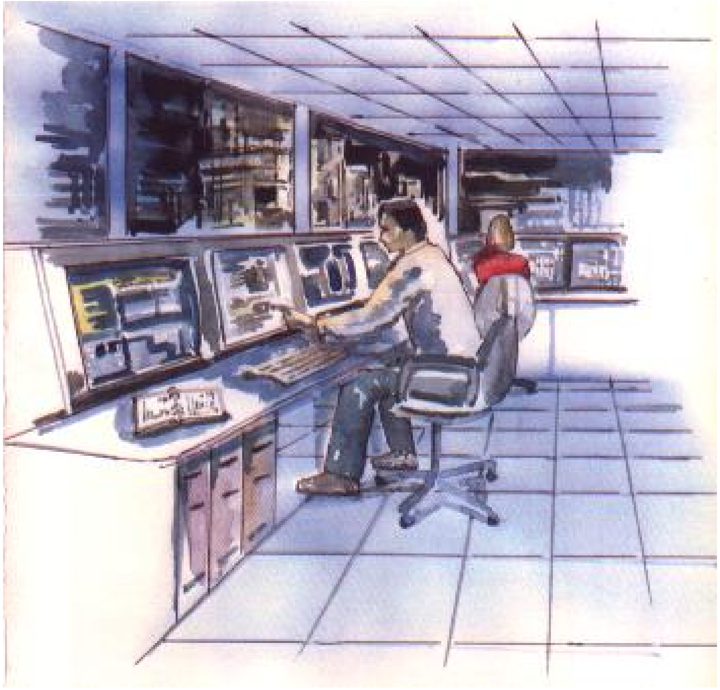
4-sight Consulting

IEC 61511 / 61508 Case study



Contents

1 SUMMARY

The scope of this case study is the overfill prevention and protection of the 12 gasoline (petrol and diesel), kerosene, aviation fuel (Jet A1), derv and gas oil storage tanks at an imaginary Oil Terminal. This includes the tank level instrumentation, information display systems, alarms and high level trip system and the operation of these systems. This case study covers the risk assessment (using Layer Of Protection Analysis (LOPA) and an Event Tree) of the existing overfill prevention and protection, the SIL requirements and the SIL achieved for the high level trip.

CONCLUSIONS

The results show that the Potential Loss of Life (PLL) attributable to a tank overfill accident at the terminal is 4.6E-06 per year. This is below the target PLL of 1E-05 per year for the overfill hazard. The major contribution to the safety risk is the vapour cloud explosion (VCE) event and a suitable high level trip protects against this event. The consequences of this event are assumed to be comparable to those predicted for the Buncefield HOSL accident and will therefore have a high severity as a large number of fatalities are assumed to occur. The contribution to the safety risk from the catastrophic tank collapse following a bund fire is significantly less.

In assessing the above risk an assumed probability of failure on demand (PFD) for a SIL 1 system of 0.03 has been used. The work then done to evaluate the overfill protection system demonstrated a PFD of 0.011 and that the existing system comfortably meets SIL 1 performance requirements. A further revision of the risk analysis using this lower PFD would therefore give lower values of Potential Loss of Life (PLL) than outlined above although this has not been carried out and the results reflect some conservatism.

The published Buncefield Fire Report (Reference 17) from the Major Incident Investigation Board (MIIB) has listed a comprehensive set of recommendations relating to the Design and Operation of Fuel Storage Sites. Recommendation No. 1 ‘Systematic assessment of safety level requirements’ has been addressed by the analysis in this case study.

Numerous recommendations have been made that cover the prevention of loss from primary containment, prevention of escalation, preventing loss from secondary and tertiary containment and organisational issues. Annex 3 and 4 to the MIIB report state present arguments relating to upgrades to component and systems and the use of independent and automatic storage tank overflow protection.

2 INTRODUCTION

This case study assesses the System Integrity of the over-fill protection for the 12 storage tanks at an imaginary oil storage terminal. IEC 61511 [Ref. 3] has been used to provide a method for establishing the required Safety Integrity Level (SIL).

IEC 61511 [Ref. 3] has also been used to provide a method for establishing the achieved Safety Integrity Level (SIL) by examining the design and installation of monitoring, control and protection systems installed to prevent tank overfill.

3 SCOPE OF THE STUDY

The scope of the study is the overfill prevention and protection of the storage tanks. This includes the tank level instrumentation, information display systems, alarms and high level trip system and the operation of these systems. This case study covers the risk assessment of the existing overfill prevention and protection, the SIL requirements and the SIL achieved for the high level trip.

The maintenance of the systems is not covered in this case study.

4 METHOD USED FOR THE STUDY

The method used is in accordance with approach to risk assessment required by the HSE in Ref. 5 (see Appendix 3 – HSE requirements for risk assessment). A semi-quantitative technique, LOPA [Ref. 10], is used to assess the risk of overfill. An event tree is used to analyse the various consequences that might arise following an overfill event including the Potential Loss of Life (PLL) from fire or explosion.

The study assumes a target for PLL of 1E-5 per year for the overfill hazard in order to calculate the required SIL for the trip system to prevent overfill.

5 OPERATION OF THE TERMINAL

The oil terminal for fuel distribution is fed with gasoline (petrol and diesel), kerosene, aviation fuel (Jet A1), derv and gas oil. The fuels are transferred into road-tankers for road distribution to their own customers. Terminal staff are responsible for checking the quality of the fuel in each delivery, for opening up the delivery route to the correct storage tank and for ensuring there is sufficient ullage to accept the delivery.

Transfer between storage tanks is rare and thus was also not included in the LOPA as it does not contribute significantly to the risk of overfill.

It is important to ensure the receiving tanks have sufficient ullage and delivery is into the correct storage tanks (single tank working) in a safe and controlled manner. The risk of deliveries arriving in the wrong order is small but this is recognised as a possible cause of an overfill or a crossover. All imports are also monitored on level displays during delivery to ensure the correct tank is receiving the correct product.

If it is identified that there is insufficient ullage for a particular delivery advice is sought from the terminal manager and the relevant contact within the supply department.

6 DESCRIPTION OF OVERFILL PREVENTION AND PROTECTION

6.1 TANK LEVEL MEASUREMENT AND DISPLAY

Levels of all the gasoline (petrol and diesel), kerosene, and aviation fuel (Jet A1), derv and gas oil tanks can be displayed on the level displays screen. During delivery the relevant tank level is displayed on the level displays screen.

