CHEMICAL ENGINEERING TRANSACTIONS
VOL. 26, 2012
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Valerio Cozzani, Eddy De Rademaeker

ISBN 978-88-95608-17-4; **ISSN** 1974-9791
DOI: 10.3303/CET1226073

Safety and Environmental Standards for Fuel Storage Sites: how to enhance the Safety Integrity of an Overfill Protection System for Flammable Fuel Storage Tanks

Pasquale Fanelli

Invensys Systems Italia S.p.A., Sesto San Giovanni (MI), Italy
pasquale.fanelli@invensys.com

Recent accidents with a catastrophic impact on Safety and Environment in the Oil & Gas (O&G) and Oil Refining industries has prompted the Regulators and the Process industry to move an important step forward to ensure to the Communities and the industry stakeholders that the risk of these accidents will be as lowest as reasonably practicable. As model for the approach between Regulators, Industry and Trade Unions in UK after the Buncefield accident the Process Safety Leadership Group (PSLG) issued in 2009 the "Safety and environmental standards for fuel storage sites" Final Report. The PSLG Final Report followed the pathway of Buncefield Standards Task Group (BSTG) by providing safety recommendations focused on improving safety in the design and operation of fuel storage sites. The PSLG Final Report safety recommendations are suitable to turn the safety investment into effective incident prevention. In this paper the PSLG Final Report safety recommendations related to the functional safety issues (reference is made to PSLG Final Report Part 1 "Systematic assessment of safety integrity level requirements" with specific reference to Appendix 2 and Part 2 "Protecting against loss of primary containment using high integrity systems"with specific reference to Appendix 4) are examined in detail aimed to conceive a safety instrumented system to enhance the Safety and Environment protection in fuel storage sites in full compliance both with the PSLG and International Standard IEC 61511 (2003) requirements. The overfill protection system for flammable fuel storage tanks of bulk hazardous liquids such as specifically gasoline and other materials such as naphtha, reformate, light crude oil, others likely to form a large vapour cloud, is examined in detail with a specific focus on safety integrity level assessment by LOPA (layers of protection analysis) method in compliance with the PSLG Final Report guidelines and IEC 61511 (2003) requirements.

1. Buncefield Accident Outline

On Sunday 11 Dec. 2005 at 6.01 am a catastrophic accident occurred at Hertfordshire Oil Storage Terminal site, generally known as the Buncefield Oil Terminal, located in the north of London.
The Terminal owned by TOTAL (60 %) and TEXACO (40 %) was operated by Hertfordshire Oil Storage Ltd. (HOSL) a Total-Chevron joint venture. The Buncefield Oil Terminal, the fifth oil depot in UK, had hazardous planning permit to store 194,000 t of HC fuels, such as gasoline, aviation fuel and diesel. Part of Buncefield Oil Terminal area was occupied mostly for aviation fuel by British Pipeline Agency (BPA), a joint venture of BP and SHELL. The accident was caused by a loss of containment of around 300 t of gasoline during a gasoline tank refilling via pipeline. The Tank 912 (cap. 6,000 m^3) at the HOSL part of the Buncefield oil storage depot was under filling with gasoline imported through the

Please cite this article as: Fanelli P., 2012, Safety and environmental standards for fuel storage sites: how to enhance the safety integrity of an overfill protection system for flammable fuel storage tanks, Chemical Engineering Transactions, 26, 435-440
DOI: 10.3303/CET1226073

