

COMAH COMPETENT AUTHORITY

DRAFT STANDARD: Safety Integrity for Overfill Prevention Systems for Bulk Fuel Storage Tanks

Standard

1. Bulk storage tanks containing petrol or other similar substances likely to give rise to a large vapour cloud in the event of an overfill should be fitted with a high integrity, automatic operating overfill prevention system that is physically and electrically separate and independent from the tank gauging system. For the purposes of this policy **high integrity** is taken to mean having a SIL rating of 1 or above as defined in BS EN 61511.
2. The COMAH Competent Authority, CA, in consultation with industry, will develop a programme to ensure improvements to overfill protection systems at relevant fuel storage sites meet this standard. This will be undertaken in accordance with the CA's Policy on Containment of Bulk Hazardous Liquids.

Background

3. The Buncefield incident highlighted the critical importance of effective overfill prevention systems in preventing the creation of a large vapour cloud. Prior to the incident typical overfill protection systems within the fuel storage sector ranged from fully automated systems, independent of the tank gauging system, to simple manual systems.
4. This standard expands upon the requirements for primary containment within the CA policy on Containment of Bulk Hazardous Liquids at COMAH Establishments.

Improvements in the Overfill Protection Systems

5. Following the incident the CA has sought to improve standards of overfill prevention and has worked closely with industry initially via the Buncefield Standards Task Group, BSTG and more lately with its successor the Process Safety Leadership Group, PSLG to identify where such improvements are necessary.
6. The Buncefield Major Incident Investigation Board, MIIIB, Design and Operations report (Annex 2) , recommended that:
 - i. the Competent Authority and operators of Buncefield-type sites should develop and agree a common methodology to determine safety integrity level (SIL) requirements for overfill prevention systems in line with the principles set out in Part 3 of BS EN 61511,
 - ii. operators of Buncefield-type sites should, as a priority, review and amend as necessary their management systems for maintenance of equipment and systems to ensure their continuing integrity in operation, and
 - iii. operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a high integrity, automatic operating overfill prevention system that is

physically and electrically separate and independent from the tank gauging system.

7. To meet recommendation 1 the BSTG Initial Report¹ proposed the use of a Layers of Protection Analysis Study, LOPA, as a suitable common methodology to determine SIL levels for overfill prevention systems. Such assessments had to be completed by June 2007. The BSTG Final Report made recommendations for improvements to management systems for maintenance of equipment and systems.
8. A CA review of a sample of SIL assessments completed since Buncefield revealed some fundamental errors in how independent layers of protection had been calculated and assigned. The CA may therefore question whether the conclusions reached demonstrate that the risks have been reduced to ALARP. A summary of the common failings is given in Annex 1.
9. Dealing with MIIB D&O recommendation 2 the BSTG Final Report² contains initial guidance of management systems maintenance of equipment, proof testing and management of operations. Operators were required to implement any changes to their management arrangements by November 2007.
10. In relation to MIIB Recommendation 3 the CA has concluded that it would be unlikely that a system that failed to meet the principles of BS61511 and which did not meet SIL 1 or above could be considered as 'high integrity'. Additionally, the CA has concluded that to avoid the risk of common cause failure associated with human error it is appropriate that an overfill prevention system should be fully automatic.

Application

11. This standard relating to overfill prevention systems will be implemented in accordance with the CA Containment Policy for Bulk Storage of Bulk Hazardous Liquids at COMAH sites and will apply to substances and storage arrangements meeting the BSTG application criteria or to other substances determined by the PSLG.

Timetable

12. This standard will be applied immediately to new sites or existing sites subject to any significant changes in equipment or operation at existing establishments. Other existing sites will be required to meet this standard based on risk and practicality. The CA will seek to agree a timetable for upgrade with individual site operators using the safety and environmental sensitivity prioritisation criteria already established. Subject to the considerations of practicality set out below the CA expects that work to upgrade all existing establishments to meet this standard should be completed by the end of December 2011.