6.2 HIGH LEVEL ALARMS

There are tank High Level Alarms included in the level displays software. These are tested weekly to ensure that the alarms are functioning correctly. In the event of a test failure the problem is investigated and acted upon immediately and also reported to terminal management.

6.3 HIGH LEVEL TRIP

There are independent level measurements on each that are connected to the high level trip logic that is completely separate from the level displays. The tank side valves (electrically powered double acting valves) for isolating flow fitted to all tanks are activated by the high level trip logic.

6.4 OVERFLOW DETECTION SYSTEMS

There are currently no facilities on site for detection of released vapour or liquid prior to ignition. In the tank areas manual detection of releases is based on routine patrols. Fire detection is currently not provided in the tank areas.

6.5 FIRE WATER PUMPS, MAINS AND STORAGE TANK

Two diesel driven fire water (FW) pumps are installed in the fire pump house. For the storage area each tank sprinkler supply for vessel cooling is isolated from the FW main by a single valve located on the outside of the tank farm bund wall. These valves can be remotely operated for the tanks.

7 HAZARDS FROM TANK OVERFLOW

The hazards considered are mainly those associated with petrol and are taken from the COMAH report, from the HSE investigation [Ref. 1] following the Buncefield fire 11th December 2005 and from specific consequence modelling.

7.1 POOL FIRES

One consequence resulting from a release of petrol from the tank to the bund is a pool fire with possible escalation. The event tree Figure 15-1 - Event tree following tank overfill has identified a number of outcomes associated with bund fires.

7.1.1 Overtopped Bund Fire

The most severe fire event is that represented by codes 0070 and 0100 and described as ‘Overtopped Bund Fire’. The accident sequence modelled in the event tree is that an overfill event occurs at one of the petrol tanks and this leads to a full bund that is ignited. Without control or tank protection it is possible that the other tanks in the bund will fail in time and collapse. The possibility therefore exists for a bund overtop where a surge of fuel and firewater mixture spills into the adjacent bunds to the east or offsite to the north and west. The postulated worst case could be several thousand tonnes although the frequency of this would be extremely low.

The timescale in which a pool fire develops and then the time for failure of the tanks within the bund should mean that personnel both on-site and of-site have reasonable time to reach a safe distance. For the purposes of assigning the severity for this scenario it is not assumed to involve high numbers of fatalities. It is assumed that 1 or 2 persons from the emergency services could become fatalities if a surge event occurs.

7.1.2 Bunded Pool Fires

Where no catastrophic tank failure occurs, any pool fire from overfilling is assumed to be contained within the bund. The event tree Figure 15-1 - Event tree following tank overfill models the events which are not extinguished early as outcome codes 0080 and 0110. The heat flux hazard ranges for these events are taken from the COMAH report [Ref. 12] as follows in Table 1.

Table 1 - Pool Fire Thermal Radiation.

Hazard Description	Distance to Thermal Radiation (m) from pool centre			
	16kW/m^2	**10kW/m^2**	**8kW/m^2**	**6.3kW/m^2**
80m diameter pool fire – Petrol	83	105	113	120

The predicted hazard ranges show that the heat flux for a bunded pool fire could reach the occupied buildings on site and properties outside the terminal. However due to the time for the event to develop and that available for escape it is assumed that this event is unlikely to result in fatalities.

7.2 VAPOUR CLOUD EXPLOSION (VCE)

The COMAH report has identified VCE events from internal tank explosions as representative scenarios. The event tree within this case study Figure 15-1 - Event tree following tank overfill has concentrated on events associated with the overfilling protection systems and the worst case outcome identified is an explosion event of the magnitude of the Buncefield (HOSL) explosion.

The assumption in this analysis is that the over fill event would lead to a drifting cloud, based on a worst case composition i.e. high C3/ C4 (LPG) content for 'winter blend' and stable F2 conditions. A cloud of significant size could be generated and drift off site. Assuming that ignition occurs and an explosion of comparable magnitude to the HOSL event occurs then for the purposes of this analysis it is estimated that an overpressure contour of 200mbar occurs at 200m from the cloud centre.

There will be an occupancy effect that reduces the likely event frequency when most persons are at risk but it is certainly foreseeable that a few hundred people could be within this 200m contour. The possibility therefore exists that multiple offsite fatalities could occur and for the purposes of this analysis it is assumed that the number of fatalities is about 50 people.

On the event tree Figure 15-1 - Event tree following tank overfill the outcome described, is given code 0090 ‘Severe VCE (HOSL)’.

8 HAZARD IMPACT ANALYSIS - FREQUENCY AND SEVERITY

The event tree for the tank overfill (see 14 Appendix 1 - LOP) illustrates the key elements in the possible consequences of an overfill. The description of the scenarios in section 8 (above) provides the event severity in terms of equivalent fatalities. The results for the safety risk analysis are presented in terms of probability of lives lost (PLL) per year and shown in Table 2. Figure 14-1 - LOPA leading to tank overfill shows the frequency for all tanks, but only overfill of the petrol tanks could result in Severe VCE (HOSL) events thus the analysis assumes that only half the tank overfill events apply to petrol tanks.

Table 2 - Safety Risk Analysis Results

Hazard Description	**Safety Risk Parameters**			
	Event Tree Code	**Event Frequency (/yr)**	**Event Severity (Fatalities)**	**PLL (/yr)***
Severe VCE (HOSL)	0090	1.33E-07	50	3.33E-06
Overtopped Bund Fire	0070, 0100	2.60E-06	1	1.30E-06
Bunded Pool Fire	0080, 0110	3.89E-06	0.01 (est)	1.95E-08
Total Safety PLL (/yr) for Tank Overfilling Accident				**4.6E-06 / yr**

9 ASSESSMENT OF SIL ACHIEVED BY HIGH-HIGH LEVEL TRIPS

9.1 INTRODUCTION TO ASSESSMENT OF ACHIEVED SIL

The assessment below relates specifically to the operation of the high-high level trip, as initiated by high level switches located one each of the main product storage tanks.

