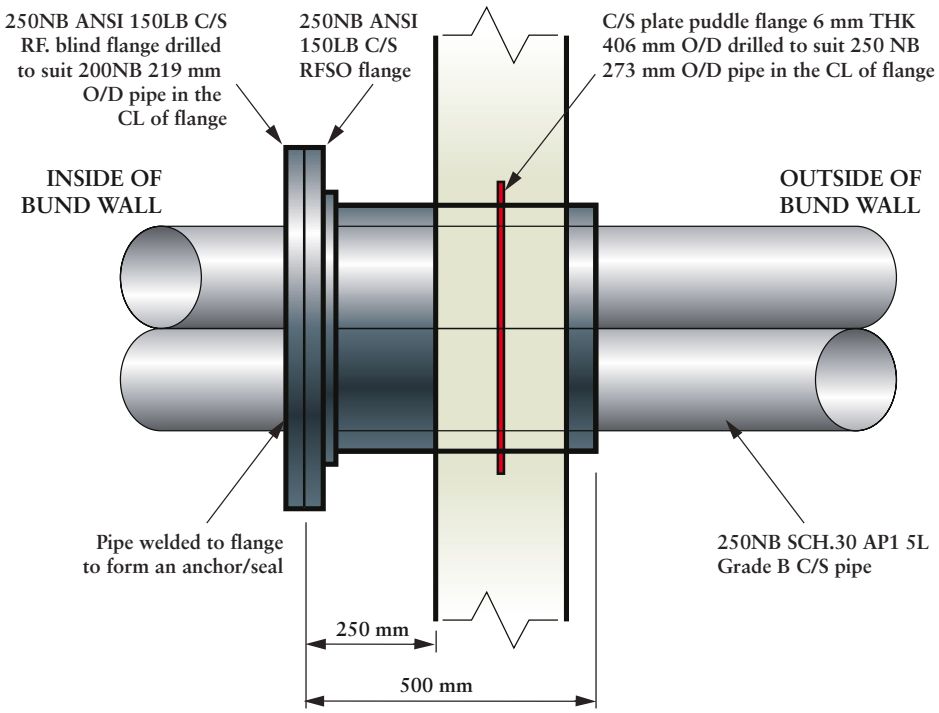


Figure 3 *Example puddle flange cast into a bund wall*

Bund capacity

182 The minimum capacity for bunds containing tanks in scope at existing installations is 110% of the largest tank.

Firewater management and control measures

183 Well-planned and organised emergency response measures are likely to significantly reduce the potential duration and extent of fire scenarios, and so reduce firewater volumes requiring containment and management. Site-specific planning of firewater management and control measures should be undertaken with active participation of the local Fire and Rescue Service, and should include consideration of:

- bund design factors such as firewater removal pipework, aqueous layer controlled overflow to remote secondary or tertiary containment (for immiscible flammable hydrocarbons);
- recommended firewater/foam additive application rates and firewater flows and volumes at worst-case credible scenarios; and
- controlled-burn options appraisal, and pre-planning/media implications.

Tertiary containment

PPSLG will undertake further work to develop more detailed guidance on tertiary containment.

184 This guidance applies only to the loss of secondary containment from bunds containing tanks within the scope. At installations where bunds contain tanks within scope, operators should assess the requirement for tertiary containment, on the basis of environmental risk, and to make site action plans for improvement.

185 The term 'tertiary containment' is used to describe containment systems and measures to contain potentially polluting liquids which may escape as a result of loss of secondary containment, and would otherwise be released into the environment causing pollution.

Risk assessment

186 A risk assessment should be undertaken to determine the extent of the requirement for tertiary containment, taking into account:

- foreseeable bund failure modes, including:
  - the amount of spilled substances, including hydrodynamic effects of catastrophic tank failure and emergency response actions such as firefighting;
  - the potential impact of fire on bund integrity including joints in walls and floors;
  - worst-case foreseeable delivered firewater volumes including firefighting agents;[28] and
  - passive and active firewater management measures.
- environmental setting, including:
  - all relevant categories of receptors as specified in *Guidance on the interpretation of Major Accident to the Environment;*[29]
  - proximity of receptor, eg groundwaters under the site;
  - site and surrounding topography;
  - geological factors affecting the permeability of surrounding land and environmental pollution pathways; and
  - hydrogeological factors affecting liquid pollutant flows and receptor vulnerabilities;
- known pathways and potential pathways to environmental receptors in the event of failure of secondary containment;
- likely environmental impact consequences, in terms of extent and severity, of the pollutant and/or firewater quantities and flows resulting from foreseeable bund failure scenarios.

Design standards

187 Based on the scope and capacity determined by the site-specific risk assessment, tertiary containment should be designed to:

- be independent of secondary containment and any associated risks of catastrophic failure in a worst-case major accident scenario;
- be capable of fully containing foreseeable firewater and liquid pollutant volumes resulting from the failure of secondary containment;
- be impermeable to water and foreseeably entrained or dissolved pollutants;
- use cellular configuration, to allow segregation of 'sub-areas' so as to limit the extent of the spread of fire and/or polluted liquids;
- operate robustly under emergency conditions, for example in the event of loss of the normal electrical power supply;
- avoid adverse impacts on firefighting and other emergency action requirements;
- allow the controlled movement of contained liquids within the site under normal and emergency conditions;

- facilitate the use of measures for the physical separation of water from entrained pollutants;
- incorporate practical measures for the management of rainwater and surface waters as required by the configuration; and
- facilitate clean up and restoration activities.

188 On-site effluent treatment facilities, sized to allow collection and treatment of polluted firewater, are a desirable design feature, but may only be justifiable at larger establishments.

Design options

189 Selection of tertiary containment options will be highly dependent on site-specific factors such as layout, topography and available space. The term 'transfer systems' (CIRIA Report 164[23] Ch13) is used to describe the means for collecting and conveying spillage/firewater to remote and combined secondary and tertiary containment.

190 Design options for tertiary containment include:

- local cellular tertiary containment surrounding secondary containment – gravity fed;
- local gravity collection systems at identified failure points, connected with:
  - gravity transfer to remote containment;
  - pumped transfer to remote containment;
  - tankage dedicated to tertiary containment; and
  - sacrificial land;
- local dedicated gravity drainage and collection sump(s), capable of handling total emergency liquid flows into secondary containment, and connected with pumped transfer to remote containment.

191 Remote tertiary containment may serve more than one secondary containment system, as long as it is designed to be capable of accommodating total foreseeable flows and quantities.

192 Existing secondary containment systems may be used to provide tertiary containment for other secondary containment, as long as foreseeable secondary containment failure scenarios are mutually exclusive and equipment (eg pumps) is independent and reliability of emergency operation is assured.

193 Some tertiary containment assessments, carried out in response to the BSTG initial report recommendations,[9] have considered the environmental receptors surrounding the installation and potential pathways for pollution flows. However, many concentrated solely on assessing the maximum practical use of installed containment capacity, and determining the consequent firefighting attack duration. Buncefield showed that consequences might be much more extensive than expected.

194 Assessment of tertiary containment should start with an initial worst-case assumption that available secondary containment will fail or capacity will be exceeded, and the consequent firewater flows and directions should be identified and estimated. Based on this, implementation of basic good practice measures should be considered, eg site kerbing/banking, sleeping policemen/ramps, permanent or temporary measures to close off potential environmental pathways and/or direct flows, and temporary emergency containment provision. This could include the provision of pollution containment equipment, eg pipe-blockers, drain sealing mats and land booms.

195 Further assessment should consider firewater volumes from worst-case credible scenarios. Implementation of additional measures should be considered by means of a cost–benefit analysis comparison versus the expected value of the consequences. Consideration of tertiary containment measures beyond basic good practice should be informed by an integrated risk assessment of the primary/secondary/tertiary controls as a whole.

Published guidance

196 General guidance on the design of remote containment systems (including lagoons, tanks and temporary systems such as sewerage storm tanks and sacrificial areas such as car parks, sports field and other landscape areas) is available in numerous documents including CIRIA report 164,[23] and PPG18.[30]

197 Catchment areas used for tertiary containment often serve a dual purpose, eg roadways, hard standing, car parks. Such areas are normally routinely drained to surface water drainage systems. Therefore, to be considered for emergency tertiary containment, such areas must be capable of reliable emergency sealing of drains and interception of pollutants. Furthermore, arrangements must not compromise emergency access or unduly compromise day-to-day operations.

198 Major accident case studies provide valuable approaches to tertiary containment design, for example:

- Allied Colloids, Bradford (July 1992);
- Monsanto, Wrexham (1985);
- Sandoz, Switzerland (1986);

The first two of these are described in CIRIA report 164,[23] Ch6.

Risk assessment guidance

199 Numerous guidance documents are available on environmental risk assessment. A selection is listed in the *References* section of this report.

200 Suitable and precautionary methodologies should be used for the above risk assessment. In view of the high uncertainties in modelling the transport of entrained or dissolved pollutants in liquids escaping secondary containment, it is recommended that assessments concentrate on quantifiable physical parameters such as those indicated in Table 2.

Table 2 *Environmental risk assessment check list*

Action/parameter	**Guidance**
For the worst-case foreseeable severe pool fire scenario	
Identify firewater volumes	Energy Institute IP19[28]
Assess firewater management effects	
Identify bund potential failure points	MIIB second progress report[31]
For each failure point, assess: ● likely liquid/firewater flow and volume ● direction of escaped liquid flows	
For the worst-case catastrophic tank failure	
Identify expected liquid volumes, flow directions and receiving locations outside bund walls	
For the surrounding environment, construct a conceptual site model	
Construct conceptual site model	EI *Environmental guidelines for petroleum distribution installations*[32]
Identify surrounding environmental receptors, eg sites of special scientific interest, rivers, agricultural land. Classify in terms of receptor type and sensitivity/importance	Environment Agency www.environment-agency.gov.uk/; Natural England www.naturalengland.org.uk/, DEFRA[29] Tables 1-12
Identify geological characteristics	
Identify hydrogeology	British Geological Survey www.bgs.ac.uk/
Identify flow gradients and likely flow outcomes	
Identify direct pathways, eg drains, boreholes	
Identify indirect pathways to sensitive receptors, eg permeable ground	
Assess permeability of ground and thus permeation flow-rates and quantities of pollutant into ground	CIRIA report 164[23]
Consider appropriate defensive tertiary containment measures	
Kerbing to roadways, car parks etc, toe walls, area grading	
Eliminate direct pathways, eg cap boreholes	
Emergency drain seals (eg auto-actuated bellows)	
Overflows to remote containment lagoons	
Channel spillages to remote containment	
Additional hardstanding	
Dedicated tankage	
Transfer to other secondary containment	

High reliability organisations

201 The need for high reliability organisations follows from the 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.

202 Of particular importance are:

- understanding and defining the role and responsibilities of the control room operators (including in automated systems) in ensuring safe transfer and storage;
- 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.

Roles, responsibilities and competence

203 Operators should ensure that they have:

- clearly identified the roles and responsibilities of all those involved in managing, performing, or verifying work in the management of fuel transfer and storage, including contractors; and
- implemented a competence management system, linked to risk assessment for fuel transfer and storage, to ensure that anyone whose work impacts on the control of major accident hazards is competent to do so.

Roles and responsibilities

204 Clear understanding and definition of roles and responsibilities and assurance of competence in those roles are essential to achieve high reliability organisations for the control of major accident hazards.

205 Organisational changes such as multi-skilling, delayering or downsizing, in which staff are expected to take on a wider range of responsibilities with less supervision, increase the need to check competence. Each company also has a responsibility to ensure their fitness standards are suitable for the risks involved in the transfer and storage of fuel.

206 COMAH guidance[12] identifies a range of personnel for which the roles, responsibilities, accountability, authority, and interrelation of personnel should be identified. They include all those involved in managing, performing or verifying work in the management of major hazards, including contractors.

207 All key safety-related aspects of roles and responsibilities relating to fuel transfer and storage should be clearly specified, either in job descriptions or elsewhere. This is essential for indentifying training needs and assuring competence.

Competence

208 Competence means the ability to undertake responsibilities and to perform activities to a recognised standard on a regular basis. It is a combination of practical and thinking skills, experience and knowledge.[33-35]

209 Training and development seeks to create a level of competence for the individual or team, sufficient to allow individuals or teams to undertake the operation at a basic level. Over time, as practical experience grows, operations can be carried out at a more complex level. Training is required not just for normal operation but also for abnormal/upset and emergency conditions etc.

210 Training alone is not sufficient. HSE research report *Competence assessment for the hazardous industries*[36] highlights the need for organisations to recognise the difference between merely recording a person's experience and training, and assessing their competence.

211 The purpose of a competence management system is to control in a logical and integrated manner a cycle of activities that will assure competent performance. The aim is to ensure that individuals are clear about the performance expected of them, that they have received appropriate training, development and assessment, and that they maintain or improve their competence over time.

212 The key issue for sites to consider is the competence of staff in relation to the control of major accident hazards (MAHs) associated with fuel transfer and storage, and how this is identified, assessed and managed.[35] MAH competency needs to be appropriately linked to the MAH and risk analysis and key procedures. The aim is to assure competence in safety-critical tasks, and associated roles and responsibilities.

213 Competency for major accident prevention is necessary at all levels in the organisation, not just the front line. There should be standards set for competency at all levels, and these should be process/job specific. The National or Scottish Vocational Qualification (NVQ/SVQ) system can provide some general and some site-specific competencies, but is not usually linked to MAHs. Operators of COMAH sites need adjust their systems to make this link.

214 *Competence assessment for the hazardous industries*[36] is a useful reference. It aims to provide:

- an authoritative view of what comprises good practice in the field of competence assessment in relation to control of MAHs; and
- a model of good practice.

215 *Developing and maintaining staff competence*[33] is also a useful text on competence management. It was written for the rail industry, but it is equally applicable to many other industries. The competence management system (CMS) described consists of 15 principles linked under five phases, as follows:

- establishing the requirements of the CMS;
- designing the CMS;
- implementing the CMS;
- maintaining competence; and
- audit and review of the CMS.

216 The guidance can be used from any point in the cycle for improving existing systems, or for setting up and implementing new competence management systems. It describes:

- the principles and factors that should be considered in any CMS;
- how to ensure that the competence of individuals and teams satisfies the requirements of existing legislation; and
- guidance and responsibilities relating to medical and physical fitness.

217 HSE's Human Factors Briefing Note No 2[34] and Core Topic 1: *Competence assurance*[35] also provide useful summaries of requirements for competence management.

Staffing and shift work arrangements

218 Operators should:

- ensure they can demonstrate that staffing arrangements are adequate to detect, diagnose and recover any reasonably foreseeable hazardous scenario in relation to fuel transfer and storage; and
- ensure that shift work is adequately managed to control risks arising from fatigue.

219 Staffing and shift work arrangements are critical to the prevention, control and mitigation of major accident hazards. Site operators should be able to demonstrate that staffing arrangements ensure there are sufficient alert, competent personnel to deal with both normal operation and hazardous scenarios arising from abnormal events in fuel transfer and storage.

220 Some high hazard organisations have set staffing levels based on steady-state operations. HSE Contract Research Report *Assessing the safety of staffing arrangements for process operations in the chemical and allied industries* CRR 348/2001,[37] was commissioned to provide a method to demonstrate that staffing arrangements are adequate for hazardous scenarios as well as normal operations.

Safe staffing arrangements

221 CRR 348/2001 gives a practical method for assessing the safety of staffing arrangements and is supplemented by a user guide *Safe staffing arrangements – user guide for CRR 348/2001 methodology.*[38]

222 The CRR 348/2001 method provides a framework for companies to assess the safety of their staffing arrangements with focus on assessing the staffing arrangements for capability to detect, diagnose and recover major accident scenarios. It is a facilitated team-based approach taking several days for each study and using control room and field operators as team members.

223 The method has three key elements:

- definition of representative scenarios (preparation for study);
- physical assessment of the ability of staff to handle each scenario by working through eight decision trees for each scenario (approximately two hours per scenario);
- benchmarking 11 organisational factors using 'ladders' – this is a general assessment by the team and not scenario based (approximately one hour per ladder).

224 Note that both CRR 348/2001 and associated user guide are required for the method, since the guide gives an additional benchmarking ladder for assessing automated plant/equipment.

225 The basis for the method can be found in *Reducing error and influencing behaviour* HSG48,[16] as an assessment of individual, job and organisational factors. The physical assessment, using the eight decision trees for each scenario, focuses on job factors assessing the capability of the operators to:

- detect a hazardous scenario, eg is the control room continuously manned?
- diagnose a hazardous scenario; and
- recover from a hazardous scenario, including assessment of communications.

Safe shift work arrangements

226 High-level guidance on alertness and fatigue is given in the CRR348/2001 methodology and specific guidance on shift work is given in *Managing shift work* HSG256.[39] An overview is given in *Managing fatigue risks.*[40]

227 The introduction to HSG256 outlines the aim of the guidance to improve safety and reduce ill health by:

- making employers aware of their duty under law to assess any risks associated with shift work;
- improving understanding of shift work and its impact on health and safety;
- providing advice on risk assessment, design of shift work schedules and the shift work environment;
- suggesting measures to reduce the negative impact of shift work; and
- reducing fatigue, poor performance, errors and accidents by enabling employers to control, manage and monitor the risks of shift work.

228 The main principle of the Health and Safety at Work etc Act (HSW Act) is that those who create risk from work activity are responsible for the protection of workers and the public from any consequences. Generically, the two types of risk arising from fatigue derive from the probability of sleepiness and the increased probability of error.

229 Consistent with this and *Successful health and safety management* HSG65,[41] HSG256 details a systematic approach to assessing and managing the risks associated with shift work under the following five headings:

- Consider the risks of shift work and the benefits of effective management. For example, fatigue affects vigilance and monitoring tasks, particularly on night shifts.
- Establish systems to manage the risks of shift work; the need for senior management commitment is highlighted.
- Assess the risks associated with shift work in your workplace.
- Take action to reduce these risks. The guidance includes a number of useful tables giving non-sector-specific examples of factors relating to the design of shift work schedules, the physical environment and management issues such as supervision.
- Check and review your shift-work arrangements regularly. Include suggested performance measures such as the HSE Fatigue and Risk Index Tool and Epworth sleepiness scale.

