HSE

Health and Safety
Executive

A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks

Prepared by **Health and Safety Laboratory**
for the Health and Safety Executive 2009

RR716
Research Report

HSE

Health and Safety
Executive

A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks

Colin Chambers, Jill Wilday & Shane Turner
Health and Safety Laboratory
Harpur Hill
Buxton
Derbyshire
SK17 9JN

In response to the Buncefield incident, the Major Incident Investigation Board (MIIB) made recommendations to improve safety in the design and operation of fuel storage sites. Two of these recommendations were that loss of primary containment (tank overfill) should be prevented by a high integrity system, and that industry should agree to undertake a systematic assessment of safety integrity levels using commonly agreed methods.

The Buncefield Standards Task Group (BSTG), consisting of representatives from industry and the control of major accident hazards (COMAH) Competent Authority, also stated in its final report, Paragraph 16, "Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve." The BSTG report suggests a layer of protection analysis (LOPA) study be used to provide a more consistent approach to safety integrity level (SIL) determination.

Therefore, in response to the MIIB and BSTG recommendations this study aimed to identify common trends and instances of good practice and areas requiring discussion / improvement in the way in which LOPA studies were carried out by operators of sites that bulk store fuels such as petrol.

This study is part of ongoing work to stimulate discussion between concerned parties with the aim of contributing to the development of improved guidance.

Further guidance can be found on the relevant HSE websites.

http://www.buncefieldinvestigation.gov.uk
http://www.hse..gov.uk/buncefield/response.htm

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

HSE Books

© Crown copyright 2009

First published 2009

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of the copyright owner.

Applications for reproduction should be made in writing to:
Licensing Division, Her Majesty's Stationery Office,
St Clements House, 2-16 Colegate, Norwich NR3 1BQ
or by e-mail to hmsolicensing@cabinet-office.x.gsi.gov.uk

ACKNOWLEDGEMENTS

The authors would like to acknowledge the help and advice from HSL colleagues in the Risk Science Unit, who made useful contributions regarding the human factors aspects of this work. I would also like to thank all those in the Health and Safety Executive (HSE), including Control and Instrumentation specialist inspectors from the Hazardous Installations Directorate, who supplied example layers of protection analysis (LOPA) assessments so that the work could proceed.

CONTENTS

1 INTRODUCTION 4
1.1 Study method 5
1.2 Report structure 6

2 COMPANY A; LOPA ID 1 7
2.1 Introduction 7
2.2 Risk tolerance criteria 7
2.3 Initiating events 7
2.4 Conditional modifiers 12
2.5 Protection layers 13
2.6 General comments 14
2.7 LOPA conclusions 14

3 COMPANY B; LOPA ID 2 15
3.1 Introduction 15
3.2 Risk tolerance criteria 15
3.3 Initiating events 15
3.4 Conditional modifiers 17
3.5 Protection layers 18
3.6 General comments 19
3.7 LOPA conclusions 20

4 COMPANY C; LOPA ID 3 21
4.1 Introduction 21
4.2 Risk tolerance criteria 21
4.3 Initiating events 21
4.4 Conditional modifiers 22
4.5 Protection layers 22
4.6 General comments 23
4.7 LOPA conclusions 24

5 COMPANY D; LOPA ID 4 25
5.1 Introduction 25
5.2 Risk tolerance criteria 25
5.3 Initiating events 25
5.4 Conditional modifiers 30
5.5 Protection layers 30
5.6 General comments 31
5.7 LOPA conclusions 31

6 COMPANY E; LOPA ID 5 33
6.1 Introduction 33
6.2 Risk tolerance criteria 33
6.3 Initiating events 33

6.4 Conditional modifiers....35
6.5 Protection layers....36
6.6 General comments....37
6.7 LOPA conclusions....37

7 COMPANY F; LOPA ID 6....39
7.1 Introduction....39
7.2 LOPA Risk tolerance criteria....39
7.3 Initiating events....39
7.4 Conditional modifiers....40
7.5 Protection layers....41
7.6 General comments....41
7.7 LOPA conclusions....42

8 COMPANY G; LOPA ID 7....43
8.1 Introduction....43
8.2 Risk tolerance criteria....43
8.3 Initiating events....43
8.4 Conditional modifiers....44
8.5 Protection layers....45
8.6 General comments....45
8.7 LOPA conclusions....46

9 MAIN FINDINGS....47
9.1 General trends....47
9.2 Initiating events....47
9.3 Conditional modifiers....49
9.4 Protection layers....49
9.5 Risk tolerance criteria....49
9.6 Conclusions....50

10 APPENDIX A – LOPA CASE DATA: SUMMARY OF CM, IE & IPL....52

11 APPENDIX B – LOPA CASE DATA: SUMMARY OF MITIGATED & UNMITIGATED CONSEQUENCE, TARGET SIL & SIL GAP....55

12 REFERENCES....56

13 GLOSSARY....57

EXECUTIVE SUMMARY

Background

In response to the Buncefield incident, the Major Incident Investigation Board (MIIB) made recommendations to improve safety in the design and operation of fuel storage sites. Two of the MIIB recommendations for the design and operation of fuel storage systems were that loss of primary containment (tank overfill) should be prevented by a high integrity system, and that industry should agree to undertake a systematic assessment of safety integrity levels using commonly agreed methods.

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. Its aim was to translate the lessons from Buncefield into effective and practical guidance that industry could implement as rapidly as possible.

As stated in the BSTG final report, Paragraph 16, "Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve." The BSTG report suggests a layer of protection analysis (LOPA) study be used to provide a more consistent approach to safety integrity level (SIL[1]) assessment.

The LOPA method has been adopted by industry, which has submitted LOPA studies for its fuel storage overfill prevention systems to the Health and Safety Executive (HSE) for assessment. HSE would like to identify any common issues associated with industry's application of the LOPA method, which can then be fed back to industry.

The Hazardous Installations Directorate (HID) of HSE therefore asked the Health and Safety Laboratory (HSL) to analyse a sample of LOPA studies submitted by operators of Buncefield-type COMAH sites that store flammable liquids such as petrol; seven of these LOPA studies are presented in this report.

Objectives

- Assess a sample of LOPA studies submitted to HSE by operators of top tier COMAH sites that bulk store fuels such as petrol, whose loss of containment could result in a vapour cloud explosion (VCE);
- Outline common trends and instances of good practice and areas requiring discussion /improvement;
- Provide a report that will allow HSE to provide feedback to those who perform LOPA studies (dutyholders and consultants).
- Publishing this Report to stimulate further discussion and improvements in LOPA and similar studies.

[1] *Where the failure of a process can result in a certain level of risk, suitable prevention measures that are able to control, protect or mitigate this level of risk, need to be implemented. In the process sector, conformance to BS EN 61511 enables the safety performance requirements for these risk reduction measures to be quantified by means of the Safety Integrity Level (SIL). The SIL, which is assigned to a safety integrity function (SIF), determines the rigour applied to the development and operation of the safety instrumented system (SIS) which implements the SIF. BS EN 61511 also states the maximum performance claims that can be made by the basic process control system (BPCS), which does not conform to this standard.*

Caveats

The LOPA study reviews in this work are based on the information supplied by companies, or their consultants, to HSE. They have for the purpose of this study been taken at face value without any other knowledge of the sites or systems involved.

We would stress that the data (including risk targets) in this Report are not endorsed by HSL or HSE.

One of the key messages of this study is that a LOPA or similar risk study has to be justified against the particular circumstances at the establishment and the legal requirements for health and safety. This includes the organisational and procedural aspects as well as the safety integrity of technical systems.

Main Findings

The majority of LOPA studies assessed were for petrol import, however, some were for kerosene and other flammable liquids such as ethanol. The majority of substance transfers were from ship or pipeline, with one exception being from railcar and another being tank-to-tank transfers.

A number of issues for discussion with industry and other stakeholders were identified in the way LOPA studies were performed. These included:

- Quality of data and data sources used varied widely. In the majority of LOPA studies assessed in this work, some data used were found to be inappropriate and / or contained a high degree of uncertainty.

- The degree of rigour applied to the LOPA studies considered in this work varied widely.

- There were inconsistencies in how dependencies between initiating events and protection layers are handled in some of the LOPA studies assessed in this work.

- In some LOPA studies initiating events were broken down into a number of components, with an error probability assigned to each component, with the assumption that each component is independent. This may not have been the case and could have lead to unrealistically low initiating event frequencies.

- Human factors appear to dominate a number of initiating event (IE) frequencies and conditional modifier (CM) error probabilities in all the LOPA studies assessed in this work.

- A sensitivity study does not appear to have been carried out in the majority of LOPA studies considered in this work. A sensitivity study, based on one variable, was performed in one of the LOPA studies assessed.

- Other common issues requiring attention were the use of invalid logical arguments (e.g. conflicting CM arguments), and the omission of supporting information.

It is noted that the majority of LOPA studies considered in this work were carried out by consultants who have, in general, made recommendations to their clients to implement high integrity tank overfill prevention systems, which the HSL considers (in the light of the problems identified) to be a good position to take.

A significant conclusion of this work is that industry should therefore take steps to:

- Improve the knowledge and training of those carrying out LOPA studies;

- Develop better procedures and guidance for the study, including such matters as sensitivity analyses and the standards of documentation and support information to be included;

- Improve the quality of data it uses in the LOPA studies.

It is understood that HSE now intends to hold further discussions with industry regarding the findings of this LOPA study to agree a way forward.

1 INTRODUCTION

In response to the Buncefield incident, the Major Incident Investigation Board (MIIB) made recommendations to improve safety in the design and operation of fuel storage sites [1]. Two of the MIIB recommendations for the design and operation of fuel storage systems were that loss of primary containment (tank overfill) should be protected by a high integrity system, and that industry should undertake the systematic assessment of safety integrity levels using commonly agreed methods.

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. Its aim was to translate the lessons from Buncefield into effective and practical guidance that industry could implement as rapidly as possible.

As stated in the BSTG final report [2], Paragraph 16, "Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve." The BSTG report suggests a layer of protection analysis (LOPA) study to provide a more consistent approach to safety integrity level (SIL[1]) assessment.

The LOPA method appears to have been widely adopted by industry, which has submitted LOPA studies for its fuel storage overfill prevention systems to the Health and Safety Executive (HSE) for assessment.

Aims

The aims of this project were to:

- Assess a sample of LOPA studies submitted to HSE by operators of top tier COMAH sites that store fuels such as petrol, whose loss of containment could result in a vapour cloud explosion (VCE);
- Outline common trends and instances of good practice and areas requiring discussion/improvement;
- Publish this Report to stimulate further discussion and improvements in LOPA and similar studies

Caveats

The LOPA study reviews in this work are based on the information supplied by companies or their consultants to HSE. They have for the purpose of this study been taken at face value without any other knowledge of the sites or systems involved.

We would stress that the data (including risk targets) in this Report are not endorsed by HSL or HSE.

One of the key messages of this study is that a LOPA or similar risk study has to be justified against the particular circumstances at the establishment and the legal requirements for health and safety. This includes the organisational and procedural aspects as well as the safety integrity of technical systems.

1.1 STUDY METHOD

HSE supplied HSL with 15 LOPA studies, of which a representative sample of seven were reviewed in detail in this report. This was in order to minimise repetition in terms of type of site and fuel transfer mechanism. Data from all 15 LOPA studies is presented in Appendices A and B. Company names and other information have been removed to provide anonymity. Table 1 lists the LOPAs that have been presented in this report. The scope of these LOPA studies was the overfill prevention of tanks storing a flammable liquid, typically petrol. Examples of other flammable liquids, such as kerosene and ethanol, were also considered.

Table 1 Reviewed LOPAs

LOPA study ID	*Company*
1	Company A
2	Company B
3	Company C
4	Company D
5	Company E
6	Company F
7	Company G

The following areas have been explicitly reviewed in each LOPA report:

- the chosen risk target;
- initiating events;
- conditional modifiers;
- protection layers; and
- overall conclusions.

Consideration has been given to: why aspects of each LOPA have been included; omissions; and the basis of any assumptions.

In addition to reviewing each LOPA separately, a generic review across the sample of reports was carried out on the use of conditional modifiers and protection layers, the summary of which is presented in Appendix A.

HSL was asked to review the LOPA studies as presented, which is why it is not possible to make a detailed assessment. Some comments in this report may not be correct because the information provided is open to interpretation, and the site-specific data may differ to that presented in the LOPA.

HSL hopes that lessons learned in this work will help companies improve their LOPA studies in the future.

1.2 REPORT STRUCTURE

The remainder of the report is structured as follows:

- Sections 2 to 8 discuss each LOPA in turn.
- Section 9 presents the main findings from across all the LOPAs examined.
- Section 9 also presents the conclusions and recommendations.
- Appendices A & B present calculation data based on information given by each LOPA case.