The Emergency Shut Down (ESD) can also be initiated by:

- operation of local ESD pushbuttons (manual operation)
- operation of Terminal ESD pushbuttons (manual operation)
- operation of Terminal Fire Alarm System (manual & automatic initiation)
- operation of tank side actuators (unauthorised close initiates a Terminal ESD)

The independent high level trip system is designed to operate ‘above’ the site tank gauging system. The primary function of this trip system is to initiate an ESD and stop transfer of product to the storage tanks. Inter-tank transfers are very rare and thus delivery is the only significant source of product that could cause a high level in these tanks.

In addition, as a back-up, operation of any tank high level switch is activates the appropriate tank side valve closure. Communication with tank side valve is via a control loop with valves that are power open and power close.)

9.2 IEC 61511 REQUIREMENTS FOR SIF

Table 3 - IEC 61511 Requirements for SIF

#	Requirement	Comment / cross reference
1	a description of the safety function	Shut-off flow into tanks
2	identify and take account of common cause failures	See Section 10.1
3	a definition of the safe state of the process	Pumps shut-down and relevant tank entry valve closed
4	a definition of individually safe process states which, when occurring concurrently, create a separate hazard	None identified
5	assumed sources of demand and demand rate	See Section 14
6	proof-test intervals	See Section 10.3
7	response time	See Section 10.4
8	SIL and demand or continuous mode	SIL 1 & Demand mode
9	process measurements and trip points (settings)	See Section 10.5
10	process output actions	Shut down pumps and close tank entry valve
11	relationship between measurements and their trip points, including any required permissives	See Sections 10.5 & 10.6
12	manual shutdown	See Section 10.6
13	energize or de-energize to trip	See Section 10.1
14	resetting after a shutdown	See Section 10.6
15	allowable spurious trip rate	Not assessed in this case study
16	failure modes and desired response	See Section 10.7
17	start-up and re-start procedure	See Section 10.6
18	all interfaces with other systems	See Section 10.2.5
19	a description of modes of operation of plant	See Section 10.8
20	application software safety	Not applicable
21	overrides/inhibits/bypasses	See Section10.6
22	action on fault detection	See Section 10.7
23	mean time to repair	See Section 10.7
24	dangerous combinations of output states that need to be avoided	None identified
25	environmental conditions likely to be encountered	See Section 10.9
26	normal and abnormal modes of operation of plant	See Section 10.8
27	function necessary to survive a major accident event (escalation)	See Section 10.8.5

10 ASSESSMENT OF HIGH-HIGH TRIP

10.1 ARCHITECTURE AND COMMON CAUSE

In order to demonstrate the achievement of a particular SIL the architectural requirements specified in IEC 61511 must be satisfied by the high level trip. The hardware was selected on the basis of prior use and the requirements of Clause 11.5.3 of IEC 61511-1:2003 have been satisfied.

The trip equipment is adequately protected against interference by:

- key access to instrument cabinets and overrides; and
- rigorous access, testing and maintenance procedures operated by competent personnel.

Drawings show that for each tank the system is 1oo1 input (float level switch) and 2oo2 output (both delivery pumps need to be to shut-down) and the system is designed as fail-safe (relays that de-energise to trip.) Thus any connection failure leading to loss of communication between level sensor, the logic relays and circuit breaker will cause the pumps to shut-down.

IEC 61511 [Ref. 3] requires a minimum hardware fault tolerance of one for the sensor of a SIL 2 system unless the level measurement can be shown to be a Type A system with an SFF of greater than 60%. The ESD has zero hardware fault tolerance for the level measurement and data on SFF for high level float switches is not generally available. To calculate a precise SFF for the float switch and that test coverage is 100% would require a detailed FMEA in liaison with the supplier. Thus the assessment here is restricted to SIL 1.

10.2 HARDWARE FAULT TOLERANCE

For higher SIL, the hardware fault tolerance required depends upon the type (A or B) and safe failure fraction (SFF) of each sub-system, but Table 6 of IEC 61511-1:2003 specifies no hardware fault tolerance is required for SIL 1 sub-systems unless the logic solver is a Programmable Element (PE.)

10.2.1 Input / sensor sub-system

Each tank is equipped with a level switch comprising a micro-switch that opens on high level – actuated by movement of a displacer float. Each level switch is individually cabled (2 core cable) to tank farm instrument boxes.

10.2.2 Logic solver sub-system

Each level switch is connected to the High Level Panel and energises an individual Relay within the High Level Panel. These relays are non-PE logic solvers (Type A devices) and thus no hardware fault tolerance is required.

10.2.3 Output / final element / actuator sub-system

A NC and energised contact operates pump circuit breaker and when open shuts down the delivery pumps.

10.2.4 Power supplies

The high level trip is powered from a local distribution board. All circuits are designed 'fail open = trip.' If the power supply to the circuit breaker fails then the pumps will shut down.

10.2.5 Interfaces or any shared power supplies

There are no power shared supplies with the level displays – the trip system has an independent power supply and no interfaces with the level displays.

10.3 PROOF (TRIP) TEST INTERVALS

10.3.1 Test procedure

High level switches are tested monthly – using the in built test switch. One tank is used to initiate an ESD. Operation of this test is taken from level switch through control panel to trip the ESD circuit breaker. The remainder of tank high level switches are tested to ensure operation back to control panel that month. The test is repeated the following month – with a different tank – and repeated every month – all tanks tested over a 12 month period. Thus all elements of the system are tested.

10.3.2 PFD Calculation

Data from Appendices 3 & 4 of Ref. 13 is shown below in Table 4 and this is consistent with data from SINTEF-2006 [Refs 14 & 151.] No failure data has been included for the pumps as no failure mode has been identified where the pumps continue to operate without electric power. The tops of all the tanks are well above the delivery elevation so gravity feed would not cause an overflow.

Equipment	**λ failure rate per million hours**	**% of failures both dangerous and undetected (DU)**	**λ_{DU} failure rate per year** **(= λ DU / 11400)**
Level switch	5	50%	0.022
Logic relays (0.6 each)	1.2	10%	0.001
Circuit breaker relay	0.6	90%	0.004
Circuit breaker	2	40%	0.007
Total			**0.034**

Table 4 - Failure rates

Average PFD = (λ_{DU} x T)/2 where T = test interval in years and λ_{DU} failure rate per year.

Thus for an annual test interval

PFD = (0.034 x 1) / 2 = 0.017 which is well within the required range for SIL 1.