230 HSG256 should be supplemented by relevant sector-specific guidance, eg the Institute of Petroleum (IP) guidance *Improving alertness through effective fatigue management*, published by the Energy Institute (EI).[42] However, HSG256 is a comprehensive and practical guide with appendices covering a summary of legal requirements and practical advice for shift workers, along with a listing of assessment tools such as the HSE Fatigue and Risk Index Tool.

Shift handover

231 Operators should set and implement a standard for effective and safe communication of issues relevant to fuel transfer and storage at shift and crew change handover. For top-tier COMAH sites, a summary of the standard should be included in the next revision of the safety report.

232 Action to improve communications at shift handover is a priority issue. Transfer of volatile fuels into storage frequently continues across shift changes, and there is little doubt that unreliable communications about plant or transfer status at shift change could potentially contribute to a tank overfill. HSG48[16] discusses how unreliable communications can result from a variety of problems. It identifies some high-risk communication situations, and some simple steps that can be used to improve communications in the workplace. The Competent Authority Safety Alert review of oil/fuel storage sites in early 2006[43] indicated that many sites had structured shift handover formats in place, but some relied on event-type logs or unstructured logs that did not clearly specify the type of information that needed to be communicated.

233 The minimum provision is a handover procedure, or standard, that specifies simple and unambiguous steps for effective communications at shift and crew change. These include carefully specifying what information needs to be communicated, using structured easy-to-read logs or computer displays, ensuring key information is transmitted both verbally and in writing, and encouraging two-way communication.

234 The handover procedure should be based on the principles described in HSG48. It should:

- carefully specify what key information needs to be communicated at shift and crew change, at key positions in the organisation. The requirements may well be different for different positions, but should consider issues such as:
  - product movements, both ongoing and planned;
  - control systems bypassed;
  - equipment not working or out of commission;
  - maintenance and permitry;
  - isolations in force;
  - trips defeated;
  - critical or high-priority alarms activated and actions taken;
  - health, safety or environment incidents or events;
  - modifications; and
  - personnel on site;
- use suitable aids, such as logs, computer displays etc to provide a structured handover of key information, while aiming to cut out unnecessary information;
- capture key information that needs to be carried forward across successive shifts (eg equipment out of service);
- allow sufficient time for handover, including preparation time;
- ensure that key information is transmitted both verbally and in writing;
- encourage face-to-face, and two-way communication, with the recipient asking for confirmation, repetition, clarification etc as appropriate; and
- specify ways to develop the communication skills of employees.

235 The handover procedure should take account of situations that are known to be especially liable to problems, including:

- during maintenance, if the work continues over a shift change;
- during deviations from normal working;
- following a lengthy absence from work (either as a result of a regular long shift break or individual absence); and
- handovers between experienced and inexperienced staff.

236 Techniques that have been reported from the industry, and that companies may wish to consider in development of their procedure, include:

- use of electronic logs, with password systems for acceptance;
- systems to project electronic logs onto a screen (for team briefing);
- use of team briefings, eg with staggered shift changes between supervisors and operators;
- use of pre-printed paper logs in a structured format; and
- use of white boards for recording systems that may be out of service for several shifts.

237 Companies must have the facilities and management arrangements necessary to ensure that the standard set are indeed complied with. These include:

- arrangements to minimise distractions during handover;
- instruction and training of employees in handover procedures; and
- supervision, audit and review to ensure that the procedure is complied with and the necessary information is communicated and understood.

Organisational change and management of contractors

238 Site operating companies should ensure that:

- there is a suitable policy and procedure for managing organisational changes, and for retention of corporate memory;
- the policy and procedure ensure that the company retains adequate technical competence and 'intelligent customer' capability when work impacting on the control of major accident hazards is outsourced or contractorised;
- suitable arrangements are in place for managing and monitoring contractor activities.

Organisational change

239 Organisational changes that can adversely affect the management of fuel transfer and storage include various types of internal restructuring, reallocation of responsibilities, changes to key personnel, and contractorisation.

240 *Organisational change and major accident hazards* CHIS7[44] sets out a framework for managing organisational changes, and is recommended for high-hazard industries. Paragraphs 368-369 to *A guide to the Control of Major Accident Hazard Regulations 1999*[12] summarise the range of changes, including changes to people and the organisation, which should be subject to management of change control procedures.

Management of contractors

241 In high-hazard industries, policies regarding use of contractors or outsourcing need to be clear. If safety-critical work in relation to fuel transfer and storage is to

be contracted out, then the company should ensure that it remains an 'intelligent customer'. In other words, it should retain adequate technical competence to judge whether, and ensure that, work is done to the required quality and safety.

242 A principle, well known within the nuclear industry, is that companies should maintain the capability within their own organisations to understand and take responsibility for the major hazard safety implications of their activities. This includes understanding the safety case for their plant and the limits under which it must be operated. HSE's Nuclear Directorate publications *Principles for the assessment of a licensee's intelligent customer capability*[45] and *Contractorisation*[46] provide the basis for these principles.

243 *Organisational change and major accident hazards* CHIS7[44] extends this principle more widely to high-hazard industries, stating that if you contract out safety-critical work, you need to remain an 'intelligent customer'. In other words, retain adequate technical competence to judge whether, and ensure that, work done is of the required quality and safety.

244 An organisation that does not have intelligent customer capability runs the risk of:

- not understanding its safety report, and operating unsafely;
- not having appropriate staff to adequately deal with emergencies;
- procuring poor safety advice or wrongly implementing advice received;
- not recognising that significant plant degradation or safety-critical events are arising, or not addressing them correctly;
- not identifying the requirements for safety-critical modifications or maintenance, or carrying them out inadequately; and
- employing inadequate contractors or agency staff.

245 Even where it has not produced the safety report itself, the company should be capable of understanding it, leading the presentation of the report to the regulator, and ensuring consistency between the safety report and the design and operation of the safety management system.

246 A site operator who proposes to contract-out fuel transfer and storage arrangements should have organisational change arrangements in place to review the proposal and demonstrate that safety will not be jeopardised. 'Intelligent customer' capability and 'core competencies' should be maintained to ensure that contracting arrangements do not adversely affect the ability to manage fuel storage safely. There may be a limit to the extent that an operator can safely diminish the expertise of its organisation by using contractors for core functions; this is likely to vary with circumstances. The site operator needs to maintain sufficient expertise in all disciplines to recognise when technical questions need answering, and to judge the adequacy of the responses.

247 The site operator needs to have adequate arrangements for retention of corporate memory. The most common circumstances under which the loss of corporate memory could occur are:

- staff turnover: the accumulated knowledge of experienced staff, which is often extensive, can be lost when knowledge is not transferred from outgoing to incoming staff;
- unavailability of information: this occurs when information is not recorded, or not archived appropriately, or when information is not provided through pre-job briefing. Of particular importance is the availability of the as-built design knowledge that changes over the life of the facility; and
- ineffective use or application of knowledge: despite the existence of information

within the organisation, individuals may not be aware or may not understand they had access to information.

248 To counter the above, site operators need to develop succession plans to respond to situations involving staff movements and have in place formal arrangements for knowledge archiving and transfer of information.

Performance evaluation and measuring process safety performance

249 To maintain and improve the effectiveness of a complex process safety management system, managers must periodically evaluate the system's performance and address and communicate to others in the sector any identified deficiencies or opportunities for improvement.

250 Measuring performance to assess how effectively risks are being controlled is an essential part of a health and safety management system.[12,17] **Active monitoring** provides feedback on performance before an accident or incident, whereas **reactive monitoring** involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes.

251 Site operators should:

- ensure that they have a suitable active monitoring programme in place for those systems and procedures that are key to the control of fuel transfer and storage; and
- develop an integrated set of leading and lagging performance indicators for effective monitoring of process safety performance.

252 The presence of an effective personal safety management system does not ensure the presence of an effective process safety management system. The report of the BP US Refineries Independent Safety Review Panel (the Baker Panel report),[3] following the BP Texas City refinery explosion in 2005, found that BP's personal injury rates were not predictive of process safety performance at BP's five US refineries.

253 Used effectively, process safety indicators can provide an early warning, before catastrophic failure, that critical controls have deteriorated to an unacceptable level. The use of process safety performance indicators fits between formal, infrequent audits and more frequent inspection and safety observation programmes. It is not a substitute for auditing, but a complementary activity.

254 The main reason for measuring process safety performance is to provide ongoing assurance that risks associated with fuel transfer and storage are being adequately controlled. To measure safety performance, many companies have incorporated leading and lagging indicators, also known as 'metrics' or 'key performance indicators', into their safety management systems. Managers use these metrics to track and compare or benchmark safety performance.

255 Many organisations rely on auditing to highlight system deterioration. However, audit intervals can be too infrequent to detect rapid change, or the audit may focus on 'compliance', ie verifying that the right systems are in place rather than ensuring that systems are delivering the desired safety outcome.

256 Many organisations do not have good information to show how they are managing major hazard risks. This is because the information gathered tends to be limited to measuring failures, such as incident or near misses. System failures

following a major incident frequently surprise senior managers, who believed the controls were functioning as designed.[17]

Active monitoring

257 Active monitoring is primarily a line management responsibility.[44] It is sometimes referred to in the industry as internal auditing, but should be distinguished from the requirement for 'independent' audits, which are a separate activity. *Successful health and safety management* HSG65[41] refers to auditing as the structured process of collecting independent information on the efficiency, effectiveness, and reliability of the total health and safety management system (SMS), and drawing up plans for corrective action.

258 Active monitoring should include inspections of safety-critical plant, equipment and instrumentation as well as assessment of compliance with training, instructions and safe working practices.

259 Active monitoring gives an organisation feedback on its performance before an incident occurs. It should be seen as a means of reinforcing positive achievement, rather than penalising failure after the event. It includes monitoring the achievement of specific plans and objectives, the operation of the SMS, and compliance with performance standards. This provides a firm basis for decisions about improvements in risk control and the SMS.

260 Site operators need to decide how to allocate responsibilities for monitoring at different levels in the management chain, and what level of detail is appropriate. In general, managers should monitor the achievement of objectives and compliance with standards for which their subordinates are responsible. Managers and supervisors responsible for direct implementation of standards should monitor compliance in detail. Above this immediate level of control, monitoring needs to be more selective, but provide assurance that adequate first-line monitoring is taking place.

Reactive monitoring

261 Reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes. It includes:

- identification and analysis of injuries/causes of ill health;
- identification and analysis of other incidents, near misses, and weaknesses or omissions in performance standards;
- assessing incident/near miss potential;
- investigation and identification of remedial actions to deal with root causes;
- communication of lessons learned;
- tracking remedial actions arising from incidents/near misses etc; and
- contributing to the corporate memory.

Investigation of incidents and near misses

262 Site operators should ensure they have suitable procedures for:

- identifying incident/near-miss potential;
- investigating according to the identified potential;
- identifying and addressing both immediate and underlying causes;
- sharing lessons learnt; and
- tracking remedial actions.

263 As technical systems have become more reliable, the focus has turned to human causes of accidents. The reasons for the errors of individuals are usually rooted deeper in the organisation's design, decision-making and management functions.

264 HSG48[16] gives several examples of major accidents where failures of people at many levels (ie organisational failures) contributed substantially towards the accidents. Human factor topics of relevance to the management of fuel transfer and storage include:

- ergonomic design of plant, control and alarm systems;
- style and content of operating procedures;
- management of fatigue and shift work;
- shift/crew change communications; and
- actions intended to establish a positive safety culture, including active monitoring.

265 Investigation procedures should address both immediate and underlying causes, including human factors.

Guidance on investigation

266 HSG65[41] is a suitable reference. Not all events need to be investigated to the same extent or depth. Organisations need to assess each event (for example, using a simple risk-based approach) to identify where the most benefit can be obtained. The greatest effort should concentrate on the most significant events, as well as those that had the potential to cause widespread or serious injury or loss.

267 HSG65 Appendix 5 describes one approach that may be used as a guide for analysing the immediate and underlying causes of effects. Various other approaches are also available, and widely used within the industry. These include various in-house or proprietary systems.

Audit and review

268 Site operators should adopt and implement audit plans defining:

- the areas and activities to be audited, with a particular focus on process safety/control of major accident hazards;
- the frequency of audits for each area covered;
- the responsibility for each audit;
- the resources and personnel required for each audit;
- the audit protocols to be used;
- the procedures for reporting audit findings; and
- the follow-up procedures, including responsibilities.

269 Site operators should ensure that they have implemented suitable arrangements for a formal review of arrangements for fuel transfer and storage, including:

- the areas and activities to be reviewed, with a particular focus on process safety/control of major accident hazards;
- the frequency of review (at various levels of the organisation);
- responsibility for the reviews;
- the resources and personnel required for each review; and
- procedures for reporting the review findings.

Auditing

270 Auditing provides an independent overview to ensure that appropriate management arrangements (including effective monitoring) are in place, together with adequate risk control systems and workplace precautions. Various methods can achieve this. AIChE guidelines[47,48] draw a distinction between process safety auditing, and process safety management systems (PSMS) auditing.

271 The focus of process safety auditing is the identification and evaluation of specific hazards (eg inspecting hardware and finding the absence of a relief device, or an independent trip system). PSMS auditing, however, involves assessment of the management systems that ensure ongoing control (eg the management systems in place to ensure that pressure relief devices have been designed, installed, operated, and maintained in accordance with company standards).

272 Both types of audit are important. The process safety audit addresses a particular hazard found at a specific time. It could lead to correction of the hazard without addressing the underlying reason why the hazardous condition came to exist. The PSMS audit addresses the management systems intended to preclude the creation of hazards.

273 Such audits are formal and infrequent. Companies may decide to audit a small range of activities on a more frequent basis (eg yearly), or a more extensive range on a less frequent basis (eg three–five years). The company should decide the range and scope of its audit programme, taking into account such factors as audits/inspections imposed by others (eg the Competent Authority, parent companies or joint venture partners, insurers, trade associations), and the extensiveness of the active monitoring programme.

274 Audits that focus primarily on 'compliance' (ie verifying that the right systems are in place rather than ensuring that they deliver the right safety outcome) are not sufficient.

Process safety performance indicators

275 HSE recently published *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries.*[17] The guidance outlines six main stages needed to implement a process safety measurement system. It provides a methodology for leading and lagging indicators to be set in a structured way for each critical risk control system within the process safety management system. The Organisation of Economic Co-operation and Development (OECD) has also developed *Guidance on safety performance indicators*[49] to assess the success of chemical safety activities.

276 **Leading indicators** are a form of active monitoring focused on a few critical risk control systems to ensure their continued effectiveness. They require a routine systematic check that key actions or activities are undertaken as intended. They can be considered as measures of process or inputs essential to deliver the desired safety outcome.

277 **Lagging indicators** are a form of reactive monitoring requiring the reporting or investigation of specific incidents and events to discover weaknesses in that system. These incidents represent a failure of a significant control system that guards against or limits the consequences of a major incident.

278 **The six key stages** identified in the guidance are:

- establish the organisational arrangements to implement the indicators;
- decide on the scope of the measurement system; consider what can go wrong and where;
- identify the risk control systems in place to prevent major accidents. Decide on the outcomes for each and set a lagging indicator;
- identify the critical elements of each risk control system (ie those actions or processes that must function correctly to deliver the outcomes) and set leading indicators;
- establish the data collection and reporting system; and
- review.

Worked example

279 BSTG has prepared a worked example (Appendix 4) for developing process safety performance indicators, using HSG254 methodology, for a terminal fed by pipeline and also by a ship via a jetty.

Review

280 Reviewing should be a continuous process undertaken at different levels in the organisation. An annual review would be the norm, but organisations may well decide on a system of intermediate reviews at, for example, department level. The result should be specific remedial actions which establish who is responsible for implementation, with deadlines for completion.

281 Issues to be considered in the review process include:

- the Major Accident Prevention Policy (MAPP);
- audit programme achievement and findings;
- active monitoring of records and findings;
- process safety performance indicators;
- incident/near miss history;
- relevant lessons from incidents etc elsewhere;
- analysis of root/basic causes of incidents and near misses;
- issues from safety committees;
- tracking of safety actions; and
- risk assessment status, including reviews against changing standards.

Emergency response arrangements

282 This section covers the recommendations relating to on-site emergency response arrangements and the interface between on-site and off-site emergency response arrangements. Further recommendations will follow dealing with any additional issues in these areas that have been identified in the MIIB's emergency preparedness, response and recovery report,[50] as well as consideration of off-site issues. An overview of emergency planning requirements can be found at Appendix 5.

Principles

283 All sites in scope should prepare in writing a suitable on-site emergency plan as required by the COMAH Regulations. For lower-tier COMAH sites the plan should be prepared as part of the MAPP.

284 The emergency plans should consider the response to and mitigation of a multiple tank fire following an explosion. The plan should cover the on-site consequences of such an event and the assistance available in the form of off-site mitigatory actions.

285 The incident-specific emergency response plans should consider fire management requirements in response to, and mitigation of, a multiple tank fire. The plan should cover the on-site consequences of such an event and the assistance available in the form of off-site mitigatory actions. Any plan deemed necessary to deal with such an event must be capable of operating effectively even in the event of a preceding explosion.

286 The firefighting plan should be functionally tested and exercised at least annually. Site-specific guidance should be produced as to what is required to exercise the firefighting arrangements.

287 During preparation of the on-site plan, the operator should consult with the local authority emergency planning unit, the Environment Agency (or SEPA) and the local emergency services, particularly the local Fire and Rescue Service, on the content of the on-site plan to ensure the off-site response available is adequate to deal with the incident.