2 COMPANY A; LOPA ID 1

2.1 INTRODUCTION

This LOPA report [3] is for ship transfer of kerosene to two out of three tanks and ethanol to two out of four tanks. In both cases it is stated that the intent is only to transfer to a single tank in any delivery, although it is stated that this cannot be guaranteed.

All level gauges are local to a corresponding tank, and are monitored by site operators, who intervene on detecting a high level by initiating a manual shutdown. There is an independent high level alarm, for each tank, hard wired to a control room annunciator and klaxons at selected locations including the jetty, which is monitored by the jetty operators. If this alarm were to be activated the operator would respond by initiating a manual shutdown by communicating with the ship and personnel on site, who would take the required action such as stopping the ship's pumps then shutting the site valves, etc.

2.2 RISK TOLERANCE CRITERIA

A risk tolerance criterion of 10^{-6} is stated in the LOPA as applying for all risks environmental, financial and safety. This risk tolerance criteria description is unclear and may be inappropriate for the following reasons:

- Environmental, financial and safety risks should be assessed separately and relevant criteria applied;
- This LOPA does not state what the risk tolerance criteria are, for example, risk of what, to what and from what;
- It is not clear whether the Individual Risk (IR) target represents all risks the hypothetical individual person faces on site or just those associated with a single tank and single hazard;
- No justification for the chosen criteria is presented in the LOPA assessment report, although a reference is made to the site COMAH safety report.

2.3 INITIATING EVENTS

Overflow as a result of the following four initiating events is considered:

- Excess fuel on ship;
- Incorrect line-up or changeover;
- Capacity of tank less than expected; and
- Failure of the tank gauging system.

Comments relating to each initiating event (IE) are summarised in the following subsections. Comments are given against the components of the initiating events where relevant.

2.3.1 IE1 – Excess fuel on ship

The initiating event frequency has been calculated based on the following components:

Table 2 Initiating event 1 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	14 (ethanol) 25 (kerosene)	Use of frequency of transfers appears appropriate.
2	Third party checks amount of fuel on board ship	0.001	It is not clear from the LOPA why these components are combined in this way because it appears to say that there is an excess amount of fuel on the ship (compared with documentation) and the third party incorrectly measures the wrong amount of fuel on the ship, which happens to be the same as that on the incorrect documentation. It appears more plausible that there is an error on the documentation and the third party fails to check the amount of fuel on the ship. It is noted, however, that this may not have a major impact on the calculated IE frequency. The human error probabilities (HEPs) are taken from BS EN 61511-3 table F.3 [4] without justification.
3	Ship has excess fuel compared with documentation	0.001	
4	Tank operator monitors transfer	0.1	This component may be double counting with protection layer 1 (PL1).

General comment relating to this IE:

- Because it is stated that the import from a ship is usually to a single tank, then it would appear appropriate to take no account of the number of tanks. However, it is stated that occasionally there is insufficient capacity in the receiving tank, and a sequential filling operation is then required. This does not appear to be taken into account in this IE or elsewhere[2]. Although it is accepted that operators are less likely to fail to change over tanks as there is an expectation that a tank will be approaching its maximum level, the overfill frequency would be greater in that case than for this IE, due to components 2 and 3 in the above table then being irrelevant.

[2] *IE2 refers to incorrect changeover. However, the logic appears to refer to changeover to an incorrect tank and not failure to changeover.*

2.3.2 IE2 – Incorrect line-up or changeover

The initiating event frequency has been calculated based on the following components:

Table 3 Initiating event 2 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	14 (ethanol) 25 (kerosene)	Use of frequency of transfers appears appropriate.
2	Error in connecting tanks	0.001	It is not clear whether this probability takes account of the number of tanks on the site, as there may be an increased probability of making a mistake if there are more tanks to connect to. This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
3	2nd operator confirms transfer into correct tank	0.01	Inclusion of this component appears reasonable as long as it is not reliant on the tank gauging system and is independent of PL1. This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.

General comment relating to this IE:

- It may be better for incorrect line-up and incorrect changeover to be separated into different IEs as some of the assumptions may need to differ.

2.3.3 IE3 – Capacity of tank less than expected

The initiating event frequency has been calculated based on the following components.

Table 4 Initiating event 3 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	14 (ethanol) 25 (kerosene)	Use of frequency of transfers appears appropriate.
2	Error in dipping tank by third party	0.001	This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
3	Operator confirms level from the tank gauge, checks ullage available and calculates batch fill level	0.001	Potential for common cause with PL1 may not have been adequately taken into account because this component relies on the tank level instrument and gauge. This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.

2.3.4 IE4 – Failure of tank level instrument

The initiating event frequency has been calculated based on the following components:

Table 5 Initiating event 4 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Failure of level instrument	0.1 per year	This appears to be calculated based on the minimum allowed in BS EN 61511 [4] for a non-SIL[1] related system (10^{-5} dangerous failures per hour, which equates to approximately 0.1 dangerous failures per year). The tank gauging system failure rate is not supported by evidence: not all tank gauging systems can claim this level of reliability. The level instrument used on site is not described in this LOPA, therefore making reliability claims unverifiable.
2	Tank being filled	0.008 (ethanol) 0.028 (kerosene)	Consideration of the proportion of time a tank is being filled is accepted as common, although not universal practice.
3	Operator fails to detect tank level system failure	0.1	It is not clear whether this HEP is already included in component 1 of this IE. If this component is considered separately from component 1, then consideration should be given of how to combine the two probabilities so that the tank gauging system total dangerous failure rate is not less than the approximate value of 1E-5 per hour allowed by BS EN 61511[4] for non-SIL[3] rated systems. Currently, this HEP is combined with component 1 using the AND operator, which results in a value that is lower than 0.1, which is lower than BSEN 61511 allows for non-SIL rated systems. This HEP is taken from BS EN 61511[4] without sufficient justification.

General comment relating to this IE:

- PL1 has been ignored in this case. This would appear sensible given that failure of the tank level device is considered in the IE.
- The tank gauging system is not described in the LOPA study report, e.g. is it a float device or servo gauge?

2.3.5 IE General comments

- The LOPA does not present a description of the process used to identify the IEs considered. Therefore, it is difficult to be confident that all reasonable failure modes of the bulk fuel storage tank and its operation have been identified. The inclusion of supplementary documents such as relevant excerpts from the HAZOPS / PHA as appendices in the LOPA study report would be helpful. See discussion on supplementary documentation in the report conclusions.

- Values assumed in the IEs are generally not justified. For example, reference is made to BS EN 61511 for human error probabilities. These should be estimated taking account of the site-specific factors. In addition, the IE component values assumed appear to be on the low side, and once combined, lead to very small IE frequencies. This could suggest that either the data or method of sub-dividing the IE into as many components may not be valid.
- Each IE has been broken down into a number of discrete tasks (or components), and a failure probability or frequency for each component determined. This has lead to very low frequencies being calculated when all the components were combined. A reality check appears to suggest there may be an issue here. The dependencies between the IE tasks may differ from that presented, possibly leading to a higher frequency of occurrence. Therefore, this approach may not be valid.

2.4 CONDITIONAL MODIFIERS

The main issues with this particular LOPA study in relation to the CMs are listed below.

Table 6 Conditional modifier assessment and comments

ID	*Conditional modifier*	*Value assumed*	*Comment*
CM1	Probability of failure to detect overflow	0.9	This would seem to be a protection / mitigation layer rather than a conditional modifier because it refers to a specific action performed by an operator to detect and prevent further loss of containment. It is unclear whether the operators who are expected to detect and take action are independent of those already performing other tasks. The LOPA study does not state whether a formal procedure ensures that this mitigation measure is rigorously applied.
CM2	Probability of ignition	0.1 (kerosene)	According to an HSL fire and explosion expert this probability would appear to be conservative for kerosene.
		0.1 (ethanol)	Ethanol is more conductive than petrol hence leading to a lower probability of static build-up leading to ignition. However, ethanol has a lower flash point than petrol. Therefore, this value would appear to be low. Kerosene and Ethanol are not considered likely to present a significant risk of a Buncefield type VCE.
CM3	Probability of personnel being in affected area	0.1	It is not clear how large the affected area has been assumed to be. Potentially a kerosene pool fire could affect persons in or close to the tank bund. It is not clear how this figure was derived. Personnel being in the affected area may be assumed within the probability of fatal injury (CM4).
CM4	Probability of a fatal injury	0.1	The probability of fatality may already be accounted for in the LOPA studies stated risk criterion. If that is the case then this conditional modifier may not be valid. This is stated, in the LOPA, as being low because the onsite population is low, but this argument is in conflict with CM3, which already accounts for the probability of someone being in the affected area. The probability of a fatal injury should assume that someone is within the hazard area and should therefore be higher.

General comments relating to the above CMs:

- Some of the CM probabilities appear to be too low;
- The assumed probabilities are not justified;
- Some double counting is present.

2.5 PROTECTION LAYERS

The following two protection layers (PLs) have been assumed:

- Level gauges monitored and checked by operator; and
- High level alarm with manual closure of valve(s).

These are discussed in the following subsections.

2.5.1 PL1 – Level gauges monitored

The assumed probability of failure (0.19) of this PL may be reasonable as a minimum value. It is assumed that the Probability of Failure on Demand (PFD) of the hardware is 0.1 and the PFD of the operator to respond appropriately is 0.1. The overall failure of the protection layer is assumed to be the PFD of the hardware OR HEP of the operator. However, neither the tank level gauging system PFD or operator HEP are supported by evidence.

2.5.2 PL2 – High level alarm with manual closure of valve(s)

The assumed probability of failure has been calculated in the same way as the other protection layer. Again, the assumed probability of failure of 0.19 of this PL appears reasonable as a minimum value. It is claimed that the high level alarm is independent of the level gauge system, and that the operator here is independent of the operator who monitors the level gauge above. If these PLs are truly independent and common cause failure between them can be ruled out, as claimed, then inclusion of both PLs would generally appear reasonable. The only exception would be for IEs where either PL was already accounted for. Procedures associated with operator response to alarm should be formal and auditable; the LOPA does not state that this is the case.

2.5.3 PL general comments

General issues relating to this LOPA are summarised below:

- The major issue with the protection layers is that there is insufficient justification for the assumed PFDs. For example, the tank gauging PFD of 0.1 is not justified or supported by evidence.
- The first PL has been discounted for one of the initiating events. Where the tank gauging system is considered as part of the IE, this would be appropriate.
- Mechanical failure of the valve does not appear to have been considered in PL2. Procedures associated with operator response to alarm should be formal and auditable; the LOPA does not state that this is the case.
- The LOPA study report does not state what action is performed for PL1. It may be implied that the operator will initiate a manual shutdown: this should be explicitly stated, otherwise this is not a complete protection layer.

- The LOPA study does not account for the reliability of equipment on the ship or communication equipment and process, e.g. ships pumps, site valves, radios and communication procedures.

2.6 GENERAL COMMENTS

- Ethanol and kerosene vapour is not considered to represent a significant risk of a Buncefield type VCE.
- The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

2.7 LOPA CONCLUSIONS

The LOPA studies for ethanol and kerosene import have shown no shortfall against the assumed risk target. Based on this, the LOPA study concludes that the current protection layers comprising tank gauging system monitored by operators and independent sensors, and high level alarms with a manual shutdown process are sufficient.

HSL concludes that because the IEs are split into components with the resultant frequencies being multiplied, the IE frequencies are too low. HSL also concludes that Loss of Containment (LOC) of ethanol and kerosene is unlikely to lead to a Buncefield type explosion and that the probability of ignition for kerosene is much lower than that of petrol; although the probability of ignition for ethanol may not be lower than for petrol. Therefore, the most likely scenario is a significant pool fire or flash fire, which could lead to onsite fatalities.

Whilst the manual Emergency Shut Down (ESD) described in this LOPA to prevent tank overfill may appear suitable, a reality check suggests that the unmitigated frequency claimed may be too low. Therefore, HSL concludes that a further detailed verification of the unmitigated event frequency would be needed and should include:

(1) Human error rates appropriate to this site;
(2) In-service reliability of tank gauging system;
(3) Proper inclusion of all elements providing protection including valves and the ship's equipment; and
(4) The reliability of the ship's equipment to stop pumping.

HSE's preference is for SIL-rated independent automatic shut-off systems to be used wherever possible.

It should be noted that while the LOC of kerosene presents a low probability of a Buncefield type explosion, kerosene is considered extremely harmful to aquatic organisms. If, for example, kerosene could find its way into a watercourse, an environmental assessment may result in a more stringent tank overfill prevention system integrity level than that required on safety grounds alone.