10.4 RESPONSE TIME

The pumps will stop within a few seconds after the electric power is removed. The actuators fitted to tank side valves have closure times typically 20 -30 seconds, and the valves are signalled to close, simultaneous with ESD circuit breaker.

10.5 RELATIONSHIP BETWEEN TRIP SETTING AND REMAINING ULLAGE

The time between the trip setting and the overflow of each tank are tens of minutes which gives more than enough time for both the pumps to shut down and the tankside valves to close.

10.6 MANUAL OVERRIDES/INHIBITS/BYPASSES/RESETS

Manual Operation ESD can be achieved by initiation of Terminal ESD pushbuttons that are located throughout the site, and within Control Room. There are no bypasses, inhibits or overrides on ESD circuit breaker. There is a test facility on the Level Switch and a keyswitch bypass on the high level switch for maintenance purposes.

The tankside valve system does have a keyswitch bypass to open a specific valve. This would prevent closing of the valve when the level in the tank rose, if the key switch was left in the wrong position.

If a high level were to occur, then once the high level is corrected, the trip can be reset manually and the pumps restarted.

10.7 FAILURE MODES, ACTIONS ON FAILURE AND REPAIR

The procedure for testing will identify nearly all failure modes. Relay logic components are all ‘off shelf’ items, with spares held on site and tank high level switches are typically on two months delivery.

Typical failure modes that might occur with float devices but not be detected by testing procedures are loss of buoyancy or sticking. However it is considered that the type of device used at this terminal is extremely unlikely to be affected in this way.

10.8 MODES OF OPERATION OF THE PLANT

10.8.1 Normal filling

Normal operation is described in Section **Error! Reference source not found.** above.

10.8.2 Maintenance

All maintenance works are implemented under a permit to work system. Removal of a high level switch for maintenance would be subject to a method statement / permit to work procedure which would require controlled bypass of the tank high level switch – keyswitch operation is required.

10.8.3 Testing

High Level Switches are equipped with a manual test facility (normally padlocked.) Operational Testing is implemented in accordance with a Test Procedure, on a monthly basis, with all tests results recorded. This work is carried out under a permit to work system.

10.8.4 Reducing level after a high-high level trip

Tank levels would be reduced after a high level trip by inter-tank transfer or by transfer of product from storage tank to road vehicles.

10.8.5 Major accident

In the event of a major accident then either:

- the ESD facility would still be available to protect against high level; or
- if the major accident damaged the communications or power supplies of the ESD, then the pumps would shut down because of the de-energise to trip design.

10.9 ENVIRONMENTAL CONDITIONS

High Level Switches are flange mounted on the storage tanks. All levels switches and associated junction boxes are IP56 minimum (level switches are EExd, and junction boxes are EExe. – suitable for use in a zone 1 hazardous area.)

All associated control equipment is located within the main office / control room. – air conditioned. The equipment room is monitored by a High Sensitivity Smoke Detector System, monitoring room, and floor voids, in addition to smoke detectors.

Switchgear is located in a separate brick built / flat roof building housing the relays and circuit breakers.

10.10 ADDITIONAL ASSUMPTIONS

As well as the assumptions already described, the calculations and assessments above include some additional assumptions.

10.10.1 Safety Management System

IEC 61511-1:2003 also specifies the safety management system (SMS) that is required to ensure that a SIL 1 system is correctly operated and maintained, for example the procedures for changing trip points/settings. The SMS at the Oil Terminal is not part of this assessment.

10.10.2 Test and repair times

The calculations assume that the downtime, the whole of the proof (trip) test and repair time, is negligible compared with T, the test interval and that testing and repair is perfect. .

The test time is normally less than 4 hours compared with a test interval of hundreds of hours. Rigorous testing and maintenance procedures are operated by competent personnel to ensure this is true

10.10.3 Data about failure rates

The calculations assume that failures are random and failure rates are constant. Equipment is used well within the expected life to avoid failures caused by wear and to ensure this assumption is reasonable. The failure data used in the calculations is applicable to the equipment and the environment at the oil terminal. To provide confidence in the data:

a) the identification of the equipment is clear;

b) conservative figures have been used; and

c) more than one source of data has been used.

11 CONCLUSIONS

The results show that the **total safety PLL** attributable to a tank overfill accident on the site is 4.6E-06 per year. This is below the target PLL of 1E-05 per year for the overfill hazard. The major contribution to the safety risk is the vapour cloud explosion event and a suitable high level trip protects against this event. This is assumed to have such a high severity (as per the HOSL accident) that a large number of fatalities are assumed to occur. The contribution to the safety risk from the catastrophic tank collapse following a bund fire is significantly less.

In assessing the above risk an assumed probability of failure on demand (PFD) for a SIL 1 system of 0.03 has been used. The work then done to evaluate the overfill protection system demonstrated a PFD of 0.017 and that the existing system comfortably meets SIL 1 performance requirements. A further revision of the risk analysis using this lower PFD would therefore give lower values of Potential Loss of Life (PLL) than outlined above although this has not been carried out and the results reflect some conservatism.

The published Buncefield Fire Report (Reference 12) from the Major Incident Investigation Board (MIIB) has listed a comprehensive set of recommendations relating to the Design and Operation of Fuel Storage Sites. Recommendation No. 1 ‘Systematic assessment of safety level requirements’ has been addressed by the analysis in this case study.

12 REFERENCES AND BIBLIOGRAPHY

1. The Buncefield Investigation: Third Progress Report, Buncefield Major Incident Investigation Board, 2006.

2. Guidance for the Location and Design of Occupied Buildings on Chemical Manufacturing Sites. Published by the Chemical Industries Association; 1998.

3. International Standard IEC 61511: “Safety Instrumented Systems for the Process Industry Sector – Functional Safety”, International Electrotechnical Commission.

4. International Standard IEC 61508: “Functional safety of electrical / electronic / programmable electronic safety-related systems”, International Electrotechnical Commission.