288 The operator should provide all information (relating to the site) required by the COMAH Regulations to the local emergency planning unit to allow the off-site plan arrangements to dovetail with the on-site plan.

289 The operator should keep the on-site plan up to date and should ensure that any significant changes are communicated to the local authority and other concerned agencies.

290 The operator should ensure the on-site plan is functionally tested at least every three years. Site-specific guidance should be produced as to what is required to exercise the plan.

291 Trained, knowledgeable and competent personnel must be involved in the exercise of the firefighting plan and in the testing of the on-site plan. They must fulfil the tasks they will be expected to fulfil during an incident.

292 Whenever a plan is reviewed/tested or if there has been a material change in an aspect of an emergency arrangement, the operator should inform all contributors to the plan of any changes to arrangements and verify that the arrangements are still adequate. All contributors to the plan should be encouraged to inform the site operator proactively of any material changes affecting their contribution.

On-site emergency plan

293 A template for an on-site emergency plan can be found at www.hse.gov.uk/comah/buncefield/final.htm. It is envisaged that sites will complete this template and that it will then act as a high-level document providing an overview of the site's arrangements. Underpinning this document will be a series of detailed plans relating to specific incidents.

294 Planning should consider the scenario of a multiple tank fire following an explosion. It is not possible to provide precise information on the magnitude of the explosion at this time as research is currently (July 2007) ongoing. Once accurate information is available this will be disseminated. In the meantime, operators should make a reasonable estimate of the scale of explosion that may occur on their site and plan accordingly.

Firefighting planning and preparation

295 This topic comprises of two elements; firstly, the actions that should be put in place before an event occurs and secondly, actions that should be carried out once an event has occurred. These arrangements should be agreed by all parties involved, including off-site responders.

296 Planning aids the firefighting operations immensely by determining what is needed to extinguish the fire or manage a controlled burn, and how to deliver the required resources and manage firewater to prevent environmental impact.

297 Scenario-based incident-specific emergency response plans can identify incident control resources required for accidental release, spillages and fire and emergency response. They can also provide guidance on control and deployment of the necessary resources and importantly, can be used as a tool to exercise against, thus closing the loop from preparation to planned and exercised response.

298 Sometimes a 'controlled burn' strategy may be appropriate. Controlled burn is where the fire is not extinguished deliberately to allow the fuel to burn away in a controlled fashion. In such cases, firefighting resources will still be required, primarily to cool adjacent tanks and facilities to prevent escalation.

299 A controlled burn strategy may be appropriate if, for example:

- firewater run-off or fuel would cause significant pollution to sensitive environmental receptors such as surface and groundwater abstractions and/or designated habitats;
- the site is remote from centres of population or a controlled burn is the best option for air quality;
- the site is not capable of containing the required quantities of firefighting water and foam; or
- there is a significant risk to firefighter safety.

300 A controlled burn strategy may not be appropriate if:

- smoke plumes could result in a risk to public health, and/or large areas require evacuation;
- major transport routes require closing. If a transport route is threatened, a risk assessment will be required to determine the consequences of environmental damage against the impact on transport routes;
- there is a significant risk of the fire escalating.

301 Such deliberations should form part of the environmental and safety risk assessment carried out by the operator when producing the on-site emergency plan. This should be in consultation with the environment agencies, the local authorities, the emergency services (particularly the Fire and Rescue Service) and other stakeholders.

302 Further guidance on the use of controlled burn is available in the Environment Agency's PPG 28[51] and the FRS *Manual on environmental protection*.[52]

303 If it is decided to extinguish the fire then IP19 *Fire precautions at petroleum refineries and bulk storage installations*[53] is considered to be 'relevant good practice' under COMAH, and operators should comply fully with this good practice. New sites should comply fully with IP19. Existing operators should comply with this relevant good practice where it is reasonably practicable to do so. In effect, this means that existing operators should undertake a gap analysis between the

requirements in this code and those measures present on site. Any measures not in place but which are specified in the code should be implemented if it is reasonably practicable to do so.

304 The following is a list of the steps needed to plan for tank related fire and emergency scenarios, which have been drawn from the IP19 code of practice to aid operators. It states the questions that need to be considered and points to the relevant section in the code for further detail.

305 **Step 1** Determine the worst-case scenario for the fire event. For fuel depots this is considered to be either the largest tank in a single bund, or the largest group of tanks in a single bund. If the plan adequately covers the resources for the worst-case scenario, it can be considered capable of dealing with lesser similar events, eg fires in smaller tanks etc. (IP19 code sections 2.5–2.7, section 3.2.)

306 **Step 2** Assume a full surface tank fire and bund fire.

307 **Step 3** Determine the radiant heat hazard ranges using appropriate consequence modelling (and including weather factors) to determine safe locations for the firefighting resources deployment. (IP19 code section 2.6.) This also determines the size of monitor necessary to achieve the required throw to reach the tank roof. The actual distance from the monitor to the involved tank only depends on the effective reach of the monitor used. It is important to determine the wind direction because the monitor should be placed to allow the wind to carry the foam to the fire. Changes in wind direction will have to be accommodated in the plan. Fire monitor performance is available from the manufacturer, but be aware the figures quoted will relate to best performance. Operators should base their plan on perhaps 20% reduction in performance to counter this, and then test it appropriately to prove the effectiveness.

308 **Step 4** Determine the amount of foam concentrate and water necessary to firefight the worst-case scenario. (IP19 code Annex D).

309 **Step 5** Assess whether the necessary foam stocks are available on site. If not, consider how quickly these stocks can be brought to the site and by whom – what arrangements have been made with the Fire and Rescue Service, foam manufacturers and/or neighbouring sites. Ideally operators should have the means and quantity of foam on site to cope with a fire in the largest bund immediately. Operators will also need to consider how foam stocks can be transported around the site.

310 **Step 6** Is the water supply sufficient in terms of quantity, pressure and flow rate? (IP Code Annex D6.) The pressure required is back-calculated starting at the monitor. Most monitors require 7 to 9 bar, then add in the frictional losses from the monitor to the pumps. Operators need to remember that the system demands will not just be at the monitors; water drawn from any fixed system applications and cooling streams will also need to be considered. It is important to determine the required volumes and pressures used. Dynamic system demand testing will provide the evidence that the system can deliver the required resources.

311 **Step 7** If high volume pumps or high pressure pumps are necessary to achieve the required water capacities, where will these be provided from and how long will they take to arrive and be set up? The possibilities include fixed firewater pumps at the site, mobile firewater pumps purchased by the site, pre-arranged mutual aid from other nearby facilities or the Fire and Rescue Service. All resources will need to be considered in the plan so they can be logistically arranged for relay pumping purposes. Remember to build in redundancy to cover for the nearest resources being already in use or in repair etc.

312 **Step 8** What means are there for delivering the required foam/water to the fire? How many and what size monitors are necessary? This is determined by the area at risk and the application rates required to secure and extinguish this risk. Remember the need for compatibility where hardware is brought from a variety of sources.

313 **Step 9** How much and what size and pressure rating of hose is required? Where will this quantity of hose be obtained from? The size and quantity of hose required on the flow rate, pressure and distance from the water supply. The greater the flow rate, pressure or distance from the water supply, the larger the diameter and pressure rating of the hose needed.

314 **Step 10** How will any firewater run-off be dealt with? Hose and pumps will be necessary to transfer firewater run-off from the bund to another bund or catchment area. Alternatives include purpose-built bund overflows to a remote tertiary containment system, or increasing the capacity of an existing bund. Transfer could be by pumps or via gravity flow.

Firefighting incident management

315 The following actions should be carried out:

- Operators should contact the local authority Fire and Rescue Service (LAFRS) in accordance with the pre-incident management agreement between the operator and the Fire and Rescue Service.
- The local authority Fire and Rescue Service should rendezvous at predetermined holding point for the company concerned.
- Fire and Rescue Service Incident Commander should formally liaise with the company on-scene commander (and site fire officer if applicable), obtaining information regarding the incident, whether or not people are involved, the resources in place and the hazards and risks associated with the particular event. These persons will form the incident control team (ICT) along with any others required by the circumstances.
- Establish immediate priorities and the potential for escalation. Local scenario-specific emergency response plans (ERPs) for the plant or area should at this time be made available to, and be used by, the ICT.
- Lines of supervisory authority and the means of communication should be clearly established within the ERPs to assist in effective reporting and incident control.
- The ICT must ensure the safety of all personnel. This team should have:
  - completed a dynamic risk assessment (DRA) and if there has been time, a written record needs to be handed to the FRSIC on their arrival;
  - arranged for the DRA to be recorded and constantly reviewed. The DRA also needs to be communicated and the tactical mode declared, implemented and recorded;
  - ensured that safety officers are appointed with their responsibilities clearly established.
- The ICT should also:
  - establish the incident command position;
  - determine the operational objectives and the incident plan, including tactical and strategic considerations;
  - identify from the ERPs, the equipment, material and resources required, coordinating effort into sourcing equipment and materials to the incident;
  - obtain additional support/equipment/resources if required (via mutual aid partnerships if in existence);
  - implement the mutually agreed strategy by bringing resources on-site from the rendezvous point at this stage;

- monitor and review the implemented plan for ongoing potential hazards and the continued effectiveness of the plan at predetermined intervals. If the plan cannot be followed or if a deviation is required from it at any time then a DRA must be carried out, communicated to all concerned and recorded;
- establish welfare arrangements for all at incident scene; and
- ensure that media issues are addressed.

Further work relating to off-site elements of the firefighting process will be carried out by PPSLG.

Part 3: Work in progress on process standards

316 This Part represents interim guidance as further work will be undertaken by the Petrochemical Process Standards Leadership Group (PPSLG) to develop additional guidance to meet the recommendations of the Buncefield Major Incident Board on the design and operation of fuel storage sites and other issues. Unlike Part 2, the guidance in this Part is not as yet specified as minimum expected good practice as it is work in progress and has not been fully considered by BSTG.

317 For ease of reference, the information in this Part is presented using the relevant section headings used in Part 2. This will help show where the final guidance will be located once the next update of this guidance is published.

Protecting against loss of primary containment using high-integrity systems

Future work: The sector and the Competent Authority plan to address the issue of high-integrity, automatic overfill prevention systems and to issue more detailed guidance on this recommendation in the future.

Maintenance of records

318 Accurate records of process conditions in relation to fuel transfer and management are essential to review trends and deviations from intended outcomes. Good records are essential in investigating the root causes of incidents and being able to learn and apply lessons from incidents.

319 Site operating companies should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially have developed into a Buncefield-type incident. It is recommended that records should be retained for a minimum period of one year.

320 The following information is considered important:

- stock records to demonstrate compliance with a stock control policy;
- operational plans;
- consignment transfer agreements;
- local records of changes to consignment transfers;
- stock reconciliation records;
- incidences of high level alarm activation;
- incidences of high-high level/trip activation;
- maintenance/proof testing for high level trip and alarm systems;
- faults discovered on high level alarm or protection systems;
- communications failures between sender and receiver;
- plant/process changes;
- organisational changes;
- approval/operation of inhibits/overrides of safety systems;
- competence/training records;

- shift work/overtime records;
- shift handover records;
- routine plant tour records;
- permits to work;
- risk assessments;
- method statements; and
- active monitoring records.

Engineering against loss of secondary and tertiary containment

Bund floors – Impermeability

321 Exposed floor surfaces need to be impermeable (of low intrinsic porosity) so as to prevent permeation of enough polluting liquid to potentially cause a major accident to the environment (MATTE). The existing best practice standard on impermeability for new containment systems is stated in CIRIA report 164[23] (equivalent to 1 metre of clay with a maximum permeability (to water and relevant liquids) of 1 x $10^{(-9)}$ metres/second). However, the question remains as to the standard of impermeability that could be considered to meet minimum good practice for existing installations. Substance- and site-specific factors are likely to be important considerations. Further development of more detailed guidance will be addressed by PPSLG.

Fire-resistant bund joints

322 The best-endeavours design approach recommended in Part 2 of this report constitutes reasonable practicability for existing installations and current designs for new build. However work is needed to resolve outstanding technical design issues to inform the definition of good practice standards for fire resistance of bunds.

323 PPSLG will work to resolve the issues to enable definition of a new standard or standards for application to reinforced concrete bund construction and penetration joints. The sector aims to support this work through collaboration, research and development, and PPSLG will work to resolve the issues to enable definition of a new standard or standards for application to reinforced concrete bund construction and penetration joints. This is likely to be based on the existing standards BS 8007,[21] BS 8110,[26] BS 6213,[27] and BS 476,[25] and to be specified to achieve an adequate duration of fire resistance, taking into account the post-Buncefield learning on high-integrity primary containment and firefighting response factors, and the potential for tertiary containment.

Bund capacity

324 The minimum capacity requirement for relevant bunds at existing installations is 110% of the largest contained tank. Existing guidance also recommends that the minimum capacity should be 25% of the total tanks contained in a bund, if this is greater. The 110% criterion is well-understood, but the 25% criterion is a more arbitrary rule-of-thumb value and is not widely accepted as appropriate by the sector.

325 Additional required capacity over the 110% minimum should be determined by a risk-based assessment, taking into account additional or alternative measures (eg pre-planned firewater management measures such as recycling and controlled burn). PPSLG will work to resolve these issues.

High reliability organisations

Management of plant and process changes

326 Site operating companies should ensure they have suitable guidance for their staff about what constitutes a change, and that they have suitable arrangements in place for managing the range of permanent, temporary and urgent operational changes.

Management of change

327 Experience (eg the Flixborough disaster in 1974) has shown management of change to be an essential factor in prevention and control of major accidents.

328 Site operators require management procedures for planning and control of all changes in plant, processes and process variables, materials, equipment, procedures, software, design or external circumstances that are capable of affecting the control of major accident hazards. This approach ought to cover permanent, temporary and urgent operational changes, including control of overrides/inhibits, as well as changes to the management arrangements themselves.[47]

329 *A guide to the Control of Major Accident Hazards Regulations 1999*[12] summarises the range of changes that should be subject to management of change control procedures. Each site needs guidance to help its personnel to determine the difference between like-for-like replacement and a change. This should cover items such as:

- valves;
- piping and flanges;
- vessels/tanks;
- rotating machinery;
- instrumentation;
- software;
- process materials;
- operational changes;
- maintenance procedures;
- purchasing changes; and
- equipment relocation.

Delivering high performance through culture and leadership

330 Poor safety culture has been found to be a significant causal factor in major accidents such as BP Texas City, Chernobyl, Bhopal, the Herald of Free Enterprise disaster, several major rail crashes etc.

331 The leadership of senior managers, and the commitment of the chief executive, is vital to the development of a positive safety culture. The report of the BP US Refineries Independent Review Panel (the Baker Panel Report)[3] drew specific attention to the importance of:

- process safety leadership at all levels of an organisation;
- implementing process safety management systems; and
- developing a positive, trusting, and open process safety culture.

332 The US Chemical Safety and Hazard Board's (CSB's) Investigation Report[54] into the Texas City refinery explosion also identifies safety culture as a key issue requiring leadership of senior executives. It was particularly critical of the lack of a reporting and learning culture, and of a lack of focus on controlling major hazard risk.

333 Implementing [the MIIB] 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. [The MIIB] noted with interest the recent report[3] of the BP US Refineries Independent Safety Review Panel by James Baker's panel in the United States. Some of the recommendations and findings in that report align with [the MIIB's] 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.

Long-term industry leadership

334 The sector, in consultation with the Competent Authority, needs to put in place continuing arrangements for leadership in relation to operating and safety standards on a long-term basis. Action to improve sector leadership will be the key to facilitate implementation of our recommendations and to provide a focus for continuous improvement. PPSLG will provide that sector leadership.

335 Effective leadership of process safety to develop a positive, open and trusting process safety culture will be an essential feature within site operating companies.

Leadership and process safety culture

336 The safety culture of an organisation has been described[16] as the shared values, attitudes and patterns of behaviour that give the organisation its particular character.

337 The term 'safety climate' has a very similar meaning to safety culture. Put simply, the term 'safety culture' is used to describe behavioural aspects (what people do), and the situational aspects of the company (what the company has). Safety climate is used to refer to how people feel about safety in the organisation.[16,33]

338 When implementing guidance on leadership and safety culture for fuel transfer and storage activities, organisations should focus on ensuring that:

- clear goals and objectives are set, and made visible by leadership throughout the organisation;
- expectations are translated into procedures and practices at all levels;
- these procedures and practices are commensurate with the risk, consequence of failure, and complexity of the operation;
- all hazards are considered when implementing these expectations – personal and process safety, security and environmental;
- the workforce actively participates in the delivery of these expectations;
- there is open communication and consultation across all levels of the organisation;
- relevant metrics are set and performance assessed at appropriate intervals to determine the effectiveness of leadership across the organisation;
- lessons from incidents/near misses are shared across the organisation; and
- when the organisation uses the services of others, these additional requirements are to be used, commensurate to the task they perform.

339 There is a reasonable amount of guidance available on organisational culture:

- the Baker Panel Report[3] includes a questionnaire used for a process safety culture survey, ie it is about process safety, and not personal safety, and could be adapted as required for a review of safety culture/climate;
- the CSB Investigation Report[54] includes an analysis of safety culture, in relation to the Texas City explosion, and recommendations for improvement;
- HSG48[16] summarises the organisational factors associated with a health and safety culture, and proposes a step-by-step approach to improving this culture; and
- Human Factors Toolkit Briefing Note 7[55] is a concise briefing note providing a useful summary of the characteristics of a healthy safety culture.

340 *Leadership for the major hazard industries* INDG277[56] provides useful guidance for executive directors and other senior managers reporting to board members. It is divided into four sections:

- health and safety culture;
- leadership by example;
- systems; and
- workforce.

Each section consists of brief key points followed by more detailed explanation, to refresh knowledge of effective health and safety leadership and to challenge continuous improvement of health and safety performance.