3 COMPANY B; LOPA ID 2

3.1 INTRODUCTION

This LOPA [5] considers the level of risk due to a VCE resulting from a tank overfill of a single tank of petrol, based on there being 192 transfers per year from rail cars and pipeline. It is stated in the LOPA that if there is insufficient ullage in the target tank then a second tank may be used.

Tank gauging and overfill protection are provided by an Automatic Tank Gauging (ATG) system and operator response to alarms for each tank. Additionally, a partially independent High Level (HL) alarm and operator response for pipeline fed transfer. This system comprises a separate sensor for each tank, a common Programmable Logic Controller (PLC) and alarms with manual initiation of shut-down. The manual action is that the pipeline vendor, either by means of a signal from the independent high level alarm or by means of a telephone call from the site operator, stops the transfer pump and informs the site so that they can then close the tank import valve.

3.2 RISK TOLERANCE CRITERIA

The risk criterion stated in this LOPA is based on the company's risk acceptance criterion for a catastrophic consequence, which is defined in the LOPA as several onsite deaths or one offsite death. For the overfill of this particular tank, the risk target is stated as being 6 x 10^{-7} per year. This figure is stated as including a factor of 10 reduction to account for all other risks a person is exposed to. The LOPA states that this risk target also allows for the fact that this tank receives 60% of the imported petrol. Therefore, this risk criterion would appear to be reasonable.

3.3 INITIATING EVENTS

Overflow as a result of the following six initiating events is considered:

- Incorrectly calculating the ullage;
- Supervisor fails to divert;
- Supervisor transfers to wrong tank;
- Supervisor diverts to wrong tank;
- Exporter fails to close their export valve; and
- Failure of ATG.

Comments relating to each IE are summarised below.

Table 7 Initiating events assessment and comments

ID	*Initiating Event*	*Value assumed [per year]*	*Comment*
IE 1	Incorrectly calculating the ullage	192 x 0.0480 = 9.22	A HEART analysis was performed to determine the HEP for the operator calculating the ullage in error. The HEART analysis appears to have taken into account the site-specific circumstances and as such would appear to be reasonable. There are 192 tank fill operations per year.
IE 2	Supervisor fails to divert	192 x 0.0038 = 0.73	A HEART analysis states that the HEP for the supervisor fails to divert import to a second tank if there is insufficient ullage in the first tank is estimated at 3.8 per 1000 operations. The HEART analysis appears to have taken into account the site-specific circumstances and as such would appear to be acceptable. There are 192 tank fill operations per year.
IE 3	Supervisor transfers to wrong tank	192 x 0.0037 = 0.71	A HEART analysis states that the HEP for the supervisor transferring to the wrong tank is estimated at 3.7 per 1000 operations. The HEART analysis appears to have taken into account the site-specific circumstances and as such would appear to be acceptable. There are 192 tank fill operations per year.
IE 4	Supervisor diverts to wrong tank	192 x 0.0039 = 0.75	A HEART analysis states that the HEP for the supervisor diverts to the wrong tank is estimated at 3.9 per 1000 operations. The HEART analysis appears to have taken into account site-specific circumstances and as such would appear to be acceptable. There are 192 tank fill operations per year.
IE 5	Exporter fails to close their export valve	192 x 0.0077 x 0.2 = 0.3	Good practice requires that each receiving site must be able to shut down irrespective of supplier controls, it would appear reasonable to include this in the LOPA. There are 192 tank fill operations per year.
IE 6	ATG system failure	192 x 0.000211 = 0.04	A fault tree analysis (FTA) in the LOPA report for ATG and operator failure gives a failure probability of 2.11x10^{-4} per demand. Because the ATG (BPCS) has not been developed in compliance with BS EN 61511[4] a dangerous failure rate of no less than 10^{-5} per hour can be claimed[3]. Therefore, this value is too low.

[3] *To prevent unreasonable claims for the safety integrity of the basic process control system, BS EN 61511 places constraints on the claims that can be made. The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10-5 per hour.*

3.4 CONDITIONAL MODIFIERS

The main issues with this particular LOPA study in relation to the CMs are listed below.

Table 8 Conditional modifier assessment and comments

ID	*Conditional modifier*	*Value assumed*	*Comment*
CM1	Failure to detect overflow	0.019	Failure to detect overflow is a mitigation measure not a conditional modifier. The LOPA states that an operator walks around the site every 2 hours and would see or smell a hydrocarbon (HC) overflow. The PFD of a leak not being detected within 30 minutes is stated as 90/120 = 0.75. The LOPA states that two HC detectors might be installed near the tank, one liquid, one vapour. A PFD of 0.082 per detector is quoted. Overflow not detected by inspection and HC detectors has a PFD of 0.019, using FTA. It should be clearly stated that until the HC detectors are installed and being used, a PFD of no lower than 0.75 can be claimed.
CM2	Probability of ignition	0.09	The LOPA states that if a vapour cloud drifts beyond where hazard area classification limits are, then the probability of ignition becomes more likely and is stated in the LOPA as being 0.9. The LOPA report states that a high-energy ignition source would be required and that only 10% of ignition sources would be sufficient, resulting in an ignition probability of 0.09 being claimed. This assumption is not supported by data or cited literature. Therefore, the probability of ignition of 0.09 is considered to be unrealistically low.
CM3	Probability of personnel being in affected area	1.0	This LOPA states that the probability of someone being within the hazard zone is 1.0, due to control room manning levels and personnel touring the tank farm. This is a reasonable assumption.
CM4	Probability of a fatal injury	0.5	The probability of fatality may already be accounted for in the LOPA's stated risk criterion. If that is the case then this conditional modifier may not be valid. The company bases its probability of fatality on someone being in the control room and being subject to a 600 mbar blast overpressure, which gives a 50% fatality rate. It has failed to account for the personnel it has said will be regularly touring the tank farm and, as such, will be subject to much more than 600 mbar, therefore increasing the chances of fatality considerably. Based on this, a more realistic probability of fatality is likely to be greater than 0.5.
CM5	Likelihood of calm weather	0.461	Probability of calm weather in this geographical location is stated as being 0.461. This is the probability of stable weather with low wind speeds and is taken from the nearest Met Office weather station to the site.

3.5 PROTECTION LAYERS

The following two protection layers have been assumed:

- ATG and operator response to alarms; and
- (Partially) independent high level system with operator response (third party).

These are discussed in the following subsections.

3.5.1 PL1 – ATG alarms and operator response

The following failure probabilities are used:

- ATG PFD is 1.7173 x 10^{-2} according to an in-house component reliability database;
- supervisor fails to notice the incorrect ATG reading during hourly checks is 0.021;
- supervisor fails to act is 0.07822; and
- site to vendor phone fails is 0.000158.

Therefore, the PFD claimed for the ATG, ATG alarms and ATG and supervisor response to alarms, taken from a fault tree, is (0.017173 x 0.021) + 0.07822 + 0.000158 = 0.07874. Because the ATG has not been developed in compliance with BS EN 61511[4] a dangerous failure rate of no less than 10^{-5} per hour can be claimed[4]. Therefore the value is a little on the low side.

With the exception of the 'supervisor fails to notice the incorrect ATG reading during hourly checks', the data presented for PL1 differs from the cited sources in the Appendix of the LOPA; this discrepancy should be clarified.

The ATG failure rate data is taken from an in house database and comprises a level device, PLC logic solver and, readout and the associated cabling. The PLC reliability data used in this LOPA is for a GEM 80 programmable logic controller (PLC), which is different from the PLC used in this system. Other than the level device, it is not clear whether the in-house data used for the rest of the system is generic or based on the actual equipment used. It is also not clear whether the actual site operating conditions have been taken into account. In either case, the ATG PFD would appear to be too optimistic and cannot be claimed according to BS EN 61511, which allows a minimum PFD of 0.1 to be claimed.

Appendix 1 of the LOPA report presents a number of operator tasks that are subject to a HEART analysis. However, these HEPs differ from those used in the LOPA calculation sheet for PL1. Additionally, some HEPs are cited as originating from the BSTG final report example LOPA, instead of the HEART analyses presented in Appendix 1. The BSTG example LOPA values should not be used because they are fictitious and were produced to demonstrate the process of applying LOPA and not to present a realistic set of error probabilities or failure rates.

The supervisor tasks are not stated as being formally written in an auditable procedure and therefore their assessment should be treated with caution.
The detailed analysis used to assign PFDs to the ATG and operator response in this LOPA, although not able to be used directly, supports the minimum PFD allowed to be claimed for the BPCS (ATG).

[4] *To prevent unreasonable claims for the safety integrity of the basic process control system, BS EN 61511 places constraints on the claims that can be made. The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10-^{5} per hour.*

3.5.2 PL 2 – Independent high-high level

PL2 is stated as comprising an independent mechanical high-level float switch, which alarms via a PLC: this PLC appears to be the same as that used by the ATG high-level alarm. The independent high-level switch initiates a manual shutdown. The manual shutdown is performed by the pipeline vendor, either due to a signal from the independent high-level alarm or a telephone call from the site operator, who stops the transfer pump and informs the site so that they can then close the tank import valve.

The shared PLC introduces common cause failure between PL1 and PL2.

A mechanical float device is cited in the LOPA, but the in-house data for a radar-based level device is quoted in Appendix 2 of the LOPA report; this apparent discrepancy should be clarified. The PFD used for the PLC is taken from the in-house database, and is based on the 'Gem 80' PLC, which is not the PLC described in the LOPA. The software used in the PLC has also been given a generic PFD from an unknown source. Therefore, neither the PLC nor PLC software error probabilities can be considered realistic.

3.5.3 PL general comments

- The use of generic failure rate data from failure rate databases should be treated with caution, because even though the data could be for similar equipment, it is likely to have been assessed under different circumstances. Therefore, the generic failure rate may not be applicable to the equipment considered in this LOPA.
- In this LOPA, key component failure rates, such as that quoted for the PLC, appear to have been used in isolation without taking into account the whole system to which they belong. Component failure rates should be combined with other system aspects such as: other system components, cabling, system architecture and operational aspects, as part of a system in-situ analysis to produce a system PFD.
- Error probabilities cited for both PL1 and PL2 appear to differ from the data presented in the LOPA report appendix; these discrepancies should be clarified.
- This LOPA labels the protection layers as independent PLs (IPLs). However, the PLs do not satisfy independence criteria due to shared components. Therefore, they should be referred to as PLs and their error probabilities should also be used or omitted accordingly.

3.6 GENERAL COMMENTS

- This LOPA states that the tolerable risk factor is reduced by a factor of 10 to account for all other risks a person is likely to be exposed to, which appears reasonable.
- The LOPA states that this risk target also allows for the fact that the receiving tank only receives 60% of the imported petrol. This would suggest that the risk target might be slightly conservative.
- Both PLs appear to share common components with the ATG and tank management system. The ATG system failure is claimed as an initiating event. Therefore, for IE6 neither PL1 nor PL2 should be credited in the LOPA without incorporating the

Common Cause Failure (CCF) into the calculations. IE6 and PL1 share the same ATG system, and PL1 and PL2 share the same PLC. Because PL1 and PL2 share the same PLC they fail to meet the LOPA independence criteria. Additionally, because neither PL1 nor PL2 comply with the requirements of BS EN 61511 neither are able to claim a PFD less than 0.1.

- The LOPA does not state whether all elements in the protection loop have been considered, e.g. valves and pumps, etc?
- This LOPA assumes that two hydrocarbon (HC) detectors per tank will be installed; this should be confirmed before credit can be claimed.
- The LOPA incorrectly combines the PFDs of the HC detectors and operator touring the tank farm.
- The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

3.7 LOPA CONCLUSIONS

The LOPA calculations have shown the frequency of mitigated consequence with PL1 is 3.79 x 10^{-4}, leaving a shortfall against the stated risk target of 2.64 x10^{-3} (requiring a SIL2[1] SIF).

Because the PLC software present in the overfill protection system is not certified, the consultant states that this system could not be considered to conform to BS EN 61511[4] and recommends replacement of the current overfill protection system with a Safety Instrumented System (SIS) that complies with the requirements of SIL2 as defined in BS EN 61511.

HSL concludes that if the LOPA data values in the CM's and PLs, used were replaced with more realistic ones the LOPA calculations would give a frequency of mitigated consequence of 8.0 x10^{-3} per year; leaving a shortfall against the stated risk target of 1.25x10^{-4}, which would require a SIL3[1] rated SIS. In general the IE frequencies in this LOPA study appeared higher than in other LOPA studies looked at and it is possible that this LOPA has been overly conservative when assigning HEPs to each IE. Note that, even when a human reliability assessment is performed, such assessments require subjective judgements to be made; a careful analysis of the task being assessed along with the associated performance shaping factors is required to ensure that HEPs are meaningful.