5. “Guidance on ‘as low as reasonably practicable’ (ALARP) decisions in control of major accident hazards (COMAH)”, http://www.hse.gov.uk/comah/circular/perm12.htm

6. “Reducing risks, protecting people – HSE’s decision making process”, HMSO, 2001, ISBN 0 7176 2151 0

7. “HID’s approach to 'As Low As Reasonably Practicable' (ALARP) decisions”, http://www.hse.gov.uk/comah/circular/perm09.htm

8. HSG 190. “Preparing safety reports - Control of Major Accidents Hazards Regulations 1999” HSE Books, 1999, ISBN 0717616878

9. “Application of Safety Instrumented Systems for the Process Industries”, Instrument Society of America Standards and Practices, ANSI / ISA-SP 84.01-1996

10. “Layer of Protection Analysis – Simplified Process Risk Assessment”, American Institute of Chemical Engineers, 2001, ISBN 9-780816-908110

11. Methods For The Determination of Possible Damage, TNO Green Book CPR16E

12. Buncefield Report No.5, Recommendations on the design and operation of fuel storage sites, Major Incident Investigation Board (MIIB), April 2007.

13. Reliability, Maintainability and Risk, 6th Edition, David J Smith, Butterworth-Heinemann, ISBN 0-7506-5168-7, 2001

14. SINTEF-2006 Reliability Data for Safety Instrumented Systems, PDS Data Handbook. April 2006, Sydvest Software

15. 3.SINTEF-2006 Reliability Prediction Method for Safety Instrumented Systems, April 2006, Sydvest Software

13 ABBREVIATIONS

CIA	Chemical Industries Association
COMAH	Control Of Major Accident Hazards (Regulations)
ESD	Emergency Shut-Down
F2	Atmospheric conditions - Very stable wind, speed 2 metres / second
FS	Float Switch
HOSL	Hertfordshire Oil Storage Limited
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
λ_{DU}	Undetected failures per million hours
LPG	Liquified Petroleum Gas
MAH	Major Accident Hazard
NC	Normally Closed
PE	Programmable Element
PFD	Probability of Failure on Demand
PLL	Potential Loss of Life
PLLH	Potential Loss of Life per Hazard
R2P2	“Reducing Risks, Protecting People”, HSE publication
RRF	Risk Reduction Factor
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
VCE	Vapour Cloud Explosion