341 *A review of safety culture and safety climate literature for the development of a safety culture inspection toolkit* RR367,[57] provides a review of safety culture and safety climate literature. It is a comprehensive research report that highlights key aspects of a good safety culture, as outlined below:

- leadership;
- key criteria of successful leadership, to promote a positive safety culture, are:
  - giving safety a high priority in the organisation's business objectives;
  - high visibility of management's commitment to safety; and
  - effective safety management systems.

Communication

342 A positive safety culture requires effective channels for top-down, bottom-up and horizontal communications on safety matters.

Staff involvement

343 Active employee participation is a positive step towards controlling hazards. In particular:

- ownership for safety, particularly with provision of safety training;
- safety specialists should play an advisory or supporting role;
- it should be easy to report safety concerns; and
- feedback mechanisms should be in place to inform staff about any decisions that are likely to affect them.

344 *Involving employees in health and safety* HSG217[58] provides more detailed guidance on employee involvement.

A learning culture

345 A learning culture, vital to the success of the safety culture within an organisation:

- enables organisations to identify, learn and change unsafe conditions;
- enables in-depth analysis of incidents and near misses with the sharing of feedback and lessons; and
- requires involvement at all levels.

A just and open culture

346 Companies or organisations with a blame culture over-emphasise individual blame for human error at the expense of correcting defective systems:

- organisations should move from a blame culture to a just culture;
- those investigating incidents should have a good understanding of the mechanism for human error;
- management should demonstrate care and concern for employees; and
- employees should feel that they are able to report issues or concerns without fear of blame or possible discipline.

Process safety management

347 The COMAH Regulations require the operator of a COMAH establishment to demonstrate that a major accident prevention policy and a safety management system for implementing it have been put into effect in accordance with the information set out at Schedule 2 of the Regulations.

348 One of the recommendations of the report of the BP US Refineries Independent Safety Review Panel (the Baker Report)[3] was that BP should establish and implement an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces and manages process safety risks at its US refineries. These recommendations are equally applicable to sites with Buncefield-type potential.

Implementing a process safety risk management system

349 COMAH establishments are required to ensure that their Major Accident Prevention Policy (MAPP) adequately addresses process safety, and that they have implemented effective arrangements for process safety management. This involves establishing and implementing an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces and manages process safety risks at those sites. The system should be endorsed at senior management level, and be communicated at all levels at those sites.

350 Process safety management involves a particular type of risk management – identifying and controlling the hazards arising from process activities, such as the prevention of leaks, spills, equipment malfunctions, over-pressures, excessive temperatures, corrosion, metal fatigue, and other similar conditions. Process safety programs focus on, among other things, the design and engineering of facilities; hazard assessments; management of change; inspection, testing and maintenance of equipment; effective alarms; effective process control; procedures; training of personnel; and human factors.

351 The Center for Chemical Process Safety (CCPS) of the American Institution of Chemical Engineers (AIChE) has produced a series of books identifying good practice on various aspects of process safety management. *Guidelines on risk based process safety* AIChE Center for Chemical Process Safety (CCPS) 2007,[59] is a comprehensive reference on process safety management. It is a recent publication, building on the earlier publications in the series and integrating lessons learned over the intervening years.

352 *Process safety management systems* HSE/HID/OSD Internal Document,[60] largely identifies principles of process safety management from the earlier guidance produced by CCPS. Although intended for process safety management of offshore installations, many of the principles are equally applicable onshore. Key points are:

- there is no single 'correct' model of a process safety management system; some companies have separate safety management systems for different sites, whereas others may adopt a more functional approach;
- some companies give greater emphasis than others to corporate procedures. Each should adopt arrangements that are appropriate for its business and culture;
- in principle, different standards and procedures could be used within each of the sites or functions. In practice, however, systems need to be developed within the constraints of the corporate SMS, and there will inevitably be areas of overlap;
- there is no legal requirement for a company to have a policy statement that is specific to process safety management, but it is recognised good practice, and helps to define the management requirements; and
- a good policy statement, or supporting documentation, would indicate the organisation's approach to process safety management.

353 The COMAH Regulations require operators of COMAH sites to set out a Major Accident Prevention Policy (MAPP). The MAPP would be the logical place to record policies relating to process safety management. Companies also need to ensure that they have effective arrangements to implement each element of the policy.

Hazard identification, layers of protection, and assessment of their effectiveness

354 Before Buncefield, vapour cloud explosions (VCEs) were not considered as a likely scenario at fuel storage sites. The current uncertainty regarding the explosion mechanism at Buncefield suggests that such an approach may no longer be valid.

355 Developing process safety performance indicators involves identifying the risk control systems in place for each scenario, and determining which of these are important to prevent or control the various challenges to integrity.[17] It is therefore essential to be able to provide an overview of:

- the barriers to major accidents (ie layers of protection);
- what can go wrong; and
- risk control systems in place to control these risks.

356 Various techniques are in use within the industry to give an overview of the layers of protection and evaluate their effectiveness. There is an opportunity to extend good practice within the industry.

357 One of the critical stages for developing process safety performance indicators also involves identifying the risk control systems in place for each scenario, and determining which of these are important to prevent or control the

various challenges to integrity. It is essential, therefore, to be able to provide an overview of:

- the barriers to major accidents;
- what can go wrong; and
- risk control systems that are in place to control these risks.

Identification and assessment of layers of protection

358 One of the principles of a MAPP is that the site operator should develop and implement procedures to systematically identify and evaluate hazards arising from their activities (in both normal and abnormal conditions). These procedures should address human factors with the same rigour as engineering and technical issues, and should be described in the SMS. There should also be systematic procedures for defining measures to prevent major accidents and mitigate their consequences.

359 Techniques used within the industry to help make decisions about the measures necessary include:

- bow-tie diagrams;
- layer of protection analysis (LOPA);
- fault/event trees; and
- tabular records of the hierarchy of control measures.

360 **A bow-tie diagram** is a means of representing the causes and consequences of a hazardous occurrence, together with the elements in place to prevent or mitigate the event. The 'knot' in the middle of the bow-tie represents the hazardous event itself. Such an event might be 'Loss of containment' or 'Storage tank overfill' etc.

361 There may be a number of 'causes' that lead to this event (eg human error, corrosion) and these are each listed on the left-hand side of the diagram. For each 'cause', safety elements that will serve to prevent or reduce the likelihood of the event are represented as 'barriers'. These 'barriers' may be physical (eg cathodic protection system to prevent corrosion) or procedural (eg speed limits).

362 If the event does occur, it is likely that there will be a number of possible 'outcomes' (eg fire, explosion, toxic effects, and environmental damage). These 'outcomes' are represented on the right-hand side of the diagram. As with the 'causes', safety elements serving to mitigate the effect of the hazardous event and prevent the 'outcome' are listed for each 'outcome'. Again, these may be hardware (eg bunding, foam pourers) or procedural (eg ignition control, spill response).

363 Bow-tie diagrams have a number of advantages. They:

- provide a visual representation of causes/outcomes/barriers;
- are easily understood and absorbed;
- may be developed in a workshop setting similar to a HAZID (hazard identification);
- may be used to rank outcomes using a risk matrix; and
- help identify 'causes' with inadequate barriers.

364 Bow-tie diagrams can be used as a stand-alone qualitative hazard identification tool or as the first step in a quantified risk assessment. Depending on the software used, the data in a bow-tie diagram may be output as a hazard register and responsibilities for ensuring that barriers are effective may be assigned.

365 **Layer of protection analysis (LOPA):** In the last ten years or so, LOPA has emerged as a simplified form of quantitative risk assessment (QRA). LOPA is a semi-quantitative tool for analysing and assessing risk. This analytical procedure looks at the safeguards on a process plant to evaluate the adequacy of existing or proposed layers of protection against known hazards. It typically builds on the information developed during a qualitative hazard evaluation, such as a process hazard analysis (PHA) and can be used to meet the risk assessment requirements of BS EN 61508[18] and BS EN 61511.[2] Significant scenarios are identified and frequencies are estimated for the worst-case events. Risk categories are assigned to determine the number of independent protection layers (IPLs) that should be in place. For a measure to be an IPL it should be both independent and auditable.

366 **ARAMIS:** A project funded by the European Commission on Accidental Risk Assessment Methodology for Industries (ARAMIS), in the context of the Seveso II Directive, has recently been completed. The project aimed to develop a harmonised risk-assessment methodology to evaluate the risk level of industrial establishments by taking into account the accident-prevention tools (safety devices and safety management) implemented by the operators.

367 The user guide to ARAMIS, which has the following major steps, is available online:[61]

- methodology for identification of major accident hazards (MIMAH);
- identification of safety barriers and assessment of their performances;
- evaluation of safety management efficiency to barrier reliability;
- identification of reference accident scenarios;
- assessment and mapping of the risk severity of reference scenarios; and
- evaluation and mapping of the vulnerability of the plant's surroundings.

368 **MIMAH** is a standardised systematic approach for the identification of hazards. MIMAH is complementary to existing methods, such as HAZOP (hazard operability study), FMEA (failure modes and event analysis), checklists etc and ensures a better exhaustiveness in terms of hazard- and safety-barrier identification. Bow-ties are the basis of MIMAH methodology in ARAMIS. LOPA is a means of assessing the performance of safety barriers.

369 Evaluation of SMS efficiency is based on:

- identification of the safety barriers in the technical system;
- assessment of the SMS using an audit; and
- an assessment of safety culture using questionnaires.

370 The results of the two assessments are processed and modify the nominal reliability of the safety barriers, thereby linking the quality of the SMS with the quality of the barrier.

Emergency response arrangements

Future work: The sector and the Competent Authority plan, in co-operation with the emergency services and relevant local authority and government departments, to address outstanding issues raised in the MIIB's report on emergency response.[50]

Part 4: Comparison of BSTG recommendations with the MIIB report on the design and operation of fuel storage sites

Topic	Extent to which the recommendations in the MIIB design and operation report have been addressed.
Systematic assessment of safety integrity levels	
Control and safety systems for petroleum storage tanks	MIIB Recommendation 1: Agreed methodology for the determination of safety integrity levels (SIL). BSTG action fully addresses this issue.
Incorporating the findings of SIL assessments into COMAH safety reports	MIIB Recommendation 1: Application of SIL methodology to be demonstrated in COMAH safety report. BSTG action fully addresses this issue.
Protecting against loss of primary containment using high-integrity systems	
Management systems for maintenance of equipment and systems to ensure their continuing integrity in operation	MIIB recommendations: 2.1: Periodic proof testing of 'high-high' level detection. 2.2: Changes to equipment and systems to ensure any such changes do not impair the effectiveness of equipment and systems. 4: Overall system engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity. 5: High-high level detection/shut-off system should be proof tested. BSTG action fully addresses these issues.
High-integrity, automatic operating overfill prevention systems	MIIB Recommendation 3: Fitting a high-integrity, automatic operating level detection and shut-off system that is physically and electrically separate and independent from the tank gauging system. BSTG action partially addresses this issue. Further work required by PPSLG. In the first instance this will be to resolve the practical difficulties associated with pressure surge.
Tank overfill prevention: defining tank capacity	No MIIB design and operation recommendation on this issue. BSTG initial recommendation.[9]
Fire-safe shut-off valves	No MIIB design and operation recommendation on this issue. BSTG initial recommendation.
Remotely operated shut-off valves (ROSOVs)	No MIIB design and operation recommendation on this issue (for tank outlets). BSTG initial recommendation.

Topic	Extent to which the recommendations in the MIIB design and operation report have been addressed
Testing of overfill protection systems	MIIB recommendations: 4: Overall system engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity. 5: High-high level detection/shut-off system should be proof tested. BSTG action fully addresses these issues.
Safe management of fuel transfer	MIIB recommendations: 6: The receiving site has ultimate control of tank filling. The receiving site should be able to terminate a transfer without depending on the actions of a remote third party. 7: The sector and the Competent Authority should review the adequacy of existing safety arrangements, including communications, employed by those responsible for pipeline transfers of fuel. BSTG action fully addresses these issues.
Maintenance of records	MIIB Recommendation 9: Arrangements for the systematic maintenance of records. BSTG work in progress – further work required on this issue.
Engineering against loss of secondary and tertiary containment	
Leak-tight bund walls	MIIB Recommendation 17: The Competent Authority and the sector should jointly review existing standards for secondary and tertiary containment with a view to producing revised guidance by end of 2007. BSTG action partially addresses these issues. Further work required.
Bund floors – exposed floor surfaces	
Fire-resistant bund wall joints	
Bund capacity	
Firewater management and control measures	MIIB Recommendation 17: Further work required to fully address this issue.
Tertiary containment	MIIB Recommendation 17: BSTG action partially addresses this issue. Further work required.
High reliability organisations	
Roles, responsibilities and competence	MIIB Recommendation 19: Industry and the Competent Authority develop guidance/standards on how to achieve a high reliability industry. BSTG action partially addresses this issue. Further work required.
Staffing and shift work arrangements	MIIB Recommendation 19: BSTG action partially addresses this issue. Further work required.

Topic	Extent to which the recommendations in the MIIB design and operation report have been addressed.
Shift handover	MIIB Recommendation 19: BSTG action partially addresses this issue. Further work required.
Organisational change and management of contractors	MIIB Recommendation 19: BSTG action partially addresses this issue. Further work required.
Management of plant and process changes	MIIB Recommendation 19: BSTG action partially addresses this issue. Further work required.
Delivering high performance through culture and leadership	
Process safety culture and leadership	General MIIB recommendation: Implementing [the MIIB] 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. The sector, in consultation with the Competent Authority, needs to put in place continuing arrangements for leadership in relation to operating and safety standards on a long-term basis. Action to improve sector leadership will be the key to facilitate implementation of [the MIIB] recommendations and to provide a focus for continuous improvement. BSTG work in progress. Further work required to fully address this issue.
Process safety management	General MIIB recommendation. BSTG work in progress. Further work required to fully address this issue.
Hazard identification, layers of protection and assessment of their effectiveness	General MIIB recommendation. BSTG work in progress. Further work required to fully address this issue.
Performance evaluation and process safety performance measurement	MIIB recommendations: 9: 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. 23: Arrangements to collate incident data on high potential incidents, evaluate trends, and communicate information on risks, their related solutions and control measures to the industry. 24: Thorough investigation of root causes of failures and malfunctions of safety and environmental protection critical elements during testing or maintenance, or in service. Develop an incident database. Collaboration to ensure lessons are learned. BSTG action partially addresses this issue. Further work required.
Emergency arrangements	
Principles	No MIIB design and operation recommendation on this issue. BSTG new recommendation.

Topic	Extent to which the recommendations in the MIIB design and operation report have been addressed.
On-site emergency plan	No MIIB design and operation recommendation on this issue. BSTG new recommendation.
Firefighting planning and preparation	No MIIB design and operation recommendation on this issue. BSTG new recommendation.

Appendix 1: Example LOPA assessment for an overfill scenario

1 This is an example of the layers of protection analysis (LOPA) technique as applied to a tank overfill scenario. The analysis estimates the safety risk for a given scenario based on hardware reliability and human error rates, then compares this to appropriate risk tolerance criteria. This simplified example is intended to illustrate the methodology and does not provide a model solution of a SIL assessment which operators may simply adopt. A case-specific assessment will be required for each operation. To maintain the simplicity of the example, environmental risks have not been included but should be included in the case-specific assessment.

2 The extent and effectiveness of the site's management systems are critical to risk mitigation. Basic management systems (such as training, procedures, labelling, auditing, etc) are assumed to be in place when a LOPA is performed. However, more extensive systems will further reduce the risk (such as job aids, cross-checking, intelligent tank management software, etc), and should be credited within the analysis if they are present at an actual site.

3 The numbers are for illustration only. Each individual site will need to generate figures that are relevant to their own operation.

4 The example is presented in the following sections:

- Background information putting the example in context;
- Identification of applicable initiating events, independent protection layers and conditional modifiers based on the background information;
- Assigning values to be used in the example and performing the calculation (and comparing the answer to risk tolerance criteria);
- LOPA summary table (calculation);
- Description of the LOPA technique;
- Background information on human error;
- Factors affecting the values used in the LOPA example; and
- SIL 2 safety instrumented system with automatic shutdown.

Background information putting the example in context

5 A hypothetical small tank depot site has three external floating roof gasoline tanks (Tanks A, B and C), which are connected to a single-source pipeline via a manifold (see Figure 4). The depot has additional tanks storing other, less hazardous, substances and is permanently manned with operations personnel. This assessment only considers one major accident hazard (MAH) scenario associated with Tank A. The other tanks would be the subject of a similar but separate assessment.

6 Note that the overall risk is not necessarily three times the risk of Tank A, due to site layout and other factors that may be different between the tanks. In addition, other MAH scenarios and non-MAHs would need to be considered and compared to the site risk tolerance criteria.

7 The normal operation is that the receiving depot extracts an agreed discrete package of gasoline from the pipeline to a single tank at the depot. The receiving

site has the sole responsibility for stopping the transfer at the agreed volume. Therefore, for this example, the sender (ie the site supplying gasoline to the pipeline) is not relevant to the assessment and is excluded as a potential initiating event.