HSL considers that at least a SIL 2 rated overfill protection system would be needed in this case.

4 COMPANY C; LOPA ID 3

4.1 INTRODUCTION

This LOPA [6] covers the import of petrol, DERV, kerosene and gas oil from rail cars. The number of transfers per year is 2 x 27 train cars per weekday plus 1 x 27 train cars on a Saturday. Overall this equates to 1144 train cars per year. Further detail on the rail car offloading method is not described in the LOPA report.

Gauging and overfill protection is provided by an ATG and operator response to alarms. The ATG system is managed by an onsite software package. Additionally, an independent high-level trip via tank-side and pipeline valves automatically stops the transfer. Overfill detection is via routine operator patrols and manual inspection.

4.2 RISK TOLERANCE CRITERIA

The LOPA states that for an extensive VCE, there could be 50 offsite fatalities. This implies that societal risk as well as individual risk should be taken into account. Given that societal risk is considered, then it may be more appropriate to use QRA as the assessment method instead of LOPA.

The potential loss of life (PLL) per year target for the tank overfill hazard was stated as 10^{-5}. No justification for this criterion was given other than it is based on company risk criteria.

4.3 INITIATING EVENTS

Three initiating events are considered in this LOPA, namely:

- Connection to wrong tank by opening the wrong tank-side valve;
- Insufficient ullage; and
- System software providing the operator interface in the ATG fails

Comments relating to each IE are summarised below.

Table 9 Initiating events assessment and comments

ID	*Initiating event*	*Value assumed*	*Comment*
IE1	Connection to wrong tank by opening the wrong valve	0.1 per year	Procedures are in place to check that the correct tank has been connected. This value is not supported by site data or a human reliability study.
IE2	Insufficient ullage	0.033 per year	Procedures are in place to check the ullage. This value is not supported by site data or a human reliability study.
IE3	System software and ATG fails	0.05 per year	The LOPA assumes the ATG failure rate to be 1 in 10 years. The LOPA assumes 50% fail to danger. It is not clear whether this figure includes the ATG hardware, software and operator response. No supporting evidence is presented for this assumption. Two failure modes are considered and it is assumed that both occur with equal probability, which is not supported by data. Because the ATG (BPCS) has not been developed in compliance with BS EN 61511[4] a dangerous failure rate of no less than 10^{-5} per hour, or a PFD of approximately 0.1 can be claimed[5]. Therefore the value is too low.

General comment relating to this IE:

- An IE relating to the operator failing to notice the incorrect ATG reading during hourly checks does not appear to have been considered.
- Time at risk does not appear to have been considered unless it is included in the risk tolerance criteria.

4.4 CONDITIONAL MODIFIERS

- No conditional modifiers are explicitly cited in this LOPA.
- In the tank areas, manual detection of releases is based on routine patrol but no credit is claimed for this task. This may be due to the possible ineffectiveness of manual detection, which relies on there being adequate manning levels at critical stages of the fuel import process.

4.5 PROTECTION LAYERS

The following protection layers have been assumed:

- Operator response to software alarms; and
- Independent high level trip.

[5] To prevent unreasonable claims for the safety integrity of the basic process control system, BS EN 61511 places constraints on the claims that can be made. The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10-^{5} per hour.

These are discussed in the following subsections. Additionally, no credit is claimed for the BPCS (ATG) because the staff who monitor the process are the same staff that set up the process.

4.5.1 PL 1 – Operator response to alarms

The same staff that set up and monitor the process also monitor and respond to the high and high-high alarms. Credit is claimed because alarms provide a second chance to detect and correct errors. An HEP of 0.1 is claimed, although no justification is given for this value.

4.5.2 PL 2 – Independent high level trip

This PL is described as an independent high-level trip via tank-side and pipeline valves. A SIL[6] assessment was performed retrospectively on the existing safety instrumented system (SIS) and deemed to have a PFD of 0.03. The hardwired shutdown logic initiates an ESD of the rail car transfer system by stopping the transfer pumps. The trip logic also sends a signal to a programmable device, which closes the tankside valve thus isolating the tank. It is not clear from the LOPA whether the stated SIL1[1] overfill prevention system includes failures of the programmable device.

4.5.3 PL general comments

- There is a lack of independence between PLs due to a shared PLC.
- A generic database has been used to extract failure data for key devices used in safety related systems assessed as part of this LOPA. These data are likely to be for similar equipment that would have been assessed under different circumstances than those present on this site. The data do not appear to have been modified to account for any site-specific circumstances or the system that they are part of. Therefore, the figures used should be treated with caution.

4.6 GENERAL COMMENTS

- The LOPA is based on the existing PL2 being SIL1[1] rated with a PFD of 0.03. This appears to be a retrospective assessment of an existing system and should be treated with caution because of the known difficulties in retrospectively demonstrating compliance with SILs[6]. Additionally, the logic solver appears to be shared with PL1, which introduces CCF that may not have been taken into consideration.
- The LOPA study considers the assessment of their existing overfill prevention system against the requirements of BS EN 61511. However, a more detailed assessment would

[6] *All BS EN 61511 lifecycle phases are crucial if a safety-instrumented system (SIS) is to achieve compliance with the standard. A safety instrumented function (SIF) should first be determined based on a hazard identification assessment of the process, then a suitable SIS can be designed and implemented. All this must be done in accordance with the requirements of BS EN 61511. Systematic errors as well as hardware reliability issues need to be accounted for in the development of a SIS. With an existing SIS it is likely that sufficient information will not be available to determine whether the SIS was developed using the level of rigour that BS EN 61511 requires for a given SIL, especially if the system contains a programmable element. However, if an existing SIS is a simple hardwired system (BS EN 61511 type A), then a demonstration of the existing SIS architectural construct and reliability together with evidence of proper maintenance and proof testing may be enough to satisfy the requirements of the standard.*

be required before reaching a definitive conclusion. In general, the assessment appears to be reasonable in terms of its consideration of the principles laid out in BS EN 61511, but its handling of shared components lacks clarity.

- The company risk tolerance criteria stated a PLL of 10^{-5} per year is not adequately justified.
- The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

4.7 LOPA CONCLUSIONS

LOPA calculations presented a total PLL of $4.6\text{x}10^{-6}$ per year, which exceeds the stated target of PLL $1\text{x}10^{-5}$ per year; therefore the LOPA calculations suggest no further risk reduction is required.

The LOPA consultant states that the residual risk is still in the 'tolerable if ALARP' region and recommends further remedial actions are performed. The consultant does not recommend an increase in SIL[1] rating for the tank overfill prevention system.

HSL concludes that because the tanks are filled from rail cars, this reduces the risk of a tank overfill event resulting in the spillage of significant amounts of fuel.

HSL notes that the LOPA describes a legacy assessment of PL2 against the requirements of BS EN 61511 for a SIL1 rated SIS. PL2 is described as a hardwired logic based system[6] and is claimed to meet the requirements for a SIL1 SIS as defined in BS EN 61511. Subject to further detailed assessment and on-site verification of the SIL 1 claim, the overfill system described in this LOPA would appear to be adequate.

5 COMPANY D; LOPA ID 4

5.1 INTRODUCTION

This LOPA [7] considers the overfill of fuel storage tanks based on four transfers from ship per year and 20 transfers from pipeline per year of petrol to 10 tanks.

Tank gauging and overfill protection are provided by an ATG system and operator response to the ATG alarms. The ATG alarms are audible in the control room and repeated to the site radio system. The normal fill and high level alarms are linked through the ATG display, then into the tank gauging software system. Fill level and high alarms are audible in the control room and are repeated on through a radio system. A further high-high level alarm is hard wired and is communicated in the same manner across the site. In both cases, transfer is manually stopped.

In the event of a power failure, the transfer is manually stopped because level monitoring on tanks will fail.

5.2 RISK TOLERANCE CRITERIA

A risk tolerance criterion of 10^{-6} has been stated in the LOPA as being for all risks environmental, financial and safety. This risk tolerance criteria description is unclear and may be inappropriate for the following reasons:

- Environmental, financial and safety risks should be assessed separately and relevant criteria applied;
- This LOPA does not state what the risk tolerance criteria are, for example, risk of what, to what and from what;
- It is not clear whether the IR target represents all risks the hypothetical individual person faces on site or just those associated with a single tank and single hazard;
- No justification of the chosen criteria is presented in the LOPA assessment report, although a reference is made to the site COMAH safety report.

5.3 INITIATING EVENTS

Overflow as a result of the following five initiating events are considered:

- Excess fuel on ship;
- Incorrect line-up or changeover;
- Wrong product sent from ship;
- Capacity of tank less than expected; and
- Failure of ATG.

Comments relating to each IE are summarised in the following subsections. Comments are given against the components of the initiating events where relevant.

5.3.1 IE1 – Excess fuel on ship

The initiating event frequency has been calculated based on the following components.

Table 10 Initiating event 1 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	4	Use of frequency of transfers appears appropriate.
2	Third party checks amount of fuel on board ship	0.001	These components seem a little unusual, because it appears to say that there is an excess amount of fuel on the ship (compared with documentation) and the third party incorrectly measures the wrong amount of fuel on the ship, which happens to be the same as that on the incorrect documentation. It appears more plausible that there is an error on the documentation and the third party fails to check the amount of fuel on the ship. It is noted, however, that this may not have a major impact on the calculated IE frequency. These HEPs are taken from BS EN 61511-3 table F.3 [4] without justification.
3	Ship has excess fuel compared with documentation	0.01	
4	Tank operator monitors transfer	0.75	This may be double counting with PL1. This HEP is taken from BS EN 61511-3 table F.3[4] without justification.
5	Tank-side operator monitors level gauge	0.001	There appears to be a possible common cause between this, the previous task and PL1. It is not clear whether this has been taken into account. They all rely on the ATG. This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
6	Probability that a given tank is affected	1/9	If the overfill frequency of a specific tank is being calculated then this factor may be appropriate. However, any tank must have an equal probability of being filled. Also, the risk target would then have to be reduced by the number of tanks, which has not been done.

General comment relating to this IE:

- It is stated that as the import from a ship is a sequential filling operation, then overfill would only occur on the last tank. However, this ignores overfill because of failure to connect to the next tank in the sequence. There is, therefore, a potential to overfill more than one tank on each ship transfer, as the capacity of each tank could be less than the charge from the ship. This does not appear to be taken into account in this IE or elsewhere[7]. Although operators may be less likely to fail to change over from one tank to the next in a sequential filling operation, because there is an expectation that a tank will be approaching its maximum level, the overfill frequency would be greater in that case than for this IE due to components 2 and 3 in the above table then being irrelevant.

[7] *IE2 refers to incorrect changeover. However, the logic appears to refer to changeover to an incorrect tank and not failure to changeover.*

5.3.2 IE2 – Incorrect line-up or changeover

The initiating event frequency has been calculated based on the following components.

Table 11 Initiating event 2 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	24	Use of frequency of transfers appears appropriate.
2	Error in connecting tanks	0.001	It is not clear whether this probability takes account of the number of tanks on the site, as there may be an increased probability of making a mistake if there are more tanks to connect to. It possibly relates to the assumed multiplier used in component 5, for the number of wrong tanks. This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
3	Second operator confirms transfer into correct tank (using ATG in control room)	0.01	This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
4	Probability that overfill caused as tank level is already high	0.85	The basis of this component is not clear. Why should only tanks that are full lead to an overfill event, especially as a ship's load is often greater than a tank's capacity, even when empty? It may be due to the extra time available before an overfill occurs and therefore it is more likely that it can be prevented. Clarification of the assumptions made is required.
5	Number of wrong tanks	9	There are two common scenarios on a site that could lead to the operator lining up the wrong tank. Either an operator is requested to line tank 'X' and knows which tank this is and simply connects to the wrong tank in error; or the operator thinks a different tank, say tank 'Y' is tank 'X' and hence connects to tank 'Y' in error. These scenarios represent different levels of risk. Therefore, the use of this multiplier may not be valid, and each site should perform a task analysis before considering how to handle the number of wrong tanks. The value used in this case would appear to be conservative.

General comments relating to this IE:

- It is not clear why PL1 has been ignored for this initiating event. It may be because of the ATG being claimed as a component in the IE, but no justification is presented in the LOPA report.
- It may be better for incorrect line-up and incorrect changeover to be separated into different IEs because some of the assumptions may need to differ.

5.3.3 IE3 – Wrong product sent from ship

The initiating event frequency has been calculated based on the following components.

Table 12 Initiating event 3 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	24	Use of frequency of transfer appears appropriate.
2	Operator selects incorrect manifold line	0.001	This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
3	Sampling of product during transfer	0.001	This HEP is taken from BS EN 61511-3 table F.3 [4] without justification.
4	Overfill due to cross connection of diesel and petrol at the ship	0.5	This only becomes an issue if quantities of diesel are greater than petrol. If quantities of diesel are not greater than petrol, this IE is invalid.