¹ Buncefield Standards Task Group: Initial report - recommendations requiring immediate action: <http://www.hse.gov.uk/comah/buncefield/bstg1.htm>

² Buncefield Standards Task Group (BSTG) final report: <http://www.hse.gov.uk/comah/buncefield/final.htm>

13. This new standard will not be implemented until completion of a period of consultation with stakeholders. See the workshop proposals set out in paragraph 15 below.

Practicality

14. In some circumstances the fitting of an automatic shutdown system may give rise to other more serious safety risks associated with hydraulic pressure surge. In such cases existing sites will not be required to move to this new standard until suitable practical solutions have been developed. The CA will work with the sector via the PSLG to identify the exact nature of these practical difficulties, the number of sites and tanks so affected and to initiate work to devise practical solutions to these problems. Once appropriate solutions are available to overcome problems associated with pressure surge at existing sites then site operators will be required to implement improvements to meet this standard with three years of that date.

Interim Arrangements

15. For existing sites yet to meet this standard the CA will work with the sector via the PSLG to identify additional measures necessary to ensure the integrity of the overfill protection system. This is likely to entail ongoing assurance that existing overfill prevention systems are operated and maintained in accordance with the conclusions of the operator's agreed risk assessments conducted as part of the BSTG Final Report. The CA will implement a programme of ongoing verification visits to ensure that such measures are implemented and maintained.

Next Stages

16. The CA will hold a workshop with the sector to:

- share the findings of the LOPA SIL assessments so far reviewed either by HSL or by C&I inspectors,
- discuss the implementation of the decision to seek SIL 1 or, where appropriate, SIL2,
- to initiate work to;
 - resolve the practical solutions to hydraulic pressure surge; delineate the extent of this issue;
 - determine any additional measures to be adopted at sites yet to meet this standard, and
 - determine whether further guidance is required on the application of BS61511 to bulk tank storage installations.

Annex 1: Summary of Common Failings in LOPA Assessments for Bulk Tank Overfilling Prevention Systems

1. HSE and HSL have reviewed a number of LOPA studies relating to overfill prevention systems prepared in accordance with the BSTG Final Report. A number of errors and problems have been identified:

- Human error probability too optimistic,
- Independence of human operators (Double counting of benefit from human tasks),
- Risk factors due to the number of tanks on any particular site,
- Little available data on Automatic tank gauging (ATG) errors and failures,
- Incorrect logic used to combine various factors,
- Incorrect handling of number of filling operations,
- Difficulty in analysing time at risk i.e..filling duration,
- Uncertainty of ignition probability,
- Uncertainty of probability of fatal injury,
- Uncertainty of occupancy probability,
- Uncertainty of probability of human detection of overfill,
- Unjustified valve reliability,
- Data not justified by site experience,
- No consideration of common cause failures of equipment,
- Inappropriate risk targets,
- All hazard risk targets applied to single events,
- Incorrect handling of risk targets eg sharing between tanks,
- Difficulty in estimating probability of vapour cloud explosion, and
- Difficulty in establishing and verifying all initiating events (causes).

Annex 2: MIIB Recommendations³ on the Systematic assessment of safety integrity level requirements

1. The Competent Authority and operators of Buncefield-type sites should develop and agree a common methodology to determine safety integrity level (SIL)⁴ requirements for overfill prevention systems in line with the principles set out in Part 3 of BS EN 61511.

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

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

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

3. Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a high integrity, automatic operating overfill prevention system⁵ (or a number of such systems, as appropriate) that is physically and electrically separate and independent from the tank gauging system.

³ Recommendations on the design and operation of fuel storage sites, 29 March 2007:
<http://www.buncefieldinvestigation.gov.uk/reports/recommendations.pdf>

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

⁵ The factors that determine the type of independent automatic system required will include the effects on the upstream system, for example if filling from a refinery process, a ship or a railway vessel. For all systems the outcome required is the same, ie automatically stopping supply to the dangerously full tank by means that are fully independent of the tank gauging system.