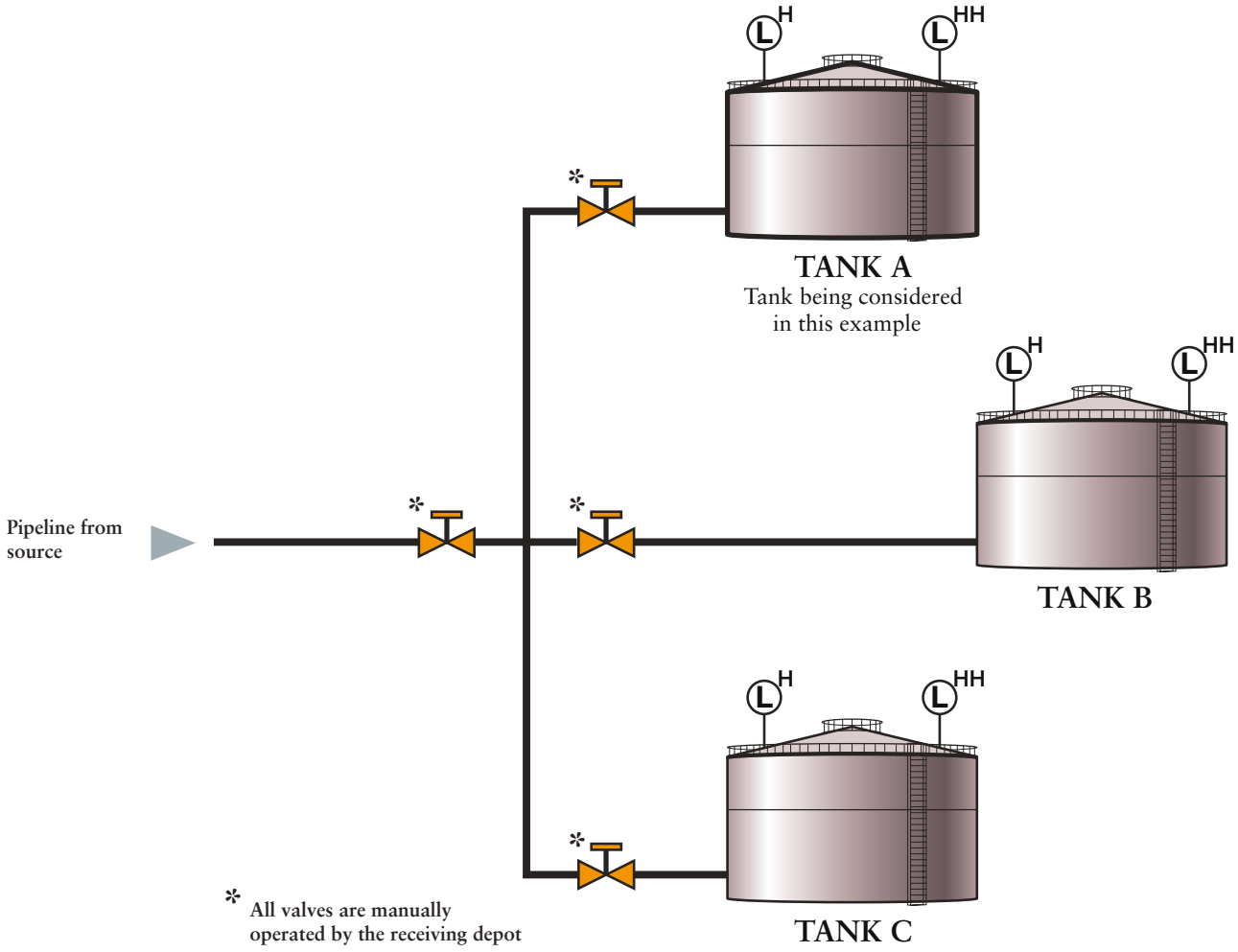


Figure 4 *Site layout*

8 Before a transfer takes place, the receiving site manually dips and cross-checks the automatic tank gauge (ATG) on the receiving tank, to confirm that it is reading correctly. All ATGs at the receiving depot are also cross-checked during a daily stock verification. Therefore, for this example, the likelihood that ATG failure is an initiating event is relatively low, but for completeness it is included as Initiating Event 3 (IE3).

9 There is one transfer per week at a flow rate of 250 m^3/hr. The average transfer volume is 3000 m^3 and therefore takes approximately 12 hours. There are clear written procedures in place at the receiving depot which detail alarm response actions required in the event of an alarm. The time to complete the alarm response actions has been assessed as 30 minutes in the worst case. The alarm response actions are simple, no diagnosis is required by the operator before taking action and there are 40 minutes between the independent high-high alarm activation and overfill. The operators at the depot undertake regular monitoring of the transfer. This includes logging all of the tank levels every hour, and cross-checking this log against the expected tank movements.

10 Competency, manning levels and workloads have been assessed and demonstrated as acceptable.

Identification of initiating events, independent protection layers and conditional modifiers based on the background information

11 This section uses a template of potential initiating events (IEs), independent protection layers (IPLs) and conditional modifiers (CMs) to select which ones are applicable to this example. The items in this section that are not applicable to the example are shown in *italics*.

Potential initiating events

12 Potential initiating events:

- Incorrect ullage calculation by the receiver (hence trying to put too much into tank).
- Incorrect tank line up (wrong tank being filled due to opening wrong valve or passing valve at receiving site).
- ATG fails to danger.
- The sender *of the transfer fails to stop at the agreed volume*:
  - sender enters/miscalculates volume;
  - sender's hardware fails to stop transfer (eg control system failure, control valve fails to close when required, etc);
  - sender's monitoring system fails (eg ATG, flows, alarms, etc);
  - *sender fails to manually stop transfer*.

Potential independent protection layers at the receiver's site

13 ATG with audible and visual alarms:

- 'stop gauge' notification set by operator to indicate the end of the transfer;
- high level alarm;
- *high-high level alarm;*
- alarms audible and visual inside a control room;
- *alarms audible and visible to the outside operator.*

14 Notes for consideration:

- control room manning during transfer is a factor;
- alarms could be automatically relayed to outside operators via radio or similar;
- sufficient time must be available for manual response to alarms;
- alarm systems must be maintained and tested at a suitable frequency; and
- defined (written) response to alarms.

15 Independent high level alarm:

- maintained and tested at a suitable frequency;
- sufficient time must be available if manual response to the alarm is required;
- *with or* without automatic shutdown;
- manual dipping (can be used instead of an ATG or as a cross-check for the ATG).

Potential conditional modifiers

16 Potential conditional modifiers (ie post overfill):

- Bund contains vapour and mist.
- Detection of overfill:
  - personnel see (directly or by CCTV) or smell overflow and act to stop transfer;
  - hydrocarbon detectors alert operator to stop transfer.
- Rate of flow (and therefore likelihood of gas cloud outside bund).
- Likelihood of conducive environmental conditions:
  - wind speed and direction;
  - ambient temperature;
  - congestion.
- Likelihood of an ignition source on site and off site.
- Likelihood of personnel in vicinity who could be affected.
- Likelihood of fatality (personnel may be there, but they may not receive fatal injuries).

Assigning values to be used in the example and performing the calculation

Worst credible consequence

17 An overfill of tank leading to large-scale leak of blended gasoline into tank bund. A vapour/mist cloud could develop and, if ignited, could lead to an explosion and large fire. Personnel within or close to the tank bund may be engulfed in the fire; however, there will be time to escape before ignition. The proximity of the tank presents a risk that off-site personnel may be affected. Therefore 'multiple fatalities' (2–10 people) is the worst-case credible consequence.

Initiating events applicable to this example

IE1: Starting a transfer with an incorrect Tank A ullage calculation (hence trying to put too much into Tank A).

18 Transfers into the tank occur on average once per week, giving a total frequency of filling of 52 times per year. Before a transfer, the operator will calculate the ullage in the tank and will enter into the control system a 'stop gauge'. The operator may make a mistake in the calculation and therefore transfer an amount that is in excess of the ullage in Tank A.

19 It will be assumed that the operator makes an error in the calculations of capacity in the tank at a rate of 1 in 100. In this case, blended gasoline will continue to be fed into the tank and potentially cause it to overfill. However, the operator will be aware of the time the blend is expected to take, and will check the tank level at least every hour during the blend. Therefore, there is a chance that the operator will notice the error, and will shut down the transfer manually before the tank overfills. The site procedures require that tank levels be cross-checked at the start of a transfer, again after 15 minutes, then subsequently every hour. The maximum fill levels of the tanks are identical and well known. Therefore the probability that the initial error is missed by cross-checks is low, and is taken as 0.1 for this example.

20 Therefore the total frequency of potential overfill is 52*0.01*0.1 = 0.052 per year. **Frequency of IE1 = 0.052 per year.**

IE2: Starting a transfer with an incorrect tank line up of Tank B or C. (Tank A being filled due to opening wrong valve when intending to fill tank B or C.)

21 In addition to transfers into Tank A, there are also transfers into Tanks B and C, 52 times per year per tank. On each occasion (of transferring to Tank B or C), there is the possibility that the gasoline is directed into Tank A in error, by making an error in valve configuration or tank line-ups. It is therefore possible that Tank A could be selected as the receipt tank in error, leading to an overfill.

22 Operators are well versed in this type of activity and it can be considered as a routine operation. Therefore, the chance that a mistake is made and that the incorrect tank is lined up to receive a gasoline transfer is taken as 1 in 1000. In addition, the site procedures require that the line-up be cross-checked by an independent operator. Therefore the probability that the initial error is missed by the cross-check is low, and is taken as 0.1 for this example.

23 By chance, Tank A may already have a low level and in such circumstances the operator will have plenty of time to recognise the mistake and rectify the situation. The probability that the tank is overfilled from a low level after a line-up mistake is considered low enough to neglect it in this LOPA. However, if the tank is already at a high level, then the operator may not notice the line-up mistake and the tank could be overfilled. It is estimated that the probability of the tank already being at a high level, when incorrectly lined-up is 1 in 2.

24 Therefore the total frequency of potential overfill is (52*2)*(0.001)*0.5*0.1 = 0.0052 per year. **Frequency of IE2 = 0.0052 per year**.

IE3: ATG fails to danger.

25 A failure modes and effects analysis (FMEA) based on site-specific data was used to generate the relevant fail to danger rates for the ATG. The three scenarios identified were:

- Gauge develops large zero drift before transfer. Zero drift is in low direction and is greater than the level difference between the ATG high alarm point and the tank maximum level point. The zero error is missed by the daily stock checks and the manual dip cross-check at the start of the transfer.
- Gauge reads correctly at start of batch but then reads progressively low as transfer is underway and is not noticed by the hourly checks. Error by end of transfer is greater than the level difference between the ATG high alarm point and the tank maximum level point.
- Gauge sticks and is not noticed by the hourly checks.

26 The FMEA study concluded that the combined frequency rate is 0.0006 per year, which includes the relevant enabling events for each scenario. The frequency is a relatively low number as the relevant failure modes must occur at specific times and remain undetected by the various checks. **Frequency of IE3 = 0.0006 per year.**

Note: For this example, an FMEA study was used. There are various methods for estimating this initiating event – any method used must be justified. The details of the FMEA study are outside of the scope of this LOPA example.

Independent protection layers at the receiver's site

IPL1: ATG with audible and visual alarms followed by operator action.

27 The depot has written procedures that clearly define operator action in the event of any alarms. The tank is fitted with a servo-type ATG, which measures the level in the tank and has a high alarm.

28 In addition to the ATG high alarm, it is standard practice for the operator to set a 'stop gauge' alarm lower than the ATG high alarm, before transfers, to warn that the end of the transfer is approaching. The 'stop gauge' alarm gives a reminder to the operator to stop transferring into the tank, in addition to general monitoring of the tank level. Both alarms are activated from the same ATG and therefore there is a common mode of failure for them.

29 The operator 'stop gauge' is only valid where feed into the tank is planned. If a tank is selected in error (eg incorrect tank line up), credit cannot be taken for it. In both cases (ie with or without the stop gauge being valid), the probability of failure on demand (PFD) of the ATG and associated operator action is estimated to be 0.1, based on limits described in BS EN 61511.
IPL1 PFD = 0.1 (includes ATG, alarms from ATG and operator response to alarms).

IPL2: Independent high level alarm

30 The independent mechanical high level float switch and alarm with operator response is defined as a safety instrumented system with a SIL 1 rating. This system has a full functional test every six months and the complete system (initiator to alarm inclusive) has a PFD of 0.007.

31 The alarm system is completely independent of the control system and requires an operator response. The emergency priority alarm is displayed in the control room in a way that anyone in the control room can respond to it (ie not only the same operator who may have missed a previous alarm).

32 The alarm response actions are simple, no diagnosis is required by the operators before taking action, and there is always more than one operator in the control room who is competent to act. Therefore a PFD of 0.01 is claimed for operator response to this alarm.

33 Total PFD is therefore a combination of the alarm working correctly, but no operator responding, plus the PFD of the alarm system itself.

Total PFD = ((1-0.007)*0.01)+0.007 = **0.017.**

Note: The example does not provide diversity of response as both IPLs are dependent on operators. More than one operator is present within the control room, but there may be common-cause failure, such as a major distraction that affects the whole site. The assessment of an actual facility would have to consider this within the LOPA and any subsequent cost–benefit analysis.

Conditional modifiers

34 Conditional modifiers (ie post-overflow) applicable to this example:

- **CM1:** Detection of overflow (personnel see or smell overflow and act to stop transfer). The depot has several low-light CCTV cameras and there will be times when someone is either close to the tank, or sees an overfill on CCTV, allowing the transfer into the tank to be stopped before a significant quantity of gasoline has been lost. This includes an elevated CCTV camera that is directed at the filling tank during a transfer to monitor the roof position. Probability that any leak goes undetected is estimated as 0.4 for this example.
- **CM2:** Probability of an ignition source on site and off site.
  The vapour/mist cloud formed could be large and may drift. Although there will not normally be sources of ignition within the bund, there may be potential sources outside of the bund and off site, therefore the vapour cloud may find a source of ignition. Probability taken as 0.3 for this example.
- **CM3:** Probability of personnel in vicinity who could be affected.
  Population in tank areas is fairly low, and within the bund is minimal. However, some of the roadways around the bunds are used by contractor work groups to move to different areas, and there may be occupancy off site, although there are no roads or occupied buildings nearby. Wind conditions may be favourable and direct the gas cloud away from people, but if the vapour/mist cloud were to drift and ignite, there is a chance that people will be present and affected. However, personnel would have a significant chance of escape before ignition, since the vapour/mist cloud would take time to drift out of the bund where occupancy is minimal. Probability taken as 0.05 for this example.
- **CM4:** Probability of fatality (personnel may be there, but may not receive fatal injuries). If a person is within the area of the explosion, there is a chance that they will be **affected, but not receive fatal injuries. Probability of fatality of 2–10 people is taken as 0.8 for this example.**

Note: The conditional modifier approach is a simplified way of considering likelihood – if sensitivity analysis indicates that these factors are critical (eg the estimated likelihood is close to the risk tolerability criteria (RTC)), a more rigorous assessment may be required (such as fault tree analysis).

35 The LOPA calculation for this example is as follows:

Likelihood = CM1xCM2xCM3xCM4x{(IE1xIPL1xIPL2)+(IE2xIPL1xIPL2)+(IE3xIPL2)}

= 0.4x0.3x0.05x0.8x{(0.052x0.1x0.017)+(0.0052x0.1x0.017)+(0.0006x0.017)}

= 5.1 E-07 or 1 in 2 million years

36 For this example site, the risk tolerance criteria for a multiple fatality (2–10 people) is taken as 1 in 1 million years (ie if the likelihood is lower than this, then the risk is broadly acceptable). Therefore, the risk in this example lies in the broadly acceptable region, and any further risk reduction should be reviewed using cost–benefit analysis.

LOPA summary table

37 The LOPA calculation is summarised in the following table:

Scenario: Petrol storage tank overfill such that the subsequent explosion results in 2–10 fatalities

Initiating events	IE1 incorrect ullage	IE2 incorrect line-up	IE3 ATG failure
Frequency per year	0.052	0.0052	0.0006
IPL1 PFD ATG alarms (SIL 0)	0.1	0.1	-
IPL2 PFD IHLA (SIL 1)	0.017	0.017	0.017

Conditional modifiers		**Probability**
CM1	Detection	0.4
CM2	Ignition	0.3
CM3	Occupancy	0.05
CM4	Fatalities	0.8

Scenario likelihood	5.1 E^{-07} per year (1 in 2 million years)
Risk tolerance criteria	$1.0E^{-06}$ per year
Risk region	Broadly acceptable

Note: The example is intended to demonstrate the LOPA method and application to gasoline tank filling operations and overfill prevention. Factors affecting the values used in the example gives the basis and justification for the data used for the example site. Each installation should use data applicable to the site circumstances, for example location, management procedures, manning levels, tank level instrumentation, alarms, shut-down systems, etc.

Description of the LOPA technique

38 To conduct a LOPA study the following should be considered:

What is LOPA?

39 LOPA is a risk assessment technique that uses order of magnitude assumptions for the consequence severity, initiating event frequency and the failure of all the protection layers.

40 The technique calculates the mitigated risk of the consequence occurring against the risk tolerance criteria by developing an initiating event frequency together with failure rate of independent protection layers and conditional modifiers, the purpose being to ensure that there are sufficient safeguards to mitigate the scenario consequence.

Terminology

41 **Risk tolerance criteria** are limiting values for the likelihood of a specified level of harm, eg minor injury, serious injury or death. Published tolerability criteria are typically concerned with the risk of death. Criteria have been proposed for lesser harm, but none have found widespread acceptance.

42 Individual sites are responsible for selecting the appropriate risk tolerance criteria for use in their risk assessment.

43 *Guidance on 'as low as is reasonably practicable'*[62] sets out the decision-making process and includes risk tolerability criteria, as illustrated in the 'ALARP Triangle' in Figure 5. An upper limit is placed on the individual risk of fatality for an employee of 1 x 10^{-3} per year. A more stringent limit of 1 x 10^{-4} per year is set for a member of the public. In both cases, the risk of death is considered broadly acceptable if less than or equal to 1 x 10^{-6} per year.