General comments relating to this IE:

- IE3 may not be valid. If the quantity of diesel and petrol on ship are similar then sending the wrong product would not increase the probability of a tank overfill event.
- It is not clear why some of the components in the first initiating event have not been considered here, because the latter events should be the same. There appears to be an issue with consistency between the different IEs.

5.3.4 IE4 – Capacity of tank less than expected

The initiating event frequency has been calculated based on the following components.

Table 13 Initiating event 4 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Number of transfers per year	24	Use of frequency of transfers appears appropriate.
2	Error in dipping tank by third party (also checks ATG)	0.001	These HEPs are taken from BS EN 61511-3 table F.3 [4] without justification. Potential for common cause failure may not have been adequately taken into account because both components rely on the ATG. However, given the other checks, this may not be a significant issue.
3	Operator confirms level from ATG, checks ullage available and calculates batch fill level	0.001	

General comment relating to this IE:

- PL1 has been ignored in this case. This would appear sensible given that the ATG is part of the IE components.

5.3.5 IE5 – Failure of ATG

The initiating event frequency has been calculated based on the following components:

Table 14 Initiating event 5 assessment and comments

ID	*Component of IE calculation*	*Value assumed*	*Comment*
1	Failure of ATG	0.1 per year	This value appears to be based on the minimum allowed in BS EN 61511[4] for a non-SIL[3] related system (10^{-5} dangerous failures per hour, which equates to approximately to 0.1 per year). The ATG failure rate is not supported by evidence and as such should be treated with caution.
2	Tank being filled	0.004	Consideration of the proportion of time a tank is being filled is accepted as common, although not universal, practice. It may be that the number of tank fill operations per year is more appropriate, rather than the time spent filling the tank because this more accurately reflects the number of potential demands being made on the protection layers.
3	Operator fails to detect ATG failure	0.1	It is not clear whether this HEP has already been included in IE5 component 1. If it has not, then it should be combined with component 1, possibly, in the same way that the ATG hardware PFD and operator failure HEP have been combined in PL1, resulting in an ATG dangerous failure rate of no less than 0.1[3] per year as required by BS EN 61511 [4].

General comments relating to this IE:

- PL1 has been ignored in this case. This would appear sensible given that failure of the ATG is considered within the IE.

5.3.6 General comments

- There is no justification for the IEs that have been chosen and there is no description of the process used for identification of the IEs. Therefore, it is difficult to be confident in whether there are any significant gaps.
- Values assumed are generally not justified. For example, reference is just made to BS EN 61511 for human error probabilities. These should be estimated taking account of the specific features of the site and operation. In addition, some of the values assumed appear to be on the low side, such that once combined are leading to very small IE frequencies.

5.4 CONDITIONAL MODIFIERS

The main issues with this particular LOPA study in relation to the CMs are listed below.

Table 15 Conditional modifier assessment and comments

ID	*Conditional modifier*	*Value assumed*	*Comment*
CM1	Probability of failure to detect overflow	0.9	This would seem to be a protection layer rather than a conditional modifier because it refers to a specific action performed by an operator to detect and prevent further loss of containment. It is unclear whether the operators who are expected to detect and take action are independent of those already considered.
CM2	Probability of ignition	0.4	This could be too low given the very large release event that is being considered.
CM3	Probability of personnel being in affected area	0.1	It is not clear how large the affected area has been assumed to be. Based on the Buncefield damage, a radius of 250-300 metres around the tank needs to be considered. Therefore, this probability is too low.
CM4	Probability of a fatal injury	1.0	The probability of fatality may already be accounted for in the LOPAs stated risk criterion. If that is the case then this conditional modifier may not be valid. The assumption that an operator within the hazard zone of a VCE would suffer a fatal injury is reasonable.

General comments on the CMs listed here are:

- It is not clear whether the probability of a VCE is implicitly assumed in the probability of ignition. If it is included, it would be clearer if this was separated out;
- Given that a Buncefield VCE is being considered, the probability of calm weather should be included. However, if it has been included within the ‘probability of ignition’ CM, it should be explicitly stated in the LOPA report; and
- The assumed probabilities are not justified.

5.5 PROTECTION LAYERS

The following protection layers have been assumed:

- High level ATG alarm and operator response; and
- Hard-wired high-high level alarm and operator response.

These are discussed in the following subsections.

5.5.1 PL1 – High level ATG alarm

The assumed probability of failure (0.19) of this PL may be reasonable as a minimum value. It is assumed that the PFD of the hardware is 0.1 and the PFD of the operator to respond appropriately is 0.1. The overall failure of the protection layer is assumed to be the PFD of the hardware combined using the logical 'OR' operator with the HEP of the operator. However, both the ATG PFD and operator HEP are not supported by evidence.

5.5.2 PL2 – Hard-wired high-high level alarm

The high-high level alarm is hard-wired to the control room annunciator and relays the alarm via radio transmission to the jetty operator. Initially it is assumed that the PFD of this system is 0.19 (as above the overall failure of the protection layer is assumed to be the PFD of the hardware OR PFD of the operator). Because the operator cited in this PL is required to act for PL1 and IE5, there is the potential for common cause failure. Therefore, this protection layer cannot be classed as independent for IE5.

5.5.3 PL general comments

- A significant issue with the protection layers is that there is insufficient justification for the assumed PFDs.
- In addition, the first PL has been discounted for some of the initiating events. Where the ATG is considered as part of the IE, this would be appropriate. However, there is no justification for whether this PL should be included in a specific IE, and its inclusion or omission does not appear intuitive in all cases.
- The LOPA study does not state the reliability of the equipment involved in each PL loop and therefore it is not clear whether all relevant equipment in each protection loop has been included in the PFDs quoted, e.g. valves, telephone link to ship, ships shut-off system for pumps, etc.

5.6 GENERAL COMMENTS

The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

5.7 LOPA CONCLUSIONS

The LOPA calculations showed a shortfall against the risk target of 0.076, which would require a SIL1[1], as defined in BS EN 61511, SIS to meet the stated risk target.

The LOPA recommended revising PL2 to provide an automatic overfill prevention system with a PFD of $5.0x10^{-3}$, which equates to a mid range SIL2 as defined in BS EN 61511 [4].

It is not certain why the consultant recommended a SIL2[1] shut off system when the LOPA calculations suggested that a SIL1 system was required. It is assumed that data uncertainty and application of the ALARP principle could be factors that influenced the consultant's recommendation.

HSL concludes that given the uncertainties in the data and modelling used in the LOPA calculations, the recommendation to implement a SIL2 SIS would appear reasonable.

6 COMPANY E; LOPA ID 5

6.1 INTRODUCTION

This LOPA [8] considers the risk of petrol tank overfill due to onsite petrol blending operations. The LOPA states that, based on site data from the past two years, there are 960 transfers between tanks per year. The scope of this study is limited to the 11 floating roof tanks, which hold finished petrol.

Tank gauging and overfill protection are provided by an ATG system, which has normal fill and high alarms that are sent to a SCADA system. Critical alarms are audible in the site control room, where the control operator responds to them by closing the relevant inlet valves. An independent high-level switch will also sound a critical high-high level alarm that the control room operator responds to by closing the tank inlet valves.

6.2 RISK TOLERANCE CRITERIA

The LOPA states "a frequency of greater than 1 x 10^{-6} per year but less than 1 x 10^{-3} per year can be considered as tolerable if the risk is as low as reasonably practicable (ALARP)." The risk is of a tank overfill of petrol during blending operations, which require tank-to-tank transfers.

It is not clear whether the IR target stated represents all risks the hypothetical individual person faces on site or just those associated with a single tank and single hazard.

6.3 INITIATING EVENTS

Overflow as a result of the following three initiating events are considered:

- Incorrect valve selected;
- Incorrect ullage calculation; and
- Failure of level indicator.

Comments relating to each IE are summarised in the following subsections. Comments are given against the components of the initiating events where relevant.

6.3.1 IE1 – Incorrect valve selection leads to tank overfill

The initiating event frequency has been calculated based on the following components.

Table 16 Initiating event 1 assessment and comments

ID	*Initiating event component*	*Value assumed*	*Comment*
1	Number of transfers per year	960	This is based on extrapolation from one month's recorded data. It should be stated whether this is a representative figure.
2	Valve misalignment rate	0.76	This is based on the number of misalignment failures recorded in a two-year period and the number of transfers per year related to the oil blending process. The frequency of tank valve misalignment due to incorrect valve selection is stated as 0.76 per year, which, if based on site data is reasonable.
3	Probability of target tank having insufficient ullage	0.5	The basis for this probability is not clear; it appears to suggest that the target tank ullage is unknown. Additionally, why should only tanks that are full lead to an overfill event, especially when the supply more than a single tank can hold. This may be due to the extra time before an overfill occurs and therefore it is more likely that it can be prevented. Clarification of the basis of this probability is required.

6.3.2 IE2 – Incorrect ullage calculation

The initiating event frequency has been calculated based on the following components.

Table 17 Initiating event 2 assessment and comments

ID	*Initiating event component*	*Value assumed*	*Comment*
1	Operator enters tank dip level in software system used to calculate ullage and warning given if ullage is insufficient	0.001	The LOPA states that an error would occur if the scheduler entered an erroneously low level for the recipient tank. However, the tank gauging software is stated as performing a cross check of volumes and a warning is given if there is insufficient ullage. Therefore, this HEP appears to represent operator error in entering an incorrect tank level resulting in an incorrect ullage. Without a human error analysis being performed; it is difficult to determine whether this value is realistic. Additionally, the tank gauging software appears to be spreadsheet based, which leads to a possibility of errors associated with the unintended alteration of the spreadsheet calculations and possibly invalidated spreadsheet calculations. This error probability may be too low and is not supported by data.
2	Based on 16 petrol blends in December 2006	192 per year	IE2 states that there are 192 transfers per year. However, IE1 states that there are 960 transfers per year. The LOPA report states that there are typically 5 transfers per blending operation and this factor of 5 would appear to account for the difference between the numbers of transfers stated in IE1 and IE2. It would appear logical to use 960 transfers per year, which is the actual number of transfers per year rather than the 192 blending operations per year. However, this should be clarified and the relevant IE amended accordingly.

6.3.3 IE3 – Failure of tank level indicator

The initiating event frequency has been calculated based on the following components:

Table 18 Initiating event 3 assessment and comments

ID	*Initiating event component*	*Value assumed*	*Comment*
1	Radar level device failure rate	8.9 x 10^{-3} per year	The failure frequency (λ_d) is 1 / 112 or 8.9 x 10^{-3} per year. It is not clear whether the quoted mean time between failure (MTBF) is for the complete level detection system (comprising level detector, transmission elements and level indicator, and everything in between) or whether this is just the manufacturer's MTBF for the level device, which for radar devices will always be the most reliable component in the system. The latter is more likely; otherwise, this figure would appear to be too low.
2	Radar level devicePFD	3.7 x 10^{-4}	Average probability of failure on demand (PFD) can be expressed as ½Tλ_d. The LOPA report states that the test period is one year, T=1; however, in the calculation performed a test interval of 1 month is used, T =1/12. If T=1 is used the value assumed would be 4.5x10^{-3}. Hence, either the written test frequency is wrong or the numerical test frequency used in the calculation is wrong. The level device forms part of the BPCS (ATG) and as such a dangerous failure rate of no less than 0.1 per year can be claimed as per the requirements of BS EN 61511.

6.4 CONDITIONAL MODIFIERS

The main issue with this particular LOPA study in relation to the CMs are listed below.

Table 19 Conditional modifier assessment and comments

ID	*Conditional Modifier*	*Value assumed*	*Comment*
CM1	Probability of ignition	0.08	The LOPA states, "Cox et al [9] presents a review of onshore and offshore ignition data and suggest a simple ignition model based on mass release rate. For a potential leak rate of 100 kg/s (500 m^3/hr) the ignition probability is 0.08." The probability of ignition described by Cox et al [9] is for an offshore "blow-out" scenario, which is different from a Buncefield-type explosion. In Lees [10], Kletz states that the vapour cloud ignition probability increases with the size of the release, suggesting a probability of up to 0.5. Again, this was before the Buncefield event and could now be considered low. Therefore, a probability of ignition of 0.08 is extremely low and is considered to be unrealistic. Although the Buncefield explosion mechanism is not yet fully understood, it is generally accepted that a sufficiently large vapour cloud that drifts under suitable weather conditions will probably find an ignition source.
CM2	Probability of personnel being in affected area	0.05	The figure of 0.05 appears to be an unjustified estimate. It is not clear how large the affected area has been assumed to be. Based on the Buncefield damage, a radius of 250-300 metres around the tank bund needs to be considered. It is therefore suggested that this figure is too low.