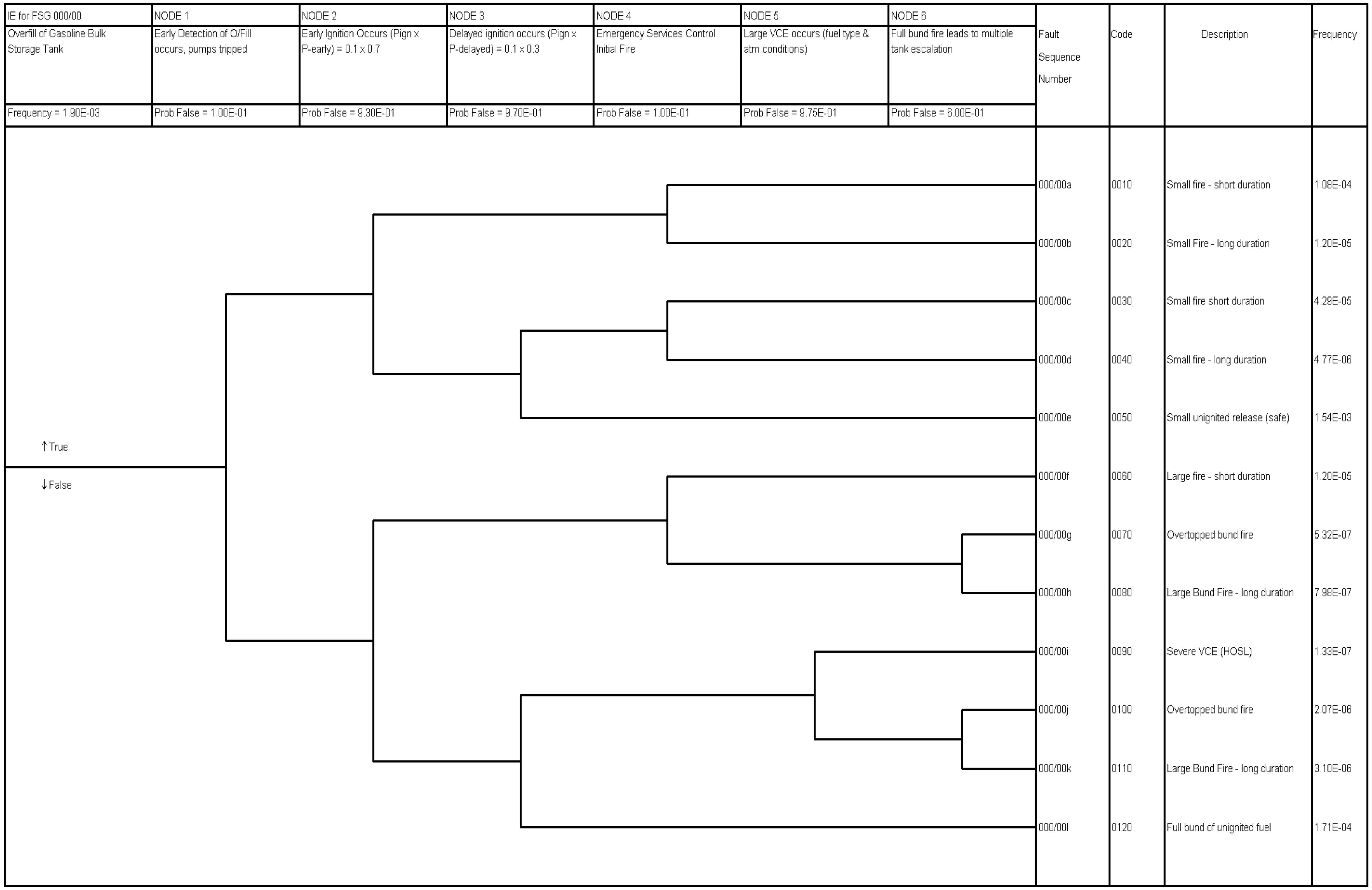
14 APPENDIX 1 - LOPA

Figure 14-1 - LOPA leading to tank overfill

Ref. IEC 61511 - 61508 Case study	Impact event description	Severity Level Potential Loss of Life (PLL)	Initiating cause	Initiating likelihood (events per year)	PROTECTION LAYERS					Intermediate event likelihood (events per year)	SIF PFD (probability)	Mitigated event likelihood (events per year)
					General process design (probability)	BPCS (probability)	Alarms, etc. (probability)	Additional mitigation (restricted access) (probability)	IPL additional mitigation (bunds, pressure relief) (probability)			
Level Displays assumed to be working correctly.	Overflow of storage tank during delivery	See Event Tree for details.	Connection to wrong tank by opening incorrect valve for example because delivery in wrong order.	0.1	Procedures require checks by staff that sufficient space is available and that correct tank is used for delivery hence frequency figures used in Column "Initiating likelihood" in events per year	Procedures require staff to monitor delivery using Level Displays but, as these are the same staff as those who are setting up the delivery no additional risk reduction is claimed.	The Level Displays include High and High High Alarms and, although the same staff respond to these alarms as those who are setting up and monitoring the delivery additional risk reduction is claimed as the alarms provide a second chance to detect an error	The site is secured by fence and locked gates with access by a gate controlled by a security guard. Approximately 13 staff are on site during delivery (plus office staff). As this analysis is of tank overflows, no risk reduction has been claimed for occ	The petrol tanks are bunded so any overflow should be contained within the bund. As this analysis is of tank overflows, no risk reduction has been claimed for the bund.		There is an independent high level trip that closes tankside valves. This system is tested yearly (assume SIL 1 hence PFD of 0.03).	
			Insufficient space in correct tank before delivery commences	0.033								
A				0.133	1	1	0.1	1	1	0.013	0.03	0.0004
Level Displays assumed to be faulty.	Overflow of storage tank during delivery	See Event Tree for details.	Level Displays assumed to fail once in 10 years (assume 50% fail high and 50% fail low) hence false low level once in 20 years.	0.05	Procedures require checks by staff that sufficient space is available and that correct tank is used for delivery hence frequency figures used in Column "Initiating likelihood" in events per year	Procedures requires staff to monitor deliveries using Level Displays but assumed to be faulty so no risk reduction claimed.	Level Displays include High and High High Alarms but assumed to be faulty.	The site is secured by fence and locked gates with access by a gate controlled by a security guard. Approximately 13 staff are on site during delivery (plus office staff). As this analysis is of tank overflows, no risk reduction has been claimed for occ	The petrol tanks are bunded so any overflow should be contained within the bund. As this analysis is of tank overflows, no risk reduction has been claimed for the bund.	.The total figure below is the estimate for tank overflows per year without the high level trip (ESD).	There is an independent high level trip that closes tankside Rotork valves. This system is tested monthly (assume SIL 1 hence PFD of 0.03).	The total figure below is the estimate for tank overflows per year with the high level trip (ESD)
B				0.05	1	1	1	1	1	0.050	0.03	0.0015
Total A+B				**Total for maloperation by staff and malfunction of Level Displays**						**0.063**		**0.0019**

15 APPENDIX 2 – EVENT TREE

Figure 15-1 - Event tree following tank overfill



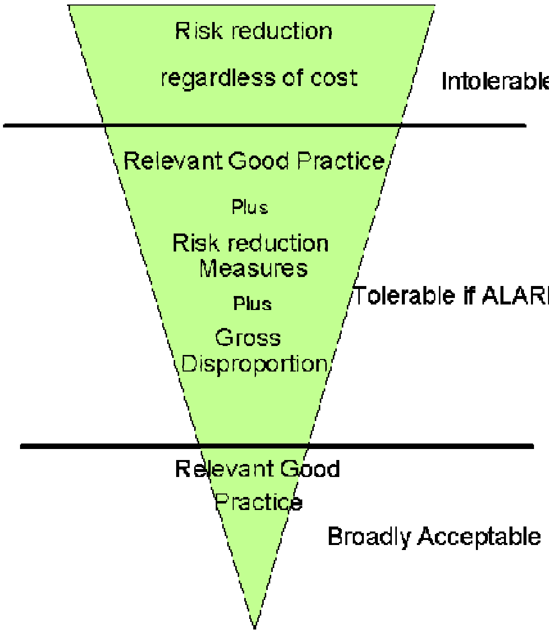
IE for FSG 000/00	NODE 1	NODE 2	NODE 3	NODE 4	NODE 5	NODE 6
Overfill of Gasoline Bulk Storage Tank	Early Detection of O/Fill occurs, pumps tripped	Early Ignition Occurs (Pign x P-early) = 0.1 x 0.7	Delayed ignition occurs (Pign x P-delayed) = 0.1 x 0.3	Emergency Services Control Initial Fire	Large VCE occurs (fuel type & atm conditions)	Full bund fire leads to multiple tank escalation
Frequency = 1.90E-03	Prob False = 1.00E-01	Prob False = 9.30E-01	Prob False = 9.70E-01	Prob False = 1.00E-01	Prob False = 9.75E-01	Prob False = 6.00E-01

Fault Sequence Number	Code	Description	Frequency
000/00a	0010	Small fire - short duration	1.08E-04
000/00b	0020	Small Fire - long duration	1.20E-05
000/00c	0030	Small fire short duration	4.29E-05
000/00d	0040	Small fire - long duration	4.77E-06
000/00e	0050	Small unignited release (safe)	1.54E-03
000/00f	0060	Large fire - short duration	1.20E-05
000/00g	0070	Overtopped bund fire	5.32E-07
000/00h	0080	Large Bund Fire - long duration	7.98E-07
000/00i	0090	Severe VCE (HOSL)	1.33E-07
000/00j	0100	Overtopped bund fire	2.07E-06
000/00k	0110	Large Bund Fire - long duration	3.10E-06
000/00l	0120	Full bund of unignited fuel	1.71E-04