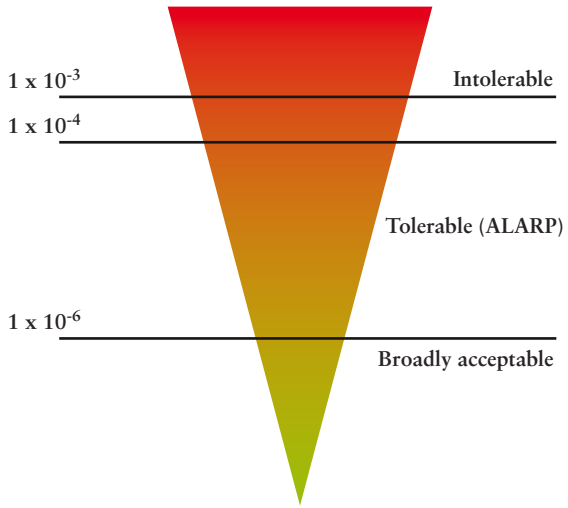


Figure 5 *ALARP – As low as reasonably practicable*

44 The LOPA uses a risk tolerance criterion of 1 x 10^{-6} per year for an event with consequences of 2–10 fatalities and equates this to a risk that is broadly acceptable. By implication, a risk that is broadly acceptable is for practical purposes ALARP (no active pursuit of further risk reduction by HSE). This simplifies the worked example, as it removes the need for further iterative steps to determine

if additional risk reduction (eg by increasing the reliability of the safety instrumented system or adding additional IPLs) would be reasonably practicable. The risk tolerance criteria is consistent with the illustrative risk matrix on the HSE website that provides guidance on ALARP.[62]

45 However, there are a couple of complications that need to be taken account of in practice:

- Firstly, it is important to note that the HSE published criteria for individual risk are concerned with the tolerability of risk from a given industrial undertaking, and not the risk from a single accident scenario. This includes other major accident risks and 'conventional' risks such as those from falls from height. There are currently no recognised single-event tolerability criteria. Those applying the LOPA technique will therefore need to develop and justify the values used in the assessment. The implication is that when there are multiple sources of hazard, the total risk from all sources must be less than or equal to the criterion value to be broadly acceptable. Hence, strictly speaking, a risk from a single accident scenario equivalent to 1×10^{-6} per year would only be broadly acceptable if it were the only possible cause of a fatality.
- Secondly, and perhaps more critically, determining tolerability criteria for events involving multiple fatalities involves a different approach. They are generally derived from graphs plotting the number of fatalities N, versus the cumulative frequency, F of all events resulting in N or more fatalities. It is therefore not strictly correct to equate the broadly acceptable criterion for individual risk of 1×10^{-6} per year with a multiple fatality event. The inaccuracy of this approximation increases with the value of N and with the number of hazardous events that contribute.

Initiating event

46 An event that when initiated could lead to an undesirable consequence. It is possible that there may be several initiating events to be considered in the scenario. It can be the case that an enabling event is required so that an initiating event becomes relevant.

Initiating event frequency

47 Once the initiation events have been determined, it is necessary to attach a frequency of the event occurring. For systems that are not continuous the failure rate data must be adjusted to reflect the time at risk. It can be equated to how many times the operation is carried out per year and multiplying the probability of failure on demand.

Independent protection layers (IPLs)

48 An independent protection layer is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence, independent of the initiating event or the action of any other layer of protection associated with the scenario. The effectiveness and independence of an IPL must be auditable.

Conditional modifiers

49 A conditional modifier is an additional assumption that modifies the probability that the scenario will result in a fatality. For example, a tank overfill may lead to overspill, but conditional modifiers would reduce the likelihood of the scenario, such as: probability of ignition, occupancy/chance of escape, fatality.

Frequency of unmitigated consequence

50 The frequency of the initiating event multiplied by the probability of an enabling event and any conditional modifiers (ie excluding the protection layers).

Frequency of mitigated consequence

51 The frequency of the unmitigated consequence multiplied by the probability of failure on demand for all the protection layers.

The team

52 LOPA requires a multi-disciplined team to perform the analysis. Typically, for the chemical industry, this could include operations personnel, process engineer, health and safety officer, instrument engineer and a person familiar with LOPA and risk assessments.

Information required to conduct LOPA

53 To effectively conduct a LOPA the following information should be available:

- risk tolerance criteria;
- data, so that initiating and enabling events and frequencies can be identified;
- information on location, occupancy etc so that any conditional modifiers can be applied; and
- details of protection layers in existence, together with PFD data if available.

Background information on human error

54 Human error data is published in various documents, for example:

- BS EN 61511 parts 1, 2 and 3:2004 *Functional safety. Safety instrumented systems for the process industry sector,*[2] table F3 which quotes a 'typical' PFD of 0.1 for operator response to alarms. However, there are no explanatory notes indicating the basis (ie in terms of amount of time available to respond). The reference states that this is a typical figure, not a minimum limit;
- *Layer of Protection Analysis*[19] quotes a PFD of 0.1 where there is a 10 minute response time, and 0.01 for a 40-minute response time, stating that 'the longer the time available for action, the lower the PFD given for human action'
- *Alarm systems – A guide to design, management and procurement* EEMUA Publication 191[63] (section 2.4.1) states a range of 0.01–0.1 for operator response to alarms within a SIL 1 system; and
- the HSE website (on safety-related systems) includes a range of 0.01–0.1, explaining that the appropriate value is dependent on response time and that it is a simple action, with well documented response, with appropriate training, that annunciator design is clear, the system is audited, etc, similar to EEMUA 191. The minimum limit is stated as 0.01.

The HSE SRAM Technical Measures[64] document on Control Systems can be found on the HSE website.

In addition, various references indicate figures of 1 in 100 to 1 in 10,000 for human performance of a routine task, including response to alarms (other than the situation of alarm flood, where the panel operator is in a highly stressed situation).

As a consequence of the Three Mile Island incident, the technical document *Handbook of human reliability analysis with emphasis on nuclear power plant applications* (Swain 1983 NUREG/CR 1983)[65] was generated. This document demonstrates that high levels of reliability are achievable with good design, management systems and appropriate manning levels. Examples of human error rates for operator response to annunciated alarms are as follows:

- 1 in 10 000 for a single panel operator;
- 1 in 100 000 for two independent panel operators;
- 6 in 100 000 for two panel operators without complete independence.

These low error rates indicate that the PFDs of 0.01 to 0.1 for operator response to alarms used in this LOPA example are conservative figures.

Table 3 *Factors affecting the values used in the LOPA example*

		Value in example	Factors and assumptions which have influenced the value used in the example	Factors that may be relevant to other sites but are not relevant to this example site
IE				• The sender of the transfer may fail to stop the transfer at the agreed volume for a number of reasons.
IE1	**Incorrect ullage**	**0.052**	• The operators at the depot undertake regular monitoring of the transfer. This includes logging all of the tank levels every hour, and cross-checking this log against the expected tank movements and rate of movement. • Manual dipping at start of each transfer to verify ATG reading. • All personnel have been adequately trained and are competent. • Workload assessments have been carried out and the depot is manned accordingly. • All depot procedures are externally audited for compliance once per year.	
IE2	**Incorrect line up**	**0.0052**	• The operators at the depot undertake regular monitoring of the transfer. This includes logging all of the tank levels every hour, and cross-checking this log against the expected tank movements and rate of movement. • Daily stock verification which cross-checks ATG readings with import/export ledger. • All personnel have been adequately trained and are competent. • Workload assessments have been carried out and the depot is manned accordingly. • All depot procedures are externally audited for compliance once per year. • Opportunity to correct un-intended action (manifold valve) is high and fully within operator's control.	

Table 3 *Factors affecting the values used in the LOPA example (continued)*

		Value in example	Factors and assumptions which have influenced the value used in the example	Factors that may be relevant to other sites but are not relevant to this example site
IE3	**ATG starts reading significantly low after transfer has started**	**0.0006**	• Manual dipping at start of each transfer to verify ATG reading is correct before transfer starts. • Daily stock verification which cross-checks ATG readings with import/export ledger. • Regular monitoring of the transfer is undertaken by the operators at the depot. This includes logging all of the tank levels every hour, and cross-checking this log against the expected tank movements and rate of movement. • All personnel have been adequately trained and are competent. • Workload assessments have been carried out and the depot is manned accordingly. • All depot procedures are externally audited for compliance once per year. • For the tank to overfill without initiating the ATG high alarm, the ATG must read low by the level equivalent to response time two plus response time three at the end of the transfer, but must be reading correctly at start of transfer, so as not to be identified as faulty by the manual dip.	
IPL				• The ATG may have more or less alarms than the example. • Alarms may be visual/audible to field operators in addition to control room operators. • ATG may have different reliability than the non-SIL certified servo gauge used in the example. • Intelligent tank management software to identify unexpected tank level changes; 'moving' and 'stuck' alarms. • Tank management software to prevent ullage calculation errors. • Automated link to final element from high-level sensor. • Hydrocarbon gas detection in bund area. • Automated or manual verification of correct line up before transfer. • Consignment agreement with supplier.

Table 3 *Factors affecting the values used in the LOPA example (continued)*

		Value in example	Factors and assumptions which have influenced the value used in the example	Factors that may be relevant to other sites but are not relevant to this example site
IPL 1	**ATG high alarm and/or stop gauge alarm followed by operator action**	**0.1** **(SIL 0)**	● Clear written procedures detailing alarm response actions. ● ATG has a high alarm plus an Operator configurable 'stop gauge' alarm. PFD used is combination of both ATG alarms. ● ATG and ATG alarms have not been designed to BS EN 61511. ● Alarm response actions are simple and no diagnosis is required by Operator before taking action. ● Sufficient time is available for manual response to alarms. ● Time to complete alarm response action is 30 minutes in worst case. ● All equipment is maintained and tested at a suitable frequency. ● All depot procedures are externally audited for compliance once per year. ● ATG accuracy is effectively checked once per week by the manual dipping at start of each transfer. ● Opportunities readily available to derive supporting evidence for ATG and Ind HH: ATG analogue trend data, hourly log, known average flow rate and all tank levels displayed in control room. ● Personal consequence of failing to respond to alarm(s) is very high for self and colleagues.	
IPL 2	**Indepe-ndent high-high level alarm followed by operator action**	**0.017** **(SIL 1)**	● Control room is permanently manned with multiple operators. ● Clear written procedures detailing alarm response actions. ● Time to complete alarm response action is 30 minutes in worst case. ● Alarm response actions are simple and no diagnosis is required by operator before taking action. ● Mechanical float switch linked to independent alarm. ● System has full functional test every six months. ● Completely independent of control system. ● The alarm is displayed in the control room in a way that anyone in the control room can respond to it (ie not only the same operator who may have missed a previous alarm). ● Several operators in control room are competent to respond to this alarm.	

Table 3 *Factors affecting the values used in the LOPA example (continued)*

		Value in example	Factors and assumptions which have influenced the value used in the example	Factors that may be relevant to other sites but are not relevant to this example site
			• All depot procedures are externally audited for compliance once per year. • Personal consequence of failing to respond to alarm(s) is very high for self and colleagues.	
CM				• Rate of flow and therefore likelihood and extent of gas cloud outside bund. • Likelihood of conducive environmental conditions (wind speed and direction, ambient temperature, tank farm layout and congestion level).
CM 1	**Detection of overfill**	**0.4**	• Depot has several low-light CCTV cameras which display in the control room. • Control room is permanently manned with multiple operators. • Tank farm is occupied for 5% of time (see CM3). Personnel in vicinity would act to stop transfer on seeing or smelling an overfill.	
CM 2	**Probability of finding ignition source**	**0.3**	• Tank farm has very few sources of ignition in immediate vicinity. • If vapour cloud was sufficiently large, it could find ignition source.	
CM 3	**Probability of two or more people in vicinity**	**0.05**	• Occupancy of tank farm area is relatively low and is likely to be individuals rather than groups. • Some contractor work groups use roadways adjacent to bunds. • Personnel would have a significant chance to escape before ignition, as vapour cloud would take time to drift out of bund where occupancy is minimal.	
CM 4	**Probability of fatality**	**0.8**	• Personnel within the general area of the tank farm at time of explosion may be injured, rather than killed. • Even in immediate area, some protection will be afforded by bunds, other tanks or being within vehicles. • Factor is based on two or more fatalities.	

In this example, for the control system(s) to operate at the appropriate SIL it is essential that the following conditions are met at all times while any tank is being filled:

- operators at the depot undertake regular monitoring of the transfer. This includes logging all tank levels every hour, and cross-checking this log against the expected tank movements and rate of movement;
- manual dipping at start of each transfer to verify the automatic tank gauge (ATG) reading;
- all personnel have been adequately trained and are competent;
- workload assessments have been carried out and the depot is manned accordingly;
- all depot procedures are externally audited for compliance once per year;
- daily stock verification to cross-check the ATG readings with the import/export ledger;
- clear written procedures detailing alarm response actions are displayed in the control room;
- alarm response actions are simple and no diagnosis is required by the operator before they are able to take action;
- sufficient time is available for manual response to alarms;
- the time to complete alarm response action is 30 minutes in the worst case;
- all equipment is maintained and tested at a suitable frequency;
- the control room is manned with multiple operators during filling operations;
- the system has a full functional test every six months;
- the alarm is displayed in the control room in a way that anyone in the control room can respond to it (ie not only the same operator who may have missed a previous alarm);
- several operators in the control room are competent to respond to this alarm; and
- the depot has several low-light CCTV cameras that display in the control room.

SIL 2 Safety instrumented system with automatic shutdown

The following example illustrates a LOPA study incorporating a SIL 2 safety instrumented system that includes an automated emergency shutdown (ESD) valve. As with the previous example this is not a model solution as each site will be required to undertake a site-specific assessment.

The provision of automation is one way of addressing the issue of diversity of human response. However, the installation of a new ESD may have other consequences that need to be considered (eg blocking in against a ship transfer or the rundown from a refinery processing unit). Detailed consideration of automated shutdown systems and determination of practical solutions for flow blockage and pressure surge will form part of the future work of PPSLG.

Scenario: Petrol storage tank overfill such that the subsequent explosion results in 2–10 fatalities

Initiating events	IE1 incorrect ullage	IE2 incorrect line-up	IE3 ATG failure
Frequency per year	0.052	0.0052	0.0006
IPL1 PFD ATG alarms (SIL 0)	0.1	0.1	-
IPL2 PFD IHLA with ESD(SIL 2)	0.017	0.005	0.005

Conditional modifiers		**Probability**
CM1	Detection	0.6
CM2	Ignition	0.3
CM3	Occupancy	0.05
CM4	Fatalities	0.8

Scenario likelihood	2.3 E^{-07} per year (1 in 4 million years)
Risk tolerance criteria	1.0E^{-06} per year
Risk region	Broadly acceptable

Appendix 2: Defining tank capacity

Worked example 1

1 The following is an example of the application of this guidance to an actual tank.

Tank parameters

2 The tank in this example is a fixed roof type (no internal floating roof) with a shell height of 20 m measured from the base, which is flat and level. The tank has a nominal maximum capacity of 10 000 m^3 if filled to the overfill level. It receives a product with an SG of less than 1.0, at rates up to a maximum of 1200 m^3/hr.

Maximum capacity (overfill level)

3 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank. For fixed roof tanks without an internal roof, loss of containment is expected to occur from a fitting in the roof, typically a PV valve or a dip hatch (if open). For the purposes of setting alarms the overfill level for tanks of this type is considered to be the top of the shell. This gives additional safety margins and greatly simplifies the overfill calculation. Thus for this example the overfill level is defined as the top of the shell. This is 20 m above the base of the tank.

LAHH

4 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

5 On this tank, the LAHH includes a trip function to terminate the transfer. For a well-designed and maintained safety instrumented protective system, a response time of two minutes between activation and complete cessation of flow into the tank is claimed. This includes the time needed to take urgent action in case the trip action is not successful – in this case to immediately close another remotely operated valve, readily accessible in the control room (the system having been designed for this emergency closure).

6 This equates to a maximum volume of 2 x 1200/60 = 40 m^3. Based on the tank dimensions, this is equivalent to a height of 0.08 m. Thus, the LAHH is set 0.08 m below the overfill level at 19.92 m.

7 There might need to be an additional allowance added to this bare-minimum figure, for ‘level surges’ during filling, and also possible thermal expansion of the contents after the transfer has been stopped.

LAH

8 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail.

9 In this case, a response time of five minutes is claimed between activation of the LAH and complete cessation of flow into the tank.

10 This equates to a maximum volume of 5 x 1200/60 = 100 m^3. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the LAH is set 0.2 m below the LAHH, or 0.28 m below the overfill level, at 19.72 m.

Normal fill level

11 The process control system should ensure that all filling operations are terminated at the pre-determined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

Worked example 2

12 The following is a second example of the application of this guidance to an actual tank.

Tank parameters

13 The tank in this example is an internal floating roof type with a shell height of 20m measured from the base, which is flat and level. The tank has a nominal maximum capacity of 10 000 m^3 if filled to the overfill level. It receives a product with an SG of less than 1.0, at rates up to a maximum of 1200 m^3/hr.

Maximum capacity (overfill level)

14 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank.

15 For internal floating roof tanks a level must be established at the point where the floating roof will be damaged by any internal roof structure. Hence for these tanks this level will always be below the top of shell.

16 For this example the overfill level is determined as the point at which the internal floating roof strikes an internal stiffening spar located 0.25 m below the top of the shell. The floating roof is 0.25 m deep. Thus the overfill level is 0.5 m below the top of the shell, or 19.5 m above the base of the tank.

LAHH

17 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

18 On this tank, the LAHH includes a trip function to terminate the transfer. For a well-designed and maintained safety instrumented protective system, a response time of two minutes between activation and complete cessation of flow into the tank is claimed. This includes the time needed to take urgent action in case the trip action is not successful – in this case to immediately close another remotely operated valve, readily accessible in the control room (the system having been designed for this emergency closure).

19 This equates to a maximum volume of 2 x 1200/60 = 40 m^3. Based on the tank dimensions, this is equivalent to a height of 0.08 m. Thus, the LAHH is set 0.08 m below the overfill level at 19.42 m.

20 There might need to be an additional allowance added to this bare-minimum figure, for 'level surges' during filling, and also possible thermal expansion of the contents after the transfer has been stopped.

LAH

21 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail.

22 In this case, a response time of five minutes is claimed between activation of the LAH and complete cessation of flow into the tank.