FinaLine pipeline from the Lindsey Oil Refinery. The filling operation started at 6.50 pm on Saturday 10 Dec. 2005 (11 hours, 11 minutes before the accident). During the early morning of 11 Dec. 2005 the weather in the terminal area was calm, cold (-1 °C) and humid. The Tank 912 was fitted with an automatic tank gauging system (ATG) which measured the rising level of fuel and displayed this on a screen in the control room. At 03.05 am (2 h, 56 min before the accident) on December Sunday 11 the ATG stopped registering the rising level of fuel in the tank although the tank continued to fill. Consequently the ATG system (tank level operator monitoring and tank high level alarm derived from the same level transmitter signal) did not work being the stuck-on tank level reading below both tank maximum operating level and tank high level alarm. Calculations carried out by the investigating authorities showed that at around 05.20 am (41 min before the accident) on December Sunday 11, the Tank 912 would have been completely full and starting to overflow. The filling of Tank 912 continued at a rate of around 550 m^3/h. Due to the practice of working on alarms the control room supervisor was not alerted to the fact that the tank was at risk of overfilling. The level of gasoline in the tank continued to rise unchecked. Eventually large quantities of gasoline (estimated 300 t) overflowed from the top of the tank through the tank vents to atmosphere conceived to avoid cone roof tank pressurization during floating deck rise (gasoline tank loading) and tank vacuum during floating deck descent (gasoline tank unloading). The Tank 912 overfilling caused a free liquid (gasoline) cascade from tank top deflector plate and from tank side wind girder. The free liquid cascade of flammable material was followed by a massive vaporization. According to the calculations (refer to PSLG Final Report Appendix 1) the gasoline vaporized from the free liquid cascade exceeded 14 % by w. of the air-gasoline vapor mixture (within the gasoline explosive limits) generated by cascade air entrainment. For an estimated gasoline overfilling time of 41 minutes from Tank 912 the overall gasoline vapor entrained according to calculation was around 25 t leading to a catastrophic vapor cloud explosion. The vapor cloud was noticed outside the facility a short time before the explosion and the site personnel promptly alerted. The fire alarm button was pressed at 06.01 am, which sounded the alarm and started the firewater pump. An explosion occurred almost immediately after, probably ignited by a spark caused by the firewater pump starting. The first explosion measured 2.4 on the Richter Scale, other minor explosions followed and the resulting fire lasted five days. The Buncefield accident caused material damages up to 1.6 billion USD. A trial at St Alban's Crown Court concluded in July 2010 with five companies being found guilty (TOTAL, HOSL, BPA, Motherwell Control Systems, TAV Engineering Ltd.), and ordered to pay a total of 15 million USD in fines. Tank 912 was fitted with a new independent safety high high level switch on 1 July 2004. This had been designed, manufactured and sub-supplied by TAV Engineering Ltd to Motherwell Control Systems Ltd., which supplied and installed the high high level switch on Tank 912 and was in charge of maintaining the ATG system.

2. Buncefield Accident Root Causes

According to COMAH Report (2011) “Why it did happen?” the main identified root causes are reported hereinafter:

1) Failure of the ATG system was the immediate cause of the incident.
2) Because those who installed and operated the high high level switch did not fully understand the way it worked, or the crucial role played by a padlock, the high high level switch on Tank 912 was left effectively inoperable after the proof test.
3) The site operator did not exercise sufficient oversight of the ordering, installation and testing procedure. While the switch was periodically tested, none of the staff at the HOSL site was aware of the need for the padlock to be replaced so that the test lever was held in the correct position.
4) There was only one visual display screen for the data provided by the ATG system on a number of tanks which meant that the status of only one tank could be fully viewed at a time.
5) On the tank screen mimic a red ‘stop’ emergency shutdown button was showed. It was meant to close all tank side valves. Unbeknown to a number of the supervisors this was not working and had never been fitted into the system.
6) The ATG system hadn’t the ability to be set to alarm in the event of inconsistencies between tank level measurements and filling data, which would have provided a way of alerting control room staff to an ‘unexpected’ static reading.

7) The lack of information undermined the ability of supervisors to plan and control the management of fuel.
8) The lack of a maintenance regime (tank level transmitter had stuck 14 times between 31 August 2005 and the accident date).
9) The absence of a fault logging process (or a process safety performance indicators system).
10) Last, but first for importance, the practice of working on alarms.