General comments relating to these CMs include:

- The values used appear too low and are not justified;
- Unrealistic assumptions appear to have been made regarding the manning levels and the blast area covered; and
- Given that a Buncefield VCE is being considered, the probability of calm weather should be included. However, if it has been included within the 'probability of ignition' CM, it should be explicitly stated in the LOPA report.

6.5 PROTECTION LAYERS

The following protection layers have been assumed:

- Operator response to ATG alarms; and
- Operator response to independent high-high alarm.

These are discussed in the following subsections.

6.5.1 PL1 – Operator response to alarms

A HEP of 0.1 is taken from BS EN 61511-3 [4] with no justification given. Operator response to alarms should not be considered in isolation as a protection layer. PL1 should include the ATG and operator response to the ATG alarms. A PFD of no less than 0.1 can be claimed[8] because the ATG does not conform to the requirements of BS EN 61511.

6.5.2 PL2 – Independent high-high level alarm

The tank high-high level alarms are based on a float / displacer tank level device. The stated generic failure frequency (λ_d) for this type of device is 19.3×10^{-6} per hour or 1.7×10^{-1} per year. Therefore, with a test interval of 1 year, the PFD $= \frac{1}{2} \times 1 \times 1.7 \times 10^{-1} = 8.5 \times 10^{-2}$. However, the float device should not be considered in isolation. The whole system should be considered, including the alarms and the cabling, not just the level device, hence this figure would appear to be too low. PL2 is non-SIL[3] rated and as such a PFD of less than 0.1 cannot be claimed.

6.5.3 PL general comments

- The high-high alarm system PFD should be calculated based on all system components, their architecture and operation, not just the main component failure rate and test frequencies.
- It would appear that the same operator responds to both the ATG alarm and the independent HHL alarm, thus the operator represents a CCF, which should result in either PL1 or PL2 being discounted.

6.6 GENERAL COMMENTS

- The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

6.7 LOPA CONCLUSIONS

The LOPA calculations showed a shortfall against the risk target of 3×10^{-3}, which would require a SIL2[1], as defined in BS EN 61511, SIS to meet the stated risk target.

The LOPA proposes a number of possible solutions to reduce the event frequency to within the broadly acceptable range including:

- Reduce the frequency of valve misalignment by identification of valves and confirmation of transfer routes. This initiating event is a major contributor to the risk from overfills of the finished petrol tanks;
- Relay the tank high level alarm to another fully manned location to reduce the probability of failure to respond to a high level;
- Install a SIL2[1] SIS that is independent of all other protection layers with the specific function of preventing overfilling of the finished petrol tanks. The proposed SIS would

[8] *To prevent unreasonable claims for the safety integrity of the basic process control system, BS EN 61511 places constraints on the claims that can be made. The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10-5 per hour.*

involve the addition of an automatic shut off valves associated with an independent HH level switch.

HSL concludes that there are a number of inconsistencies in the data values that, if corrected, would likely result in an increase by an order of magnitude in the amount of required risk reduction.

HSL also concludes that the most important of the measures proposed in the LOPA to help meet the required individual risk target is therefore likely to be the installation of a SIL2[1] rated SIS.

7 COMPANY F; LOPA ID 6

7.1 INTRODUCTION

This LOPA [11] assesses the import of kerosene to site via pipeline to an unspecified number of tanks; although experience of similar sites suggests that there will be several tanks available for import of kerosene. It is assumed that import to a single tank at a time is being assessed and that there are 50 import operations per year. These assumptions are based on the limited comments supplied with the LOPA front sheet.

Tank gauging and overfill protection are provided by an ATG system and operator response to the ATG alarms. The import Motor Operated Valves (MOV) are closed by the operator from the control room. This LOPA does not describe in sufficient detail the method of providing tank-overfilling prevention.

7.2 LOPA RISK TOLERANCE CRITERIA

This LOPA uses $3x10^{-5}$ as a Mitigated Event Likelihood, which appears to be the risk criteria associated with 1 to 10 persons being killed, taken from the company guidance. The LOPA summary sheet impact event (IE description) clearly states that a consequence of a single fatality is being considered. Therefore, a target reflecting the broadly acceptable region of the Tolerability of Risk (TOR) framework, i.e. an individual risk target of $1x10^{-6}$, may be more appropriate, provided that due consideration is taken of the fact that this is an ‘all plant, all event’ risk target and that this LOPA is only considering a tank overfill event, i.e. a single hazard.

7.3 INITIATING EVENTS

Overflow as a result of the following five initiating events are considered:

- ATG measurement fails to danger;
- Operator fails to close MOV;
- MOV fails to close;
- Incorrect line-up; and
- Incorrect ullage calculations.

Comments relating to each IE are summarised below.

Table 20 Initiating events assessment and comments

ID	*Initiating event*	*Value assumed*	*Comment*
IE1	ATG measurement fails to danger	0.1 per year	This value appears to be calculated based on the minimum allowed in BS EN 61511 for a non-SIL[3] related system (10^{-5} dangerous failures per hour, which is equivalent to 0.1 dangerous failures per year). No supporting evidence is presented for this claim.
IE2	Operator does not close MOV	0.04 per year	This HEP is taken from IEC-61511 Part 3 Page 48 Table F4, “human error resulting in material release”. No supporting evidence is presented for this claim.
IE3	MOV valve fails to close	0.011	This PFD is based on the MOV failing to move, and is taken from the CCPS LOPA book [11], Paragraph 3.5.3.2, which states that a generic MOV PFD is $1.1\text{x}10^{-2}$. The LOPA notes state that this is a PFD; therefore, it needs to be multiplied by the demand rate to give an annual frequency. If there is a delivery every 3 days (based on comment 7 in the LOPA), the demand rate would be approximately 122 (per year) and the initiating event frequency would be approximately 1.3 per year (122 x 0.011).
IE4	Incorrect line-up	0.04 per year	This HEP is taken from IEC-61511 Part 3 Page 48 Table F4, “human error resulting in material release”. No supporting evidence is presented for this claim.
IE5	Incorrect ullage calculations	0.04 per year	This HEP is taken from IEC-61511 Part 3 Page 48 Table F4, “human error resulting in material release”. No supporting evidence is presented for this claim.

7.3.1 General comments

- This LOPA does not appear to consider the operator failing to correctly perform or interpret tank dip measurements.
- The initiating event ‘operator fails to divert’ to the next tank does not appear to have been considered.
- Initiating event frequencies appear to have been taken from BS EN 61511[4] with little justification. For example, the BPCS failure rate is taken from BA EN-61511 (Part 1, Page 40, Section 9.4), and the human error resulting in material release is taken from IEC-61511 (Part 3, Page 48, Table F4).

7.4 CONDITIONAL MODIFIERS

The main issues with this particular LOPA study in relation to the CMs are listed below.

Table 21 Conditional modifier assessment and comments

ID	*Conditional modifier*	*Value assumed*	*Comment*
CM1	Time at risk	0.43	It is reasonable to consider time at risk in a LOPA and the percentage of time that a tank is being filled is an acceptable method for representing time at risk in some circumstances. However, to have a single time at risk CM may not be valid if the time at risk is already accounted for elseware in the LOPA, for example, in the risk tolerance criteria. Additionally, for some IEs in this LOPA, the number of transfers per year may have been a better measure of time at risk.
CM2	Probability of ignition	0.03	According to an HSL fire and explosion expert this would appear to be within an acceptable range for kerosene.
CM3	Probability of personnel being in affected area	0.1	Probability of a person being in the bund is stated as being 0.1. This is likely to be reasonable for a pool fire scenario.
CM4	Probability of a fatal injury	0.5	The probability of fatality may already be accounted for in the LOPAs stated risk criterion. If that is the case then this conditional modifier may not be valid. This CM appears to have been accounted for in CM3, therefore, the probability of fatality is likely to tend towards 1.0. Additionally, the probability may have been accounted for in the risk tolerance criteria.

7.5 PROTECTION LAYERS

7.5.1 PL1 – BPCS, alarms and operator action

The company ‘F’ LOPA summary sheet claims BPCS, alarms and operator response as a PL with a PFD of 0.1. The LOPA should state explicitly what part of the BPCS is being claimed as a PL. The ATG failure has already been counted in IE1.

7.5.2 PL general comments

- It would be helpful if the PFD of the BPCS and alarms were separated from that of the operator response in order to justify the values used, because the BPCS measurement ‘fails to danger’ has already been claimed in IE1.

7.6 GENERAL COMMENTS

- Values have been taken from BS EN 61511-3 [4], table F.3, without justification or supporting evidence.
- The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

7.7 LOPA CONCLUSIONS

The LOPA calculations present a shortfall of 0.216 against the company risk target. If this figure were correct then it would suggest that no further risk reduction would be required. However, factors such as data uncertainty highlighted in this LOPA and the ALARP principle should always be taken into account as well as the LOPA results.

Company ‘F’ only supplied an annotated spreadsheet showing the LOPA calculations, hence there was no supplementary documentation or detailed explanatory text. The company did not recommend the addition of further risk reduction measures.

HSL concludes that there are a number issues in the company ‘F’ LOPA that, even if addressed, would result in a SIL1[1] or higher SIS being required to meet risk targets.

A number of possible errors have been identified in the company ‘F’ LOPA, the correction of which, could lead to the requirement for a SIL1[1] or higher system being required for the jet fuel tank overfill scenario. However, a lack of information regarding the nature of the existing protection system and about the process in general has made it difficult to draw firm conclusions.

HSE colleagues have stated that the company have now decided to implement a SIL2 SIS as defined in BS EN 61511.

8 COMPANY G; LOPA ID 7

8.1 INTRODUCTION

This LOPA [13] covers overfill of two tanks storing a flammable substance, with properties similar to those of petrol. The tanks are filled from a main processing plant via a pipeline.

Tank gauging and overfill protection are provided by an ATG and operator response; the operator is able to initiate a manually ESD from the control room. Magnetically coupled float switches are used to initiate automatic closure of relevant plant valves. Loss of level signal, plant control valve signal or loss of air automatically closes the relevant plant valves.

8.2 RISK TOLERANCE CRITERIA

Company G has not explicitly stated its risk criteria, although it does refer to applying the ALARP principle. They remark that their mitigated frequency approaches the broadly acceptable level. This could imply that their individual risk of fatality target could be close to $1x10^{-6}$ per year.

8.3 INITIATING EVENTS

Comments relating to each initiating event are summarised below.

Table 22 Initiating events assessment and comments

ID	*Initiating event*	*Value assumed*	*Comment*
IE1	Operator failure to monitor tank contents	0.05 per year	The LOPA report states that this value is chosen because “Operator not considered being under stress”. However, this figure appears to be low and is not supported by evidence and should be treated with caution.
IE2	Failure of level instrument	0.2 per year	A hydrostatic transmitter failure rate is stated with no justification. Use of the device failure rate in isolation of the complete loop is not acceptable. However, the value stated appears to be plausible.
IE3	ATG failure	0.5 per year	The ATG system is stated as providing tank level and high-level alarm displays, and tracking of the failure logic, which tracks the valve closures that have been initiated by the trip logic. The failure rate from all causes is stated as 5 per year with a dangerous failure fraction of 0.1. The dangerous failure fraction is not defined and the value of 0.1 is not justified. It is not clear whether the claimed ATG failure rate is the dangerous failure rate. Regardless of this, the value used appears to be overly cautious.
IE4	Inlet valve failure	0.2 per year	Two tanks are filled from a single pipeline from the plant.

	A selection switch is used to choose only one tank. It is possible that the unselected valve may be (partially) open due to spindle or seal failure. This valve failure could result in the substance being pumped into the wrong tank. The MTBF for this type of valve is stated as being 5 years, which leads to an estimated failure rate of 0.2 per year. This failure rate is not supported by data, i.e. it is not stated how many failures, if any, have occurred since the valve was installed. However, the value stated appears to be plausible.

8.3.1 General comments

- The frequencies are too low and are not sufficiently justified.
- Possibly unrealistic claims are made for the ATG reliability.

8.4 CONDITIONAL MODIFIERS

The main issues with this particular LOPA study in relation to the CMs are discussed below.