23 This equates to a maximum volume of 5 x 1200/60 = 100 m3. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the LAH is set 0.2 m below the LAHH, or 0.28 m below the overfill level, at 19.22 m.

Normal fill level

24 The process control system should ensure that all filling operations are terminated at the pre-determined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

25 The normal fill level and the LAH should not coincide. The normal fill level and LAH should be close to maximise the usable capacity of the tank, but sufficiently separated so as to avoid spurious alarms, eg due to level surge or thermal expansion when the tank is filled to the normal fill level.

26 Any process alarm/notification used to indicate that the normal fill level has been reached must be clearly distinguishable from the LAH, and reflect the higher priority response applicable to the LAH.

27 In this example, an allowance of five minutes is given for the process control system (including the operator) to terminate the transfer when the level reaches the normal fill level. This equates to a maximum volume of 5 x 1200/60 = 100 m^3. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the normal fill level is set 0.2 m below the LAH, or 0.48 m below the overfill level, at 19.02 m.

Worked example 3

28 The following is a third example of the application of this guidance to an actual tank.

Tank parameters

29 The tank in this example is an external floating roof type with a shell height of 22 m measured from the base (which is flat and level) and a diameter of 24 m giving 450 m^3/m. It receives a product with an SG of less than 1.0, at rates up to a maximum of 1100 m^3/hr, resulting in a rising level rate of 2.43 m^3/hr.

Maximum capacity (overfill level)

30 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank. The company standard for its external floating roof tanks requires:

- 800 mm for the depth of the floating pontoon;
- 750 mm for the depth of the primary and secondary seal;
- 50 mm additional free clearance between moving parts of the roof and seal, and any parts fixed to the shell.

The total allowance is therefore 1600 mm, and so the overfill level is this distance below the top of the shell, or 20.4 m above the base of the tank.

LAHH

31 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

32 This tank does not have a trip function to terminate the transfer. The company has determined the actual response time for all its tanks, based upon actual timed emergency response exercises, has documented that as part of its tank level documentation, would review it when any relevant change was made, and tank level documentation is included on its audit schedule. Rather than use specific values per tank, a conservative value of 10 minutes is used for all tanks, in order to achieve standardisation and clarity.

33 This 10 minutes equates to a height margin of 0.4 m (2.43 x 10/60). Thus, the LAHH of the independent device is set 0.4 m below the overfill level at 20.0 m.

LAH

34 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail. In this case, the company uses the same 10 minutes response time, having confirmed that the same actions would be taken between activation of the LAH and complete cessation of flow into the tank. Again, the 10 minutes margin results in another 0.4 m drop to this LAH setting for the ATG at 19.6 m.

Normal fill level

35 The process control system should ensure that all filling operations are terminated at the predetermined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

36 The normal fill level and the LAH should not coincide. The normal fill level and LAH should be close to maximise the usable capacity of the tank, but sufficiently separated so as to avoid spurious alarms, eg due to level surge or thermal expansion when the tank is filled to the normal fill level. This is the point at which operations stop the transfer, and valves are closed. The company has decided that its 10 minute gap is again applicable, and so the normal fill level is set at 19.2 m.

37 Any process alarm/notification used to indicate that the normal fill level has been reached must be clearly distinguishable from the LAH, and reflect the higher

priority response applicable to the LAH. This alarm is on the company's tank information system computer. This particular company also sets an additional 'warning' level, again in the TIS, which is intended to alert operations to prepare to stop the transfer. The 10 minutes is again used, to give 18.8 m.

Appendix 3: Job factors for management of fuel transfer

1 The following job factors should be taken into account when establishing systems and procedures governing the safe transfer of fuel:

Planning tools

- Provision of clear information on short-term and long-term outages of plant or instrumentation.
- Provision of job aids for calculating availability, eg when filling multiple tanks.
- Provision of equipment to allow effective communication between all parties.
- Provision of user-friendly plans to communicate and agree plans between planners/senders and receivers.
- Good planning tools to predict end of transfer.

Site facilities

- Clear information on expected and actual flows and rates.
- Clear displays of levels/ullages.
- Manageable alarm and information systems – good practice applied in design.
- Clear labelling of plant and equipment, in the field and in the control room.
- Labelling systems to avoid confusing tanks, pipes and pumps.
- Adequate lighting.
- Facilities/arrangements to minimise distractions at shift handover.
- Reliable equipment eg valves that work.
- Adequate maintenance of facilities.

Job design

- Jobs designed to keep operators motivated.
- Operators not overloaded/distracted from responding.

Information, instructions and procedures

- Clear, unambiguous, user-friendly information and diagrams of plant.
- Instructions/job aids for line setting allowing operators to see clearly all valves needing to be checked.
- Procedures for non-routine settings.
- Procedures to transfer product from sender to receiver.
- Procedures for verification that the correct movement has begun.
- Arrangements to identify unauthorised line movement.
- Procedures for monitoring flow and fill.
- Clear unambiguous displays of levels/alarms and plant status.
- Clear instructions to take on alarm.
- Procedures for changeover.
- Feedback to confirm correct operation of valves.

- Check lists for complex, infrequently used, or critical systems.
- Contingency procedures for abnormal situations.
- Ability to recover current or established settings after a system crash.

Emergency response systems and procedures

- Emergency procedures taking account of power/air failures, fires/explosions and floods.
- Systems for emergency shutdown.
- Reliable communication links, including inter-site links.
- Emergency control centre with adequate equipment and information aids.
- Criteria for activating emergency response plans.
- Suitable means of raising the alarm, on site and off site.
- Efficient call-out system (eg automated phone system, duty rota).
- Suitable PPE.
- Suitable muster areas, including safe havens, and equipment.
- Suitable means of detection, including patrols, CCTV, gas detection.
- Suitable isolations.
- Clear identification and labelling of plant.
- Suitable site access arrangements.
- Planning for recovery after an event.

Appendix 4: Key requirements for operational planning

1 The BSTG has analysed the human factor isues involved at the various safety-critical stages in fuel transfer operations, including operational planning. We are not aware of any authoritative guidance in this area. This Annex records the various factors identified, so that they may act as an aide memoire for senders and receivers in their review of procedures for agreeing and communicating operational plans. Operational planning takes into account all stages of the plan development and approval, up to the stage of implementation via the consignment transfer agreement.

Job factors

2 Job factors for effective planning include:

- the provision of a clear stock control policy, eg maximum and minimum working levels, maximum flow rates, maximum number of parcels, strategic stock levels, workable contractual rules, tank throughput per year etc;
- clear communication protocols between planning/sender and receiver (eg the consignment transfer agreement);
- effective tools to communicate receiver plant information to planners (INPUT);
- effective tools/programmes to communicate plans to receivers (OUTPUT);
- reliability of equipment and systems;
- availability of suitable planning procedures;
- jobs designed to keep staff motivated; and
- flexibility in the planning arrangements.

Person factors

3 Person factors include the following characteristics, skills and competencies:

- to work under pressure and multi-task;
- understanding of the site;
- numeracy;
- communication skills (including command of English and IT systems);
- negotiation skills; and
- ability job interest/motivation.

Organisational factors

4 Factors important to organisational success include:

- the safety culture of all parties involved;
- the use of suitable stock control policies;
- the provision of adequate resources to cover all modes, eg absence of key staff, out-of-hours issues, changes to plan, emergencies;
- defining clear roles and responsibilities, and providing adequate supervision;
- defining clear communication channels between sender and receiver;
- identifying potential conflicts, and providing mechanisms to resolve them;

- ensuring staff (eg shift team members) are not fatigued and have a manageable work load; and
- empowering people to stop imports if necessary

Assurance factors

5 Factors important to assuring overall success include:

- setting key performance indicators for deviations from plan (eg hitting the high level alarm, number of stock outs, number of in-line amendments, highest level etc);
- investigation of incidents and near misses arising from planning failures, and sharing the lessons across all parties;
- ensuring there is a mechanism for feedback from the receiver to the sender on the quality of operational plans; and
- including the examination of operating practice against the policy and procedure as part of audit arrangements.

Appendix 5: Process safety performance indicators

Example workbook for a fuel storage terminal with pipeline and jetty filling

This annex provides a worked example of process safety performance indicators developed using *Developing process safety performance indicators: A step-by-step guide* HSG254.[17]

The steps in this appendix follow the key steps in HSG254.

Description of the site and activities

This example is based on a typical operational terminal with both pipeline and jetty filling. The site boundary at the point of jetty operations was selected – ship and marine activities were out of scope.

Fuel products are delivered to site from ships or via cross-country pipeline and loaded into bulk tanks. Product from bulk tanks are loaded onto road tanker for dispatch.

Overview of Steps 2–4

The main stages in selecting process safety indicators are:

- Step 2.2: Identify the scope:
  - identify the hazard scenarios which can lead to a major incident;
  - identify the immediate causes of hazard scenarios.
- Step 3: Identify the risk control systems and describe the outcome for each – set a lagging indicator:
  - identify the risk control systems (RCS) in place to prevent or mitigate the effects of the incidents identified;
  - identify the underlying causes;
  - identify outcomes of each RCS;
  - set a lagging indicator for each RCS.
- Step 4: Identify critical elements of each RCS and set a leading indicator:
  - identify the most critical elements of the risk control system and set leading indicators for each element;
  - set a tolerance for each leading indicator;
  - select the most relevant indicators for the site or activities under consideration.

Step 2.2: Identify the scope

Step 2.2.1: Identify the hazard scenarios which can lead to a major incident

Describing the main incident scenarios helps to maintain a focus on the most important activities and controls against which indicators should be set. The scenarios form a useful cross-check later on in Step 4 when the critical elements of risk control systems to be measured are determined.

For this site the main process safety incident scenarios are loss of containment (LOC) of flammable liquid or liquid fuel dangerous to the environment, particularly to the estuary. These events may lead to:

- a pool fire, vapour cloud ignition, or for gasoline a vapour cloud explosion;
- a major accident to the environment.

Step 2.2.2: Identify the immediate causes of hazard scenarios

The immediate cause is the final failure mechanism that gives rise to a loss of containment. These usually can be considered as the factors which challenge the integrity of plant or equipment.

For this site immediate causes could be, for example:

- accidental leakage – valve left open, coupling not made correctly;
- flexible hose failure;
- pipeline failure;
- valve, pump, flange, or coupling failure;
- bulk tank failure;
- road tanker failure;
- overfilling.

Step 2.2.3: Identify the primary causes

This step is important as it a prerequisite to deciding which risk control systems are important to prevent or control the challenge to integrity. For this site primary causes could be:

- under pressure;
- lightning strike;
- overpressure;
- corrosion;
- joint flange gasket aging;
- wrong material;
- physical damage;
- subsidence;
- wrong product;
- wear;
- wrong installation;
- vibration;
- overheating;
- static discharge;
- wrong specification;
- quality of material.

Step 3.1: Identify the associated risk control systems

Draw up a risk control matrix as illustrated in Table 4, to help decide which risk control systems (RCSs) are the most important in controlling the challenges to integrity identified within the incident scenarios.

Table 4 *Risk control matrix*

Risk control systems	Challenges to integrity						
	Overfilling	Accidental leakage	Overpressure	Corrosion	Wear	Physical damage	Subsidence
Control and instrumentation	■		■				
Operational procedures	■	■	■	■	■	■	
Competence	■		■				
Inspection and maintenance	■	■	■	■	■	■	■
Design	■	■	■	■	■	■	■
PTW		■				■	
Plant change	■	■	■	■	■		
Control of contractors		■				■	

Step 3: Identify the outcome and set a lagging indicator

It is vital to discuss and agree the reason why each RCS system is in place and what it achieves in terms of the scenarios identified. Without this agreement it will be impossible to measure success in delivering this outcome.

It's best to phrase 'success' in terms of a positive outcome – supportive of the safety and business priorities. The indicator can then be set as a positive or negative metric to flag up when this is achieved or when not. As success should be the normal outcome then choosing a negative metric guards against being swamped by data (reporting by exception).

The following questions may be helpful:

- Why do we have this risk control system in place?
- What does it deliver in terms of safety?
- What would be the consequence if we didn't have this system in place?

The indicator set should be directly linked to the agreed RCS outcome and should be able to measure a company's success/failure at meeting the outcome.

Step 4: Identify the critical elements of each risk control system and set leading indicators

There are too many elements to a RCS for each to be measured. It is not necessary to monitor every part of a risk control system. Consider the following factors when determining the aspects to cover:

- Which activities or operations must be undertaken correctly on each and every occasion?
- Which aspects of the system are liable to deterioration over time?
- Which activities are undertaken most frequently?

From this the critical elements, of each risk control system important in delivering the outcome, can be identified.

1 Overpressure ship-to-shore transfer

System outcomes:

- pressure less than 10 bar.

Potential lagging indicators:

- number of times pressure in the line exceeds 10 bar when offloading.

Critical elements of the RCS:

- valves not closed against ship's pump;
- correct line up;
- ship-to-shore checks done;
- set correct discharge rate (maximum pressure and rate);
- sequence of discharge;
- set up manifold;
- emergency communications;
- radio communications;
- agreed shut down plan in place – signed both parties;
- English speaker on board ship;
- trained/competent discharge crew.

Leading indicators:

- number of times ship is unloaded where the ship-shore checks are not completed correctly;
- number of times when any item is not met by ship calling at a terminal.

2 Ship-to-shore transfer accidental leakage

System outcomes:

- no leaks into water.

Lagging indicators:

- number of times a ship is offloaded where there is a leak to water.

Critical elements of the RCS:

- ship-to-shore checks completed correctly;
- inspection and maintenance of marine arms;
- trained jetty crew;
- coupling done up correctly/manifold bolted up properly;
- start pump slowly;
- walk the lines;
- lines drained down correctly/stripped.

Potential leading indicators:

- number of times the planned inspection and maintenance of marine arms not done to time;
- number of times the ship-to-shore checks not completed correctly, especially;
- new gaskets used;
- lines walked before discharge commences.

3 Bulk tank overfilling

System outcomes:

- not filled above safe operating limits.

Potential lagging Indicators:

- number of times the tank is filled above the safe operating limits.

Critical elements of the RCS:

- ullage control checklist/scheduling system;
- tank gauging and associated equipment working;
- competent people undertaking tasks;
- shift handover control;
- supply handover;
- configuration of valves and associated interlocks;
- inspection and maintenance of tank gauging system;
- inspection and maintenance of line product sensors;
- for pipeline deliveries – cross-check and fax confirmation between central ops and terminal ops OCC monitoring tank level independently.

Potential leading indicators:

- number of times ullage checks not done correctly before product transfer begins;
- number of times inspection and maintenance of tank gauging system not carried to required frequency.

4 Accidental leakage during tanker loading

Outcomes:

- during product transfer no leaks;
- breaking couplings after transfer – not more than 1 litre.

Potential lagging indicators:

- number of times there is a leak of more than 1 litre following product transfer or any leak during the transfer

Critical elements of the RCS:

- reliable equipment – couplings and faucet (hours of use and change-out time);
- operator error – stretch, position of vehicles;
- mistreatment;
- maintenance and inspection of vacuum breaker/faucet/coupler;
- truck maintenance;
- maintenance.

Potential leading indicators:

- % of STOP observations on loading bay operations where drivers are not following procedures;
- % failure of truck API inspections.

5 Tank subsidence

Outcomes:

- tank configuration within relevant API or EEMUA;
- any detectable signs of adverse distortion or movement.

Lagging indicator selected:

- number of tanks where there is adverse distortion or movement.

Critical elements of the RCS:

- inspection and maintenance of tanks;
- appropriate and timely action follow-up;
- independent review of findings.

Leading indicators:

- number of tanks inspected to schedule;
- number of corrective actions completed to time.

6 Leaks from pumps

System outcomes:

- no pump leakage due to seal failure.

Seal failure:

- wear;
- cavitation;
- incorrect installation;
- running dry;
- incorrect material;
- misalignment/vibration.

Potential lagging indicators:

- number of (detectable) leaks from pumps due to seal failure. (Any detectable leak from pump seals, picked up during normal terminal walk-round patrol, to be reported.)

Critical elements of the RCS:

- correct design of seals for the application;
- correct installation of seals;
- vibration monitoring of pumps;
- correct operation of the pumps – running only with adequate supply.

Potential leading indicators:

- number of product pump vibration checks undertaken to schedule;
- number of remedial actions raised following vibration monitoring not completed.

7 Pump/motor overheating

System outcomes:

- no pump/motor overheating

Potential lagging indicators:

- number of times fire loop activated by overheating of pump/motor;
- number of near misses referring to overheating of pump/motor.

Critical elements of the RCS:

- correct design of pump/motor for the application;
- correct installation;
- vibration monitoring of pumps;
- correct operation of the pumps – running only with adequate supply.

Potential leading indicators:

- number of product pump vibration checks undertaken to schedule;
- number of remedial actions raised following vibration monitoring not completed.

8 Corrosion of tanks

System outcomes:

- minimum thickness of tanks (wall/floor) left not exceeded due to corrosion.

Potential lagging indicators:

- number of tanks where the minimum thickness of metal has been reached/exceeded during routine inspection.

Critical elements of the RCS:

- water draw-off;
- effective tank repairs;
- tank inspection as per expected frequency;

- microbial growth management;
- record retention/management;
- coated tanks – damage and necessary repair.

Potential leading indicators:

- number of water draw-offs carried out to schedule;
- number of tanks exceeding the scheduled tank inspection interval.

9 High pressure in terminal pipework during pipeline delivery

System outcomes:

- terminal pipework not exceeding ~5 to ~10 bar during pipeline delivery. (High-pressure alarm on SCADA at 12.5 bar – recorded in computerised event log. Can set analogue alarm/indication on terminal control system.)

Potential lagging indicators:

- number of deliveries where terminal pipework pressure exceeded (5 bar) during pipework deliveries.

Critical elements of the RCS:

- alignment of valves – logic interlock;
- control valves;
- competence of staff;
- maintenance of safety critical instrumentation – surge protection/interlock logic/control valves;
- 'Station Not Ready' interlock.