The COMAH Report (2011) "Buncefield: Why did it happen?" in its Conclusions stated the following:
“The types of managerial failings revealed during the Buncefield investigation were often found at other major incidents. The report on the gas explosion at Longford, Australia in 1998 identified factors associated with the incident which were also present at Buncefield.
For example:
- poor communications at shift handover;
- lack of engineering expertise on site; and
- failure to implement management of change processes.”

3. "Safety & Environmental Standards for Fuel Storage Sites” PSLG Final Report

The Buncefield Standards Task Group (BSTG) was set up in 2006 in UK to turn the lesson learnt from Buncefield accident into an effective and practical guidance to the Industry. The Process Safety Leadership Group (PSLG) was set up in 2007 to conceive an effective framework between industry, trade unions and COMAH (Control of Major Accident Hazards) (2011) Competent Authority (C.A.), comprising HSE, EA, SEPA (UK HSE, 2009) whose role is to oversee and coordinate the regulation of major hazards in the UK and ensure that the COMAH regime operates effectively. The PSLG issued in 2009 the “Safety and Environmental Standards for Fuel Storage Sites” Final Report with the main purpose to specify the minimum standards of control which should be in place at all establishments storing large volumes of fuels, primarily referred to gasoline, but it can be extended to any HC flammable material capable of giving rise to a large flammable vapor cloud in the event of a loss of primary containment such as tanks, pipes and vessels that normally hold liquids, and the devices fitted to them to allow them to be safely operated. An initial review of commonly stored liquids using the methodology indicates that the following substances have the potential to give rise to a large vapor cloud in the event of a tank overfill:

- crude oil (RVP ≥ 0.17 bar abs.)
- raw gasoline
- reformate (light)
- iso pentane
- naphtha
- natural gas liquids (condensates)
- methyl tert-butyl ether (MTBE)
- acetone
- methyl ethyl ketone (MEK)
- SBP2 solvents
- benzene
- toluene.

Substances not considered likely to form a large vapor cloud in case of storage tank overfill according to PSLG Report, are:
- crude oil (RVP < 0.17 bar abs.)
- diesel
- kerosene
- reformate (heavy)
- ethanol
- methanol
- SBP3 solvents.

The “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report provides guidance on good practices in relation to secondary containment such as enclosed areas around storage vessels (often called bunds) created usually by concrete or earth walls. The purpose of secondary containment is to hold any escaping liquids and any water or chemicals used in fire-fighting. The PSLG Final Report provides guidance on good practices in relation to tertiary containment such as the site surface and associated drainage, boundary walls, roads, containment curbs and any features

such as road humps that can provide some retention of liquids. Proper design of drainage systems will limit loss of product out of the site and prevent lost product permeating into the ground with the potential risk that it can migrate to groundwater, or contaminate surface waters and land. The “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report provides also guidance relevant to consider the appropriate hazard identification and risk assessment technique. The guidance provided by the “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report is not an authoritative interpretation of the law, but by following this guidance it can be proved that enough was done to comply with the law. Other alternative measures to the “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report may be used to comply with the law.