Table 23 Conditional modifier assessment and comments

ID	*Conditional modifier*	*Value assumed*	*Comment*
CM1	Probability of ignition	0.4	It may be possible that the probability of ignition is already covered in the risk tolerance criteria; this should be clarified in the LOPA report. Area classification zones are cited as a reason for the cited probability of ignition. Protection from ignition sources is only effective within the hazard zones, which typically extend to a several metres from the relevant tanks and valves. Whilst this may positively impact on the flash fire scenario, it will have little impact on in Buncefield type scenario. Tanks are stated as being remote from plant areas but close to other tanks containing flammable liquids. Therefore, further justification of the cited value should be presented.
CM2	Probability of personnel being in affected area	1.0	The probability of an operator being in the hazard zone is stated as low due to remote operation. However, the LOPA assumes one person could be injured due to fire and therefore this value seems reasonable.
CM3	Staff training and familiarisation	0.2	It is not appropriate to claim credit for staff training in a LOPA [11]. It is suggested that this CM should be removed.
CM4	Site fire alarm and emergency procedures	0.5	It is not appropriate to claim credit for fire alarm and emergency response in a LOPA [11]. It is suggested that this CM should be removed.

8.5 PROTECTION LAYERS

The following protection layers have been assumed:

- Manual ESD;
- ATG Alarms and operator response; and
- Valve trip.

These are discussed in the following subsections.

8.5.1 PL1 – Manual ESD

Manual ESD is available in the control room only and not at the tank. The PFD of 0.4 is not justified by any data or analysis. It should be made clear whether this probability is for the ESD hardware failure, operator error in failing to initiate the ESD, or both.

8.5.2 PL2 – ATG Alarms

Credit for the failure of the ATG has already been claimed in IE3; failure of the tank level device has also been claimed in IE2, furthermore, operator monitoring of the tank level has already been claimed in IE1. Failure of the ATG would result in failure of ATG alarms and it is therefore not clear in this example how credit can be claimed for the ATG alarms as a protection layer. However, putting aside the issue of double counting, the probability assumed for failure of the ATG alarm appears to be for operator response to the alarm and although the PFD of 0.3 is not justified, it would appear a reasonable value if the operator has no other tasks to do at this time.

8.5.3 PL3 – Valve trip

Magnetically coupled float switches are used to initiate closure of plant valves. Loss of level signal, plant control valve signal, or loss of air causes the two plant valves to be closed automatically. Although the valve trip system has no supporting failure data, the PFD of 0.42 claimed appears to be plausible.

8.5.4 PL general comments

- The protection layers appeared to have too many common components to be effective.
- The LOPA study does not account for the reliability of equipment other than the float switches in PL3, e.g. trip amplifiers and valves.

8.6 GENERAL COMMENTS

- The inclusion of staff training and emergency planning factors are not usually considered as valid CMs, and as such may not be appropriate.
- The conclusions drawn from a LOPA study will be sensitive to all the input assumptions. Therefore, some form of sensitivity study is required to demonstrate the robustness of any conclusions. This does not appear to have been carried out.

8.7 LOPA CONCLUSIONS

The company G LOPA states that the measures proposed will bring the mitigated frequency down to 4.8x10^{-5} per year, which the company claim to be approaching the broadly acceptable level. Calculations based on the data supplied in the LOPA study suggest that a SIL 3 would bring the IR to the broadly acceptable level. However, some values used appear to be over conservative.

The LOPA recommends that an overfill prevention SIS rated at SIL2 as defined by BS EN 61511, should be fitted. HSL concluded that after consideration of the data uncertainties in this LOPA the addition of a SIL2 SIS would appear to be reasonable.

9 MAIN FINDINGS

The majority of LOPA studies assessed were for petrol import, however, some were for kerosene and other flammable liquids such as ethanol.

The majority of substance transfers were from ship or pipeline, with one exception being from railcar and another being tank-to-tank transfers and another being direct from a process on site.

A number of inconsistencies in the way LOPA studies were performed have been identified.

HSE colleagues have stated that a number of companies have plans to implement SIL[1] rated systems to prevent tank overfill that are compliant with BS EN 61511[4].

9.1 GENERAL TRENDS

Out of the 15 LOPA studies assessed in this work, 11 comprised an ATG high level alarm and operator response PL, and an independent high-high level alarm plus operator response PL. Four sites comprised an ATG high level alarm and operator response PL, and a PL comprising high-high level trip system to automatically close the import valve.

None of the tank overfill prevention systems described within the LOPA studies assessed as part of this work were claimed to be compliant with BS EN 61511 [4]. Although one LOPA study (LOPA ID 6) described their assessment of an existing hardwired, legacy, tank overfill prevention system, against the requirements of BS EN 61511 [4].

The recommendations of 11 LOPA reports suggested either replacing their existing independent HHL alarm system with a SIL rated SIS[1] or adding a new SIL rated SIS, typically incorporating the automatic closure of the import valve. In general the LOPAs did not cite difficulties in automatically closing the import valve when transferring fuel from a ship, although in reality this may be an issue requiring careful consideration.

Three LOPAs claimed that their risk target was met by their existing systems: this included both LOPAs that assessed the transfer of kerosene, and the LOPA that claimed SIL1 for it's existing automated shutdown system.

9.2 INITIATING EVENTS

The most common issue encountered in all of the 15 LOPA studies considered as part of this work was the reliance on data taken from tables in BS EN 61511 [4] without sufficient justification. These values are only suggested ranges and should be justified beyond the brief explanatory text that often came with them. This appears particularly relevant to human error probabilities (HEPs), where site-specific factors, which may vary widely, can have a significant effect. Some LOPAs included human reliability studies using the Human Error Assessment and Reduction Technique (HEART) method. If an appropriate human reliability method is selected and properly applied to provide a systematic assessment, then the inclusion of HEPs in a LOPA can add to the understanding of risk and is to be encouraged.

None of the 15 LOPAs considered in this study described the methods used for identifying, and hence including in the LOPA, all relevant IEs. Therefore, it is not possible to determine whether all the relevant IEs for each LOPA have been considered.

Several of the LOPA studies assigned non-SIL[3] rated systems a PFD of less than 0.1 when considering their alarm or trip functions in PLs, or a dangerous failure rate of less than 1x10^{-5} per hour when considering tank level detection aspects as an IE. Even if a detailed QRA produces a PFD or dangerous failure rate lower than that allowed to be claimed for a non-SIL rated system, this does not change what can be claimed according to BS EN 61511 [4].

For example, ATG failure is often cited as occurring 1x10^{-5} per hour, which is approximately 0.1 per year, without any justification or supporting evidence.

In several LOPAs, the initiating events have been broken down into a number of components, which are assumed to be independent, without apparently considering their logical dependencies. This can lead to very low initiating event frequencies.

Some IEs would be better split into separate IEs. An example of this is the commonly cited IE ‘Incorrect line-up or changeover’. These appear to be two distinctly different tasks requiring different actions to be performed.

A problem with many of the LOPAs assessed as part of this work is that the task and process descriptions are not sufficiently detailed. This makes it difficult to assess the data used and assumptions made.

There appear to be inconsistencies in how the ATG system for a tank is treated in some of the LOPAs considered in this work. The ATG is accounted for in IEs or PLs, or both. ATG functions such as monitoring of tank levels were typically cited as IEs. However, in one LOPA they were double-counted as both an IE and PL. ATG high-level alarms and operator response to those alarms were usually cited as a PL. Keeping this functionality separate while taking into account their physical associations is important when determining what credit to apportion to the ATG as an IE and PL.

Many of the LOPA studies failed to show independence between protection layers (PLs). Often, it appeared that the same level device or PLC were common between PLs. It appears to be common practice for operators who are expected to perform operational tasks to have to respond to high-level alarms. Hence, care should be taken when crediting operator response to alarms.

Two LOPAs have cited generic component failure data from standard databases to determine tank protection system PFDs used in PLs or ATG failure frequencies used in IEs. It is likely that these data were for similar but different equipment to that used on site. The values used have not been modified to account for any site-specific circumstances or the system that they are part of. Therefore, the figures used should be treated with caution.

When considering IEs that require an operator to select the correct valve for the import of petrol, many LOPAs have assigned this task a HEP. However, in the same IE, use of the number of possible wrong tanks as a multiplier may not be appropriate and requires justification.

The tank level instrument, which forms part of either the ATG system, a high-level alarm/trip system, or both, is often incorrectly considered in isolation.

9.3 CONDITIONAL MODIFIERS

There were only a limited number of different CMs cited in the 15 LOPAs considered as part of this work. The most common were failure to detect overflow, probability of ignition, probability of personnel being in an affected area, and probability of a fatal injury. Although the scenario being considered is a Buncefield-like event, only one LOPA from company B [5] explicitly stated a conditional modifier relating to still weather conditions. If calm weather conditions are included within any other CM, such as the ‘probability of ignition’, this should be explicitly stated in the LOPA.

A general comment in relation to the CMs is that the assumed probabilities were not justified and tended to be lower than expected.

There appears to be double-counting between conditional modifiers. For example, the CM ‘person being in the affected area’ often cites low manning levels to justify a low error probability. The same low manning levels are also counted in the ‘probability of fatality’ CM and indirectly in the ‘probability of detecting an overfill’ CM. Low manning levels cannot be counted more than once. Double-counting in CMs can have a significant impact on the conclusions drawn from a LOPA.

The majority of the LOPAs do not appear to properly account for the affected area associated with a Buncefield-type VCE, which may increase the probability of someone being in the affected area.

9.4 PROTECTION LAYERS

ATG hardware PFDs and operator response to alarm HEPs are usually given a value of 0.1, which is taken from BS EN 61511-3 [4] without justification, and is not supported by evidence.

Many LOPA studies did not state whether the claimed PFD for their ATG and operator response PLs included reliability data for the associated valves and pumps.

Many of the LOPA studies failed to show independence between PLs. Often it appears that the same level device or PLC are common to more than one PL. There appears to be inconsistency between the different LOPAs regarding when credit is given in these circumstances.

High-high level alarms with manual closure of tank isolation or import valves are often cited as a PL. However, the PFD of the valve does not appear to have been considered.

Those LOPA studies that considered transfer of petrol from a ship did not account for the reliability of equipment on the ship or communication equipment, e.g. ship pumps and valves, and radios.

9.5 RISK TOLERANCE CRITERIA

Many of the LOPAs studied in this work stated explicitly or implicitly (by stating that the TOR framework and ALARP principle were used) that an individual risk target of $1x10^{-6}$ per year was used to determine the required risk reduction. In the majority of LOPAs considered, it is stated that the risk target of $1x10^{-6}$ is taken for all risks. It was not clear what was meant by ‘all risks’.

Two LOPA studies cited tolerable risk targets of 1x10^{-5} or higher and claimed that to be for an annual risk of fatality to more than one person: in these cases the chosen risk target does not seem appropriate. Additionally, one LOPA study stated that their risk target applied to between 10 and 50 onsite and offsite fatalities. This strongly suggests that societal risk as well as individual risk should be taken into account, with the more onerous of the two risk targets being applied in any SIL calculations. Consideration of societal risk if found relevant, may often require more stringent safety measures to be applied.

Several LOPA studies did not clearly state their risk criteria, e.g. a risk of what, from what and to what.

9.6 CONCLUSIONS

The majority of LOPA studies considered in this work have areas that need significant improvement. However, it is noted that in many cases the LOPA studies were carried out by consultants, who have in general made recommendations to their clients to improve the protection systems to SIL1[1] and above as defined in BS EN 61511 [4], which the author considers (in the light of the problems identified) to be a good position to take. However, it is not within the scope of this report to identify whether the companies have implemented these recommendations (this is part of other work by HSE).

The degree of rigour applied to LOPA studies, and in particular the data values used, vary widely. Some LOPAs were reliant on standards and other published sources of generic data for their initiating event and protection layer data values. While others used analytical methods such as fault trees and human reliability studies to synthesise more appropriate data for the site in question, many drew on inappropriate generic data or referenced inappropriate examples.

Some LOPA study reports reviewed included human reliability studies using the Human Error Assessment and Reduction Technique (HEART) method. If an appropriate human reliability method is selected and properly applied to provide a systematic assessment, then the inclusion of HEPs, combined with supporting explanations in a LOPA can add to the understanding of risk and is to be encouraged.

The level and quality of the supplementary documentation provided with a LOPA study (necessary to be able to effectively assess whether a LOPA is valid) varied widely. Some included fault trees, event trees, HEART (human error) analyses, and reliability data from their site or from component reliability databases.

The conclusions drawn from a LOPA study will be sensitive to all input assumptions. Therefore, it would be good practice to include as part of the LOPA study a sensitivity analysis to demonstrate the robustness of any conclusions. This has only been carried out in one of the LOPA studies assessed.

LOPA may appear to be an easy method to apply at first but this is deceptive. It needs a good knowledge of the plant being studied, and how it is operated both normally and in emergency conditions. Secondly, the LOPA practitioner needs some experience in numerical safety studies so that mistakes such as selection of inappropriate data, double counting, and invalid logical arguments about independence between layers of protection are not made.

A significant conclusion of this work is that industry should therefore take steps to:

- Improve the knowledge and training of those carrying out LOPA studies;

- Develop better procedures and guidance for the study, including such matters as sensitivity analyses and the standards of documentation and support information to be included;

- Improve the quality of data it uses in the LOPA studies.