16 APPENDIX 3 – HSE REQUIREMENTS FOR RISK ASSESSMENT

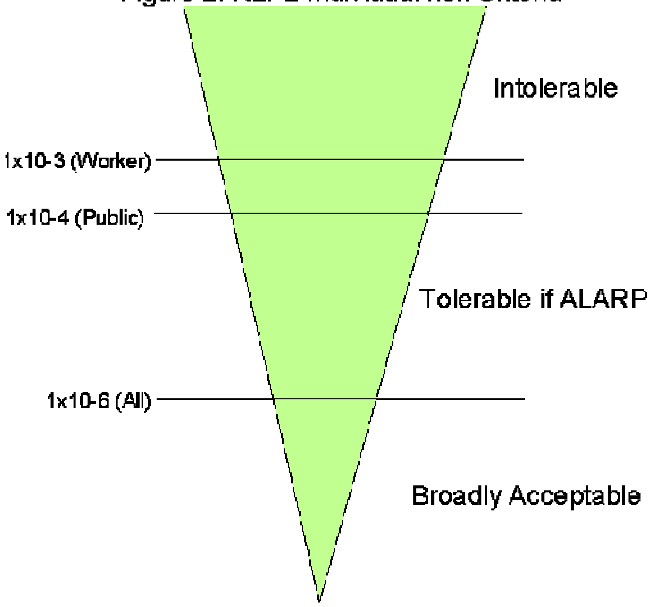
Figure 1 shows the HSE requirements [Ref. 3] to demonstrate that risks have been reduced As Low As Reasonably Practicable (ALARP). Figure 1 shows risk increasing up the page; three regions or ranges of risk labelled: Intolerable, Tolerable if ALARP, and Broadly Acceptable; and two boundaries, sometimes called the "upper and lower ALARP boundaries." Figure 1 also indicates the approaches required to demonstrate that ALARP is being achieved for each of the three regions of risk.

Figure 1: Types of ALARP Demonstration



The HSE defines [Ref. 3 & 4 "R2P2"] the two ALARP boundaries in numerical terms for individual and societal risk. The risk criteria are individual risks of death per year (to be distinguished from other types of risk such as risk of dangerous dose used in HSE`s land use planning approach).

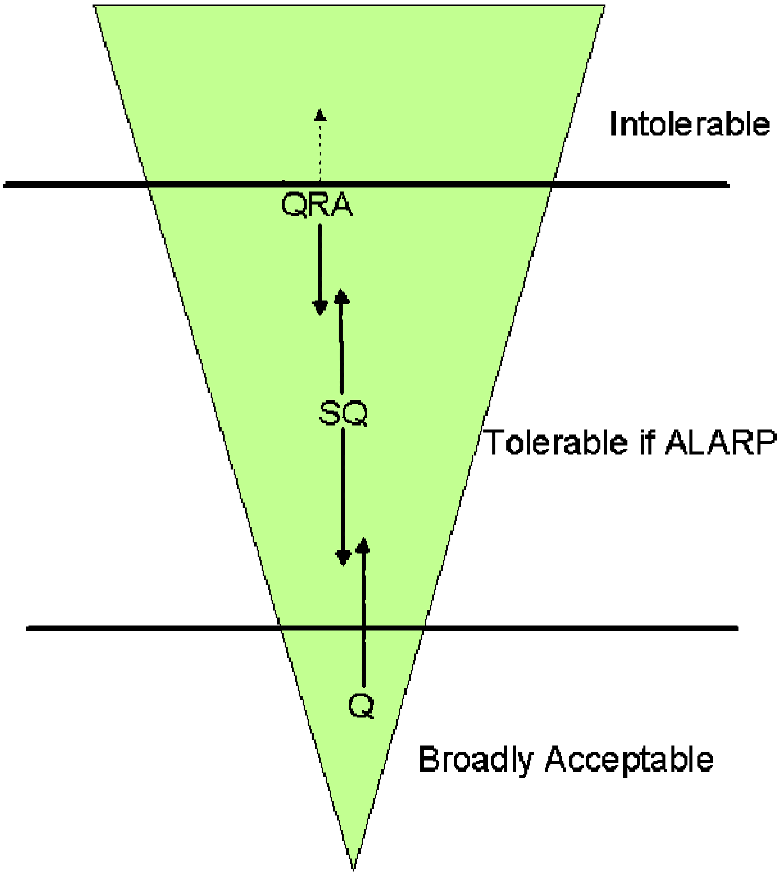
Figure 2: R2P2 Individual risk Criteria



People at risk include staff, customers, suppliers, other stakeholders and members of the public. Figure 2 uses the term “Worker” and “Public” where the HSE consider [Ref. 4 on page 46] members of the public as those who have a risk imposed on them “in the wider interest of society”. In addition members of the public may not be aware of the relevant risk controls and this might include some stakeholders, for example customers, neighbours and shareholders. Workers include employees, contractors, suppliers and all those on-site exposed to the risks. They should be competent to apply the relevant risk controls or supervised by someone who is competent. Thus this case study considers everyone in only two categories: worker and public. A diagram similar to Figure 2 can also be constructed for societal risks with appropriate criteria.

The HSE states [Ref. 3] that the type of risk assessment an assessor would expect to see in a safety report depends on the level of risk (either individual or societal) and this is illustrated in Figure 3. The definitions of Q, SQ and QRA methods are set down in HSG 190 [Ref. 6].and vary gradually in depth and level of quantification from qualitative (Q) at one end to full quantified risk assessment (QRA) at the other

Figure 3: Types of Risk Assessment



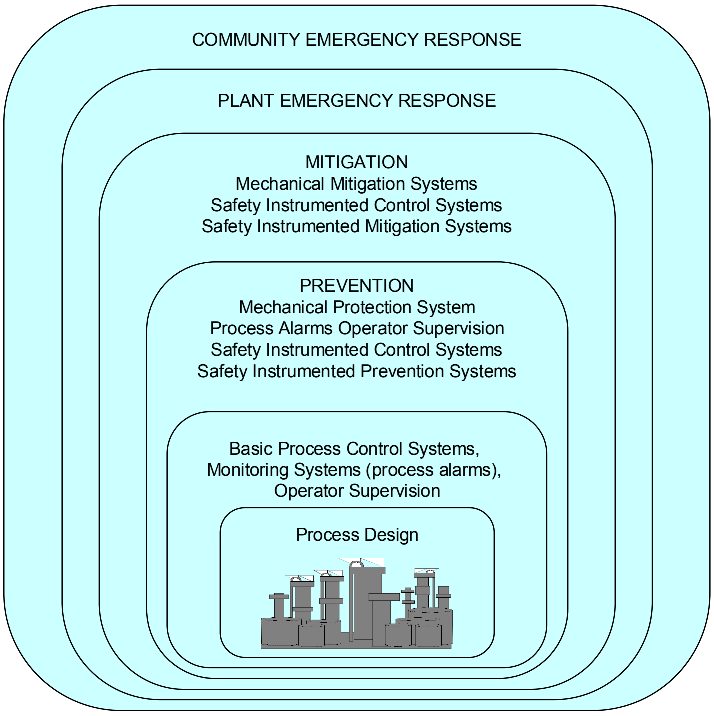
Thus for the overfill hazard at an Oil Terminal both a Semi-Quantitative (SQ) method of Layer Of Protective Analysis (LOPA) and an Event Tree (a QRA technique) were used.