Potential leading indicators:

- number of job observations undertaken of terminal staff carrying out management of pipeline delivery/terminal distribution activities (tell me/show me) undertaken on time (more frequent for newly recruited staff);
- inspection and maintenance of 'Low MV signal direct' control loop carried out to schedule.

10 Static discharge

System outcomes:

- no static discharges in tanks or road tankers.

Potential lagging indicators:

- number of static discharges – not detectable.

Critical elements of the RCS:

- earth permissive system;
- loading procedures – no splash loading;
- incorrect filters installed;
- incorrect design of equipment – tank nozzles/pipework;
- flowrate too high;
- tank earthing system;
- tank dipping equipment and procedures.

Potential leading indicators:

- number of times inspection of system maintenance overdue/shows failures;
- number of times inspection of tank earthing overdue/shows failures;
- number of times job observations (tell me/show me) on tank dipping are completed on time.

11 Physical damage

System outcomes:

- no material physical damage to equipment.

Potential lagging indicators:

- number of incident reports where physical damage has occurred.

Critical elements of the RCS:

- driver induction and training;
- competence of permanent contractors;
- control of non permanent contractors – induction;
- correct use of work control system;
- protection of 'at risk' equipment;
- traffic control system – layout, speed detection.

Potential leading indicators:

- number of near-miss reports where equipment damage is a potential;
- number of drivers not trained as required;
- number of significant work control system deficiencies found.

Table 5 *Suite of process safety performance indicators*

Challenge to integrity	Lagging indicator	Leading indicator
1 Overpressure ship-to-shore transfer*	Number of times pressure in the line exceeds 10 bar when offloading	Number of times ship is unloaded where the ship–shore checks are not completed correctly. Number of times when any item is not met by ship calling at a terminal.
2 Ship-to-shore transfer accidental leakage*	Number of times a ship is offloaded where there is a leak to water	Number of times the planned inspection and maintenance of marine arms not done to time. Number of times the ship-to-shore checks not completed correctly.
3 Bulk tank overfilling*	Number of times the tank is filled above the safe operating limits	Number of times ullage checks not done correctly before product transfer begins. Number of times inspection and maintenance of tank gauging system not carried to required frequency.
4 Accidental leakage during tanker loading*	Number of times there is a leak of more than 1 litre following product transfer or any leak during the transfer	% of STOP observations on loading bay operations where drivers are not following procedures. % failure of truck API inspections.
5 Tank subsidence	Number of tanks where there is adverse distortion or movement	Number of tanks inspected to schedule. Number of corrective actions completed to time.
6 Leaks from pumps*	Number of (detectable) leaks from pumps due to seal failure	Number of product pump vibration checks undertaken to schedule. Number of remedial actions raised following vibration monitoring not completed.
7 Pump/motor overheating*	Number of times fire loop activated by overheating of pump/motor	Number of product pump vibration checks undertaken to schedule. Number of remedial actions raised following vibration monitoring not completed.
8 Corrosion of tanks*	Number of tanks where min thickness of metal is reached/exceeded at routine inspection	Number of water draw-offs carried out to schedule. Number of tanks exceeding the scheduled tank inspection interval.
9 High pressure in terminal pipework during pipeline delivery	Number of deliveries where terminal pipework pressure exceeded (5 bar) during pipework deliveries	Number of job observations undertaken of terminal staff carrying out management of pipeline delivery/terminal distribution activities (Tell me/Show me) undertaken on time (more frequent for newly recruited staff). Inspection and maintenance of 'Low MV signal direct' control loop carried out to schedule.
10 Static discharge*	Number of static discharges – not detectable	Number of times inspection of system maintenance overdue/shows failures. Number of times job observations (tell me/show me) on tank dipping are completed on time.
11 Physical damage	Number of incident reports referring to physical damage	Number of drivers not trained as required. Number of significant work control system deficiencies found.

** Denotes the challenges to integrity for which process safety KPIs were selected for monitoring.*

Glossary

AIChE	American Institution of Chemical Engineers
ALARP	as low as reasonably practicable
API	American Petroleum Institute
ARAMIS	Accidental Risk Assessment Methodology for Industries
ATG	automatic tank gauging
BS EN	British Standard European Normal
BSTG	Buncefield Standards Task Group
CA	COMAH Competent Authority: EA, SEPA and HSE
CCPS	Centre for Chemical Process Safety of the American Institution of Chemical Engineers (AIChE)
CCTV	closed circuit television
CHIS	(HSE) Chemical Hazard Information Sheet
CIA	Chemical Industries Association
CIRIA	Construction Industry Research and Information Association
CMS	competence management system
COMAH	Control of Major Accident Hazards Regulations (as amended) 1999
CRR	(HSE) Contract Research Report
CSB	(US) Chemical Safety Bureau
DEFRA	Department for Environment, Food and Rural Affairs
DRA	dynamic risk assessment
EA	Environment Agency
EI	Energy Institute
ERPs	emergency response plans
FMEA	failure modes and event analysis
FRSIC	Fire and Rescue Service Incident Commander
HAZID	Hazard Identification
HAZOP	Hazard Operability Study
HFL	highly flammable liquid
HID	(HSE) Hazardous Installations Directorate
HSE	Health and Safety Executive
HSG	Health and Safety Guidance
HSL	Health and Safety Laboratory
HSW Act	Health and Safety at Work etc Act 1974
ICT	Incident Control Team
IE	initiating event
INDG	(HSE) Industry Guidance Note
IP	Institute of Petroleum (now EI Energy Institute)
IPL	independent protection layer
ISGOTT	International Shipping Guide for Oil Tankers and Terminals
ISO	International Standards Organisation
LAFRS	Local Authority Fire and Rescue Service
LAH	level alarm high
LAHH	level alarm high-high
LOPA	layer of protection analysis
LSHH	level switch high-high
MAH	major accident hazard
MAPP	major accident prevention policy
MATTE	major accident to the environment
MIIB	(Buncefield) Major Incident Investigation Board
MIMAH	Methodology for Identification of Major Accident Hazards
OECD	Organisation of Economic Co-operation and Development
OSD	(HSE) Offshore Safety Division
PHA	process hazard analysis

PPE	personal protective equipment
PPG	(EA) Pollution Prevention Guide
PPSLG	Petrochemical Process Standards Leadership Group
PSA	process safety analysis
PSMS	process safety management system
QRA	quantified risk assessment
ROSOV	remotely operated shut-off valve
ROV	remotely operated valve
RTC	risk tolerability criteria
SEPA	Scottish Environment Protection Agency
SGS	Shell Global Solutions
SIL	safety integrity level
SMS	safety management system
SRAG	(HSE) Safety Report Assessment Manual
TSA	Tank Storage Association
UKOPA	United Kingdom Onshore Pipeline Operators' Association
UKPIA	United Kingdom Petroleum Industry Association
VCE	vapour cloud explosion
VOC	volatile organic compound

References

1 *Recommendations on the design and operation of fuel storage sites* Buncefield Major Incident Investigation Board 2007 www.buncefieldinvestigation.gov.uk/reports/index.htm

2 BS EN 61511-1:2004 *Functional safety. Safety instrumented systems for the process industry sector. Framework, definitions, system, hardware and software requirements* British Standards Institution

3 *The Report of the BP US Refineries Independent Safety Review Panel* The Baker Panel Report 2007 www.safetyreviewpanel.com

4 94/63/EC *The control of volatile organic compound (VOC) emissions resulting from the storage of petrol and its distribution from terminals to service stations* European Parliament and Council 1994

5 BS 2654:1989 *Specification for manufacture of vertical steel welded non-refrigerated storage tanks with butt-welded shells for the petroleum industry* British Standards Institution (withdrawn and replaced by BS EN 14015:2004[6] on 2005/02/11)

6 BS EN 14015:2004 *Specification for the design and manufacture of site built, vertical, cylindrical, flat-bottomed, above ground, welded, steel tanks for the storage of liquids at ambient temperature and above* British Standards Institution

7 *Design and construction of large, welded, low-pressure storage tanks* API 620 (Tenth edition) American Petroleum Institute 2002

8 *Welded steel tanks for oil storage* API 650 (Tenth edition) American Petroleum Institute 1998 ISBN 978 9 9908 6550 9

9 *Initial Report: Recommendations requiring immediate attention* Buncefield Standards Task Group 2006 www.hse.gov.uk/comah/buncefield/bstg1.htm

10 *Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice* HSG244 HSE Books 2004 ISBN 978 0 7176 2803 2

11 *International shipping guide for oil tankers and terminals* (ISGOTT) (Fifth edition) International Chamber of Shipping 2006

12 *A guide to the Control of Major Accident Hazards Regulations 1999 (as amended). Guidance on Regulations* L111 HSE Books 2006 ISBN 978 0 7176 6175 6

13 *The Buncefield investigation: Third progress report* Buncefield Major Incident Investigation Board www.buncefieldinvestigation.gov.uk/reports/report3.pdf

14 BS EN ISO 10497:2004 *Testing of valves. Fire type-testing requirements or BS 6755-2:1987 Testing of valves. Specification for fire type-testing requirements* British Standards Institution

15 *Buncefield major incident investigation: Initial Report* Buncefield Major Incident Investigation Board 2006 www.buncefieldinvestigation.gov.uk/reports/initialreport.pdf

16 *Reducing error and influencing behaviour* HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2

17 *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

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

19 *Layer of protection analysis: Simplified process risk assessment* Centre for Chemical Process Safety 2001 ISBN 978 0 8169 0811 0

20 *Revitalising procedures* HSE Human Factors team 2007 www.hse.gov.uk/humanfactors/comah/procinfo.pdf

21 BS 8007:1987 *Code of practice for design of concrete structures for retaining aqueous liquids* British Standards Institution

22 *Construction of bunds for oil storage tanks: Design of containment systems for the prevention of water pollution from industrial accidents* Report 163 Construction Industry Research and Information Association 1997 ISBN 978 0 8601 7468 4 www.ciria.org.uk

23 *Design of containment systems for the prevention of water pollution from industrial accidents* Report 164 Construction Industry Research and Information Association 1997 ISBN 978 0 86017 476 9 www.ciria.org.uk

24 *Concrete bunds for oil storage tanks* CIRIA/Environment Agency 2001 www.environment-agency.gov.uk/commondata/acrobat/concretebunds.pdf

25 BS 476-20:1987 *Fire tests on building materials and structures: Method for the determination of the fire resistance of elements of construction (general principles) British Standards Institution and BS 476-22:1987 Fire tests on building materials and structures Methods for the determination of the fire resistance of non load-bearing elements of construction* British Standards Institution

26 BS 8110-1:1997 *Structural use of concrete. Code of practice for design and construction* British Standards Institution

27 BS 6213:2000 *Selection of construction sealants. Guide* British Standards Institution

28 *Model Code of Safe Practice Part 19: Fire precautions at petroleum refineries and bulk storage installations* IP19 (Second edition) Energy Institute 2007 ISBN 978 0 85293 437 1 www.energyinst.org.uk

29 *Guidance on the interpretation of major accident to the environment for the purposes of the COMAH Regulations 1999* DEFRA 1999 ISBN 0 11 753501 X www.defra.gov.uk

30 *Managing fire water and major spillages* PPG18 Joint publication of the Environment Agency, Scottish Environmental protection Agency and the Environment and Heritage Service for Northern Ireland 2001 www.environment-agency.gov.uk

31 *The Buncefield investigation: Second progress report* Buncefield Major Incident Investigation Board 2006 www.buncefieldinvestigation.gov.uk/reports/report2.pdf

32 *Environmental guidelines for petroleum distribution installations* (Draft6) Energy Institute 2007 www.energyinst.org.uk

33 *Developing and maintaining staff competence* (Second edition) Railway Safety Publication 1 ORR 2007 www.rail-reg.gov.uk

34 *Competence* Human Factors Briefing Note No 2 HSE 2005 www.hse.gov.uk/humanfactors/comah/02competency.pdf

35 *Competence Assurance* Core Topic 1 HSE 2005 www.hse.gov.uk/humanfactors/comah/core1.pdf

36 *Competence assessment for the hazardous industries* RR086 HSE Books 2003 ISBN 978 0 7176 2167 5 www.hse.gov.uk/research/rrhtm/index.htm

37 *Assessing the safety of staffing arrangements for process operations in the chemical and allied industries* CRR348 HSE Books 2001 ISBN 978 0 7176 2044 9 www.hse.gov.uk/research/crr_htm/index.htm

38 *Safe staffing arrangements – User guide for CRR 348/2001 methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated plant and/or equipment* Energy Institute 2004 ISBN 978 0 85293 411 1 www.energyinst.org.uk

39 *Managing shift work: Health and safety guidance* HSG256 HSE Books 2006 ISBN 978 0 7176 6197 8

40 *Managing fatigue risks* Specific Topic 2 HSE 2005 www.hse.gov.uk/humanfactors/comah/specific2.pdf

41 *Successful health and safety management* HSG65 (Second edition) HSE Books 1997 ISBN 978 0 7176 1276 5

42 *Improving alertness through effective fatigue management* Energy Institute 2006 www.energyinst.org.uk

43 *Initial report on the findings of the oil/fuel depot safety alert review* HSE 2006 www.hse.gov.uk/comah/buncefield/review.htm

44 *Organisational change and major accident hazards* Chemical Information Sheet CHIS7 HSE 2003 www.hse.gov.uk/pubns/comahind.htm

45 *Principles for the assessment of a licensee's intelligent customer capability* T/AST/049 HSE 2006 www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast049.pdf

46 *Contractorisation* T/AST/052 HSE 2002 www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/TAST052.pdf

47 *Guidelines for implementing process safety management systems* Center for Chemical Process Safety 1994 ISBN 978 0 8169 0590 4

48 *Guidelines for auditing process safety management systems* Centre for Chemical Process Safety 1993 ISBN 978 0 8169 0556 0

49 *Guidance on safety performance indicators: Guidance for industry, public authorities and communities for developing SPI programmes related to Chemical Accident Prevention, Preparedness and Response* (A Companion to the OECD Guiding Principles) OECD 2003 www2.oecd.org/safetyindicators

50 *Recommendations on the emergency preparedness for, response to and recovery from incidents* Buncefield Major Incident Investigation Board 2007 www.buncefieldinvestigation.gov.uk/reports/index.htm

51 *Pollution Prevention Guidelines* PPG28 Environment Agency www.environment-agency.gov.uk/ppg

52 *Manual on environmental protection* Fire and Rescue Service

53 *Fire precautions at petroleum refineries and bulk storage installations* IP19 March 2007

54 *Refinery explosion and fire: Investigation Report* US Chemical Safety and Hazard Investigation Board March 2007 www.csb.gov/completed_investigations/docs/CSBFinalReportBP.pdf

55 *Safety Culture* Human Factors Briefing Note No 7 HSE 2005 www.hse.gov.uk/humanfactors/comah/07culture.pdf

56 *Leadership for the major hazard industries* Leaflet INDG277(rev1) HSE Books 2004 (single copy free or priced packs of 15 ISBN 978 0 7176 2905 3) www.hse.gov.uk/pubns/indg277.pdf

57 *A review of safety culture and safety climate literature for the development of a safety culture inspection toolkit* RR367 HSE Books 2005 ISBN 978 0 7176 6144 2 www.hse.gov.uk/research/rrhtm/index.htm

58 *Involving employees in health and safety: Forming partnerships in the chemical industry* HSG217 HSE Books 2001 ISBN 978 0 7176 2053 1

59 *Guidelines for risk based process safety* Centre for Chemical Process Safety 2007 ISBN 978 0 4701 6569 0

60 *Process safety management systems* HID Semi Permanent Circular SPC/TECH/OSD/13 HSE 2003 www.hse.gov.uk/foi/internalops/hid/spc/spctosd13.pdf

61 *Accidental risk assessment methodology for industries in the framework of Seveso II Directive* http://mahbsrv3.jrc.it/aramis/home.html

62 *Guidance on 'as low as is reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)* SPC/Permissioning/12 www.hse.gov.uk/comah/circular/perm12.htm

63 *Alarm systems: A guide to design, management and procurement* EEMUA 191 (Second edition) Engineering Equipment and Materials Users' Association 2007 ISBN 0 85931 155 4

64 *Safety report assessment guidance: Technical aspects* HSE www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm#5c9e460

65 Swain A D *Handbook of human reliability analysis with emphasis on nuclear power plant applications* NUREG/CR-1278 1983

Safety report assessment guide: Highly flammable liquids HSE www.hse.gov.uk/comah/sraghfl/index.htm

COMAH safety reports: Technical policy lines to take for predictive assessors. Annex 17 HID Semi Permanent Circular SPC/Permissioning/11 www.hse.gov.uk/foi/internalops/hid/spc/spcperm11.pdf

Environment risk assessment guidance documents

Chemical storage tank systems – Good practice: Guidance on design, manufacture, installation, operation, inspection and maintenance C598 Construction Industry Research and Information Association 2003 ISBN 978 0 86017 598 8 www.ciria.org.uk

Guidelines for environmental risk assessment and management DEFRA www.defra.gov.uk

Guidance for the gasification, liquefaction and refining sector Sector Guidance Note IPPC S1.02 Environment Agency 2005 www.environment-agency.gov.uk

Emissions from storage of bulk or dangerous materials BREF European Integrated Pollution Prevention and Control Bureau Reference 2006 www.eippcb.jrc.es

Guidance document on risk assessment for the water environment at operational fuel storage and dispensing facilities Energy Institute 1999 ISBN 978 0 85293 256 8 www.energyinst.org.uk

Guidelines on the environmental risk assessment for major installations handling hazardous substances Energy Institute 1997 ISBN 978 0 85293 202 5 www.energyinst.org.uk

Guidance on the protection of land under the PPC regime: Application site report and site protection and monitoring programme Technical Guidance Note IPPC H7 Environment Agency 2003 www.environment-agency.gov.uk