4. Systematic assessment of SIL requirements

The “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report is structured in six parts:
Part 1: Systematic assessment of safety integrity level (SIL) requirements
Part 2: Protecting against loss of primary containment using high integrity systems
Part 3: Engineering against escalation of loss of primary containment
Part 4: Engineering against loss of secondary and tertiary containment
Part 5: Operating with high reliability organizations
Part 6: Delivering high performance through culture and leadership.
Aimed to reach the compliance to International Standard IEC 61511 (2003) of a safety instrumented system allocated to protect against overfilling a Fuel Storage specific reference is made to PSLG Final Report Part 1, Part 2 and relevant Appendixes 2 and 4. Reference is made also to PSLG Final Report Part 5 and relevant Appendix 5 to enhance management of operations and human factor in consistency with IEC 61511 (2003) related requirements. The overall systems for tank filling control should be of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow. High integrity systems are instrumented systems designed, implemented and maintained so that they have a high predefined probability of carrying out their intended function within a predefined time. Safety instrumented systems (SIS), having safety integrity levels (SIL) in the range SIL 1 up to SIL 4, fully compliant with the International Standard IEC 61511 (2003) "Functional Safety: Safety Instrumented Systems for the Process Industry Sector” can be regarded as high integrity systems. The systems for tank filling control owned by an organization holding a legal duty (the Owner) should meet the latest international standards such as IEC 61511 (2003) for Safety Instrumented Systems for the Process Industry Sector. Before protective systems are designed, implemented and installed the appropriate level of integrity that such systems are expected to achieve should be determined. With specific reference to safety instrumented systems (SIS), the safety integrity is defined as the average probability of a safety instrumented system (SIS) to satisfactorily perform the required safety instrumented functions (SIF) under all the stated conditions within a stated period of time. Safety integrity comprises hardware safety integrity and systematic safety integrity. For each Risk Assessment and SIL Determination Study, the Owner should be able to justify each claim, and data used in the risk assessment, and ensure that appropriate management systems and procedures are implemented to support those claims. For Major Accident Hazard (MAH) sites this will form part of the demonstration required within the Safety Report to be released to competent Authorities. Extreme care should be taken to claim high integrity of protection systems, particularly in relation to common mode failures of the allocated protection layers and any factor dramatically affecting the effectiveness of human interventions.
According to IEC 61511 (2003), clause 9:
- the safety function, a function to be implemented by an SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event, shall be allocated as protection layer;
- in case of allocation of one or more safety instrumented functions (SIFs) for each SIF the associated safety integrity level (SIL) shall be assessed.

The overfill protection system for flammable storage tanks as a safety instrumented function including sensors (e.g. level transmitters), logic solver (e.g. safety PLC TMR), final elements (e.g. flammable

feed shutoff valves) sub-systems, should be SIL assessed in conformity with IEC 61511 (2003) requirements.
According to the “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report for SIF SIL Assessment the LOPA (layers of protection analysis) method can be adopted being a suitable methodology to determine the target SIL of the safety instrumented functions.
The LOPA method is widely described in the IEC 61511 (2003) Part 3. High level alarms (independent from tank level monitoring used in tank loading/unloading operations) can be allocated as protection layers and implemented on BPCS (Basic Process Control System). In this case the maximum Risk Reduction Factor (RRF) that can be associated to the independent alarm is equal to 10. Shutoff of loading feed to flammable storage tank to prevent an overfill of flammable material should depend not only upon control and protective systems at upstream site, but also on ultimate control and protective system at receiving site.

LOPA worked example for flammable storage tanks
The risk reduction target stated in this LOPA worked example (Table 1) is based on the Company’s risk reduction acceptability for catastrophic events consistently with applicable legislation and industrial risk reduction compensation policy of insurance companies.

Table 1. LOPA worked example data

Unwanted Event Target Frequency (for multiple fatalities), occ./y	**≤ $1.0 \cdot 10^{-06}$**
Initiating Event Frequency, occ./y	
- level indicator open loop failure or malfunction (LI-1), occ./y	$1.0 \cdot 10^{-01}$
Protection Layers PFDavg. (probability of failure on demand average)	
- H level alarm (LAH-2)	$1.0 \cdot 10^{-01}$
- HH level trip (LAHH-3) with an assigned Safety Integrity Level SIL 2	$1.0 \cdot 10^{-02}$
- secondary containment Oil in Water detector (F&G System)	$1.0 \cdot 10^{-01}$
Conditional Modifiers (CM)	
- CM1 (probability of ignition of a large flammable cloud)	$1.0 \cdot 10^{-01}$
Unwanted Event Mitigated Frequency, occ./y	**$1.0 \cdot 10^{-06}$**

The result is acceptable since the Unwanted Event Mitigated Frequency is consistent with the Unwanted Event Target Frequency. The above worked example clearly shows that the risk associated to the potentially catastrophic consequences of a flammable storage tank overfilling can be reduced at least by three orders of magnitude if compared to a tank protected such as it was the tank 912 at Buncefield. Thanks to "Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report this huge safety gap can be eventually filled by taking also into consideration the impact on the overall risk associated to the large number of tanks in the same flammable storage facility.