17 APPENDIX 3 - IEC 61511 & LOPA & QRA

17.1 OUTLINE OF LOPA

If a specific residual risk is assessed as not close to broadly acceptable, or the requirement for further risk reduction is "IL 2" or greater than "IL 2", then a method of risk assessment more rigorous than qualitative is required. As shown in Figure 3, a semi-quantitative method is required, for example, Layer of Protection Analysis [Ref. 10]. The introduction of the layer of protection concept originates from the American approach to Safety Instrumented Systems in ANSI ISA S84.1996 [Ref. 7] and is illustrated in [Ref. 10]. This standard has been the major influence in the differences between IEC 61508 and IEC 61511. An outline of LOPA is given below; details are in [Ref. 8.]

Figure 17-1 - Concept of Layers of Protection


COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
MITIGATION
Mechanical Mitigation Systems
Safety Instrumented Control Systems
Safety Instrumented Mitigation Systems
PREVENTION
Mechanical Protection System
Process Alarms Operator Supervision
Safety Instrumented Control Systems
Safety Instrumented Prevention Systems
Basic Process Control Systems,
Monitoring Systems (process alarms),
Operator Supervision
Process Design

Each of the hazards is analysed in terms of:

- Consequence description ("Impact Event Description")
- Estimate of consequence severity ("Severity Level")
- Description of all causes which could lead to the Impact Event ("Initiating Causes")
- Estimate of frequency of all Initiating Causes ("Initiation Likelihood")

The Severity Level may be expressed in semi-quantitative terms, linked to target Mitigated Event Likelihoods expressed as target frequency ranges (analogous to tolerable risk levels), as shown in Table 5 - Example Definitions of Severity Levels and

Mitigated Event Frequencies; or it may be expressed as a specific quantitative estimate of harm, which can be referenced to F-N curves.

Similarly, the Initiation Likelihood may be expressed semi-quantitatively, as shown in Table 5; or it may be expressed as a specific quantitative estimate.

Table 5 - Example Definitions of Severity Levels and Mitigated Event Frequencies

Severity Level	Consequence	Target Mitigated Event Likelihood
Minor	Serious injury at worst	No specific requirement
Serious	Serious permanent injury or up to 3 fatalities	< 3E-6 per year, or 1 in > 330,000 years
Extensive	4 or 5 fatalities	< 2E-6 per year, or 1 in > 500,000 years
Catastrophic	> 5 fatalities	Use F-N curve

Table 6 - Example Definitions of Initiation Likelihood

Initiation Likelihood	Frequency Range
Low	< 1 in 10,000 years
Medium	1 in > 100 to 10,000 years
High	1 in ≤ 100 years

The strength of the method is that it recognises that in the energy and process industries there are usually several layers of protection against an Initiating Cause leading to an Impact Event.

Specifically, LOPA identifies:

•General Process Design. There may, for example, be aspects of the design that reduce the probability of loss of containment, or of ignition if containment is lost, so reducing the probability of a fire or explosion event.

•Basic Process Control System (BPCS). Failure of a process control loop is likely to be one of the Initiating Causes. However, there may be another independent control loop that could prevent the Impact Event, and so reduce the frequency of that event.

•Alarms. Provided there is an alarm that is independent of the BPCS, sufficient time for an operator to respond, and an effective action to take (a “handle” to “pull”), credit can be taken for alarms to reduce the probability of the Impact Event up to a Risk Reduction Factor (RRF) of 10 or a Probability of Failure on Demand (PFD) of 0.1.

•Additional Mitigation, Restricted Access. Even if the Impact Event occurs, there may be limits on the occupation of the hazardous area (equivalent to the F parameter in the risk graph method), or effective means of escape from the hazardous area (equivalent to the P parameter in the risk graph method), which reduce the Severity Level of the event.

•Independent Protection Layers (IPLs). A number of criteria must be satisfied by an IPL to be assured that it is genuinely independent of other protective layers and achieves RRF ≥ 10. Relief valves and bursting discs usually qualify for RRF ≥ 100.

Based on the Initiating Likelihood (frequency) and the PFDs of all the protection layers listed above, an Intermediate Event Likelihood (frequency) for the Impact Event and the Initiating Event can be calculated. The method must be completed for all Initiating Events, to determine a total Intermediate Event Likelihood (frequency) for all Initiating Events. This can then combined with the Estimate of consequence severity ("Severity Level") and compared with the numerical Corporate Risk Criteria or Targets (Mitigated Event Likelihood) and the HSE boundaries for the "Tolerable if ALARP" region. So far no credit has been taken for the risk reduction from any SIF. The ratio:

(Intermediate Event Likelihood) / (Mitigated Event Likelihood)

gives the required RRF (or 1/PFD) of the SIF, and can be converted to a required SIL using Table 1. Alternatively the inverse ratio

(Mitigated Event Likelihood) / (Intermediate Event Likelihood)

gives the required PFD of the SIF that can be converted to a required SIL.

17.2 LIMITATIONS OF LOPA

Both LOPA and QRA require numerical Corporate Risk Criteria or Targets (Mitigated Event Likelihood). If the results of LOPA are that the IL requirement for further risk reduction is none, "a" "IL 1" or "IL 2" then no further risk assessment is required. If the results of the LOPA are that the IL requirement for further risk reduction is "IL 3" or greater than "IL 3" then further risk assessment is recommended. This is because:

- higher risks require more rigorous risk assessment; and
- "IL 3" systems are very expensive to provide, operate and maintain.

17.3 QUANTITATIVE RISK ASSESSMENT (QRA) METHODS

If a specific residual risk is assessed as close to intolerable, or the requirement for further risk reduction is "IL 3" or greater than "IL 3" then a full quantitative risk assessment (QRA) is recommended. Event Trees are one example of a QRA method. Details can be found in textbooks such as Ref. 9.