5. Overfill protection systems for flammable storage tanks

The overfill protection system for flammable storage tanks should fully comply with IEC 61511 (2003) requirements relevant to SIS lifecycle, including Process Hazard & Risk Analysis, Safety functions Allocation, SIF SIL Assignment, Safety Requirements Specification (SRS), SIS design, engineering, integration, verification, validation (FAT), commissioning and startup, SAT, functional testing & FSA, operation, maintenance and proof testing, management of change (MOC), configuration management, periodic inspection and audit. A functional safety management system (FSM) in compliance with the International Standard IEC 61511 (2003) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector” should be set up, implemented and maintained throughout the SIS lifecycle up to decommissioning. The flammable storage tank normal fill level, H alarm level and HH level trip/alarm level should be set in compliance tank capacities and operating levels (designated according to the guidance) not to routinely operate on alarms. Flammable storage 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. Last, but first for importance, the human error likelihood for tank overfilling scenario should be minimized by implementing:

- automatic calculation of spare/available tank capacity;
- automatic verification of tank feed valves line-up;
- permissive logic of feed valves opening;
- discrepancy test of tank level transmitters analog input signals;
- identification on video-graphics of fuel feed route and receiving tank;
- monitoring of tank level increase in the correct fuel tank during filling;
- monitoring of tank level signal stuck-on state during filling;
- automatic shutoff of fuel feed at the end of tank filling (by BPCS);
- operating procedures for H level alarm and HH level trip/alarm.

6. Safety Performance Indicators

System Safety Outcome

■ tank filling not exceeding the max. operating limit

Critical Elements of Risk Control System

■ tank head-space control scheduling/checklist system;
■ cross-check and confirmation in writing b/n central & terminal operations
■ configuration of valves and associated interlocks;
■ competent people undertaking tasks;
■ shift handover control;
■ supply handover;
■ tank gauging and associated equipment working as per requirements;
■ inspection and maintenance of tank gauging system;
■ inspection and maintenance of line product sensors and valves;
■ inspection and maintenance of prevention & protection systems

Leading Indicators

■ nos. of times the tank head-space control scheduling/checklist is not done correctly before transfer;
■ nos. of times the inspection & maintenance of tank gauging system is not done correctly and in time;
■ shift handover control

Lagging Indicators

■ nos. of times the tank max. op. limit is passed against the nos. of product transfer operations

7. Conclusions

Regulator, Industry and Trade Unions worked together to improve by the guidance of “Safety and Environmental Standards for Fuel Storage Sites” PSLG Final Report the capability to safely operate a bulk storage of very hazardous materials such as the flammable fuels. The application of the PSLG Final Report guidelines for the overfill protection system of flammable storage tanks can reduce significantly the risk associated to loss of containment of flammable materials following a tank overflow. The compliance with the International Standard IEC 61511 (2003) of the fuel tank overfill protection system as per PSLG Final Report requirements will make throughout the Oil Terminal life-time these protective systems trustable to maintain the safe state within the Owner’s tolerable risk targets for Safety, Environment and Material Damages.

References

UK HSE, 2009, Safety and Environmental standards for fuel storage sites - Process Safety Leadership Group Final Report, HSE UK ISBN 978 0 7176 6386 6

COMAH, 2011, Buncefield: why did it happen? The underlying causes of the explosion and fire at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005, HSE UK

IEC 61511, 2003, "Functional Safety: Safety Instrumented Systems for the Process Industry", IEC CH