Caveats

The LOPA study reviews in this work are based on the information supplied by companies or their consultants to HSE. They have for the purpose of this study been taken at face value without any other knowledge of the sites or systems involved.

We would stress that the data (including risk targets) in this Report are not endorsed by HSL or HSE.

One of the key messages of this study is that a LOPA or similar risk study has to be justified against the particular circumstances at the establishment and the legal requirements for health and safety. This includes the organisational and procedural aspects as well as the safety integrity of technical systems.

The aim of publishing this Report is to stimulate further discussion and improvements in LOPA and similar studies

10 APPENDIX A – LOPA CASE DATA: SUMMARY OF CM, IE & IPL

The data presented in tables 24 to 27 and depicted in charts 1 to 3 were taken from a review of 15 LOPA studies supplied by HSE and submitted by operators of Buncefield type fuel storage site in the UK. The scope of these LOPA studies was the overfill prevention of tanks storing a flammable liquid, typically petrol.

THE DATA CITED IN THIS REPORT ARE NOT ENDORSED BY HSL OR HSE; THEY ARE SUBJECT TO CRITICISMS AS DETAILED IN THE BODY TEXT OF THIS REPORT.

Table 24 Table to show conditional modifier (CM) values for each of the sample LOPA cases

LOPA ID	CM 1 (Probability of Ignition)	CM 2 (Person in hazard area)	CM 3 (Probability of fatality)	CM 4 (Detection of overflow)	CM 5 (Probability of calm weather)	LOPA Total (CM1 X CM2 etc)
1	1.00E-01	1.00E-01	1.00E-01	9.00E-01		**9.00E-04**
2	9.00E-02	1.00E+00	5.00E-01	1.90E-02	4.61E-01	**3.94E-04**
3	1.00E-01	3.00E-02				**3.00E-03**
4	4.00E-01	1.00E-01	1.00E+01	9.00E-01		**3.60E-01**
5	1.00E-01	1.00E-01	1.00E+00	9.00E-01		**9.00E-03**
6	8.00E-02	5.00E-02	1.00E+00	1.00E+00	1.00E+00	**4.00E-03**
7	3.00E-02	1.00E-01	4.30E-01	1.00E+00	5.00E-01	**6.45E-04**
8	4.00E-01	1.00E+00	2.00E-01	5.00E-01		**4.00E-02**
9	8.00E-01	5.00E-01	1.00E-01	2.00E-01		**8.00E-03**
10	6.00E-01	5.00E-01	1.00E-01	1.00E-01		**3.00E-03**
11	5.00E-01	5.00E-01	2.00E-01	1.00E-01		**5.00E-03**
12	8.00E-01	5.00E-01	1.00E-01	2.00E-01		**8.00E-03**
13	8.00E-01	5.00E-01	2.00E-01	1.00E-01		**8.00E-03**
14	9.00E-01	7.50E-01	5.00E-01	2.00E-01		**6.75E-02**
15	6.00E-01	2.00E-01	5.00E-01	2.00E-01		**1.20E-02**

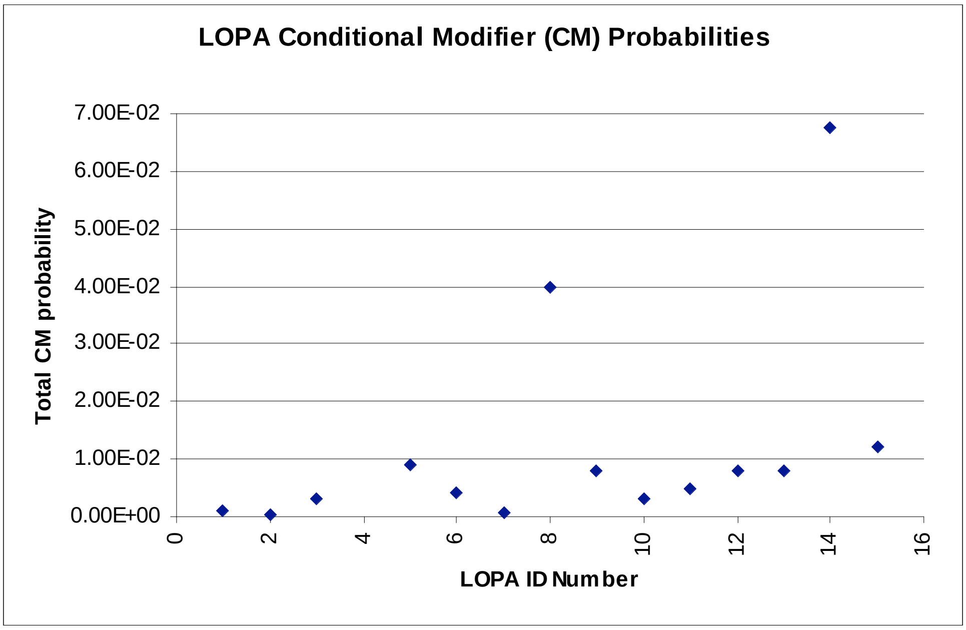

Figure 1 Chart to show the Conditional Modifier product (∏) of each LOPA case

Table 25 Table to show Initiating Event (IE) values for each of the sample LOPA cases

LOPA ID	IE 1 (overcharge)	IE 2 (incorrect product)	IE 3 (Incorrect Line-up)	IE 4 (tank capacity less than expected)	IE 5 (Level instrument failure)	IE 6 (ATG System Fails)	LOPA Total (IE1 + IE2 etc)
1	1.40E-06	1.40E-04	1.40E-05	7.99E-05			**2.35E-04**
2	9.22E+00	7.30E-01	7.10E-01	7.50E-01	3.00E-01	4.00E-02	**1.18E+01**
3	1.00E-01	3.30E-02	5.00E-02				**1.83E-01**
4	3.33E-09	1.84E-03	1.20E-05	2.40E-05	4.53E-05		**1.92E-03**
5	4.40E-08	9.00E-04	1.80E-05	3.60E-05	2.94E-04		**1.25E-03**
6	3.80E-01	no data	3.70E-04	1.92E-01			**5.72E-01**
7	1.00E-01	4.20E-01	1.00E-02	4.00E-01			**9.30E-01**
8	5.00E-02	2.00E-01	5.00E-01	2.00E-01			**9.50E-01**
9	4.28E-04	8.82E-05	2.85E-05	5.70E-05	7.42E-03		**8.02E-03**
10	1.37E-07	4.55E-05	9.10E-04	9.10E-05	1.68E-03		**2.73E-03**
11	1.41E-07	5.65E-05	2.83E-03	1.13E-04	1.72E-03		**4.72E-03**
12	4.86E-02	3.00E-06	no data	no data	2.22E-03		**5.08E-02**
13	2.00E-07	8.00E-05	8.00E-05	2.09E-03	4.00E-05		**2.29E-03**
14	2.25E-08	3.00E-05	6.00E-05	1.96E-03	3.00E-05		**2.08E-03**
15	2.48E-08	6.60E-02	6.60E-05	1.01E-03	3.30E-05		**6.71E-02**

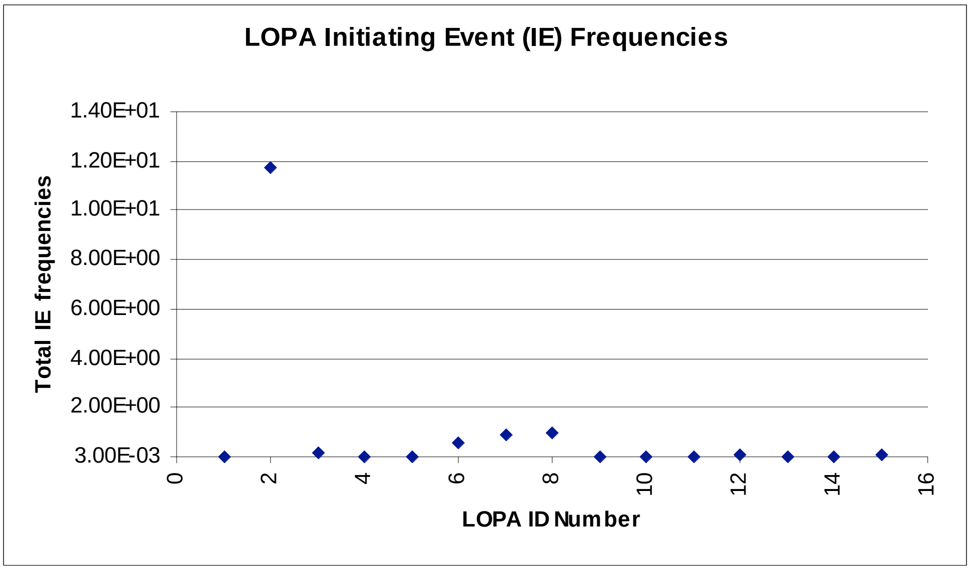

Figure 2 Chart to show the summed (∑) Initiating Event of each LOPA case

Table 26 Table to show Independent Protection Layer (IPL) values for each of the sample LOPA cases

LOPA ID	IPL 1 (Manual ESD)	IPL 2 (HH Alarms)	IPL 3 (Valve trip)	IPL 4 (Overflow detection)	IPL 5 (Fire fighing)	LOPA Total (PL1 X PL2 etc)
1	1.90E-01	1.90E-01				**3.61E-02**
2	7.87E-02	2.45E-02				**1.93E-03**
3	1.00E+00	1.00E+00	1.00E-01	1.00E+00	1.00E+00	**1.00E-01**
4	1.90E-01	1.90E-01				**3.61E-02**
5	1.90E-01	6.34E-03				**1.20E-03**
6	8.50E-02	1.00E-01				**8.50E-03**
7	1.00E-01	1.00E-01	1.00E-01			**1.00E-03**
8	4.00E-01	3.00E-01	4.20E-01			**5.04E-02**
9	3.70E-01	4.60E-01				**1.70E-01**
10	1.90E-01	1.00E-01				**1.90E-02**
11	1.90E-01	1.90E-01				**3.61E-02**
12	1.90E-01	1.00E+00				**1.90E-01**
13	1.90E-01	1.90E-01				**3.61E-02**
14	1.90E-01	1.00E+00				**1.90E-01**
15	1.90E-01	1.90E-01				**3.61E-02**

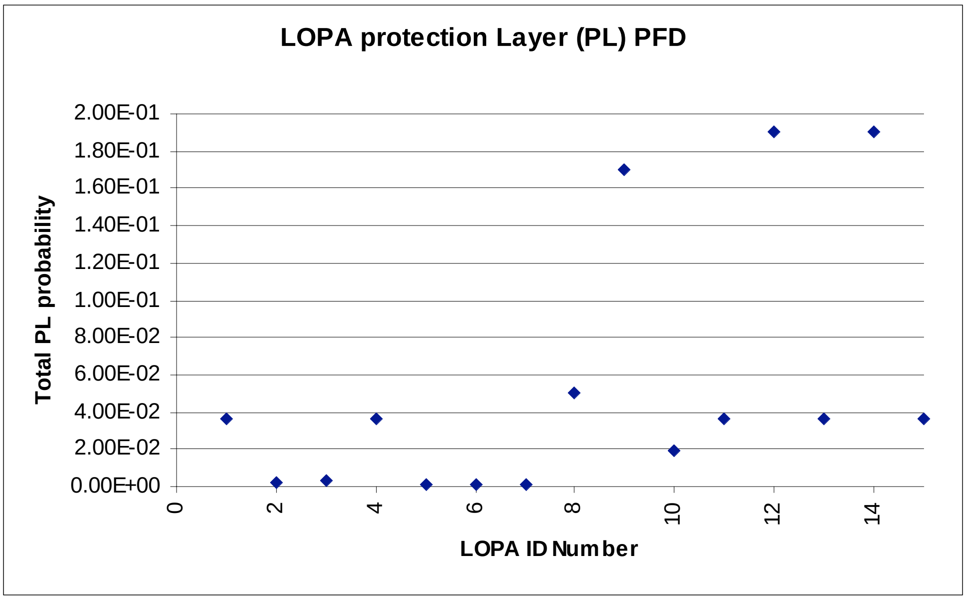

Figure 3 Chart to show the product (∏) of the Independent Protection Layer for each LOPA case

11 APPENDIX B – LOPA CASE DATA: SUMMARY OF MITIGATED & UNMITIGATED CONSEQUENCE, TARGET SIL & SIL GAP

THE DATA CITED IN THIS REPORT ARE NOT ENDORSED BY HSL OR HSE; THEY ARE SUBJECT TO CRITICISMS AS DETAILED IN THE BODY TEXT OF THIS REPORT.

Table 27 Table to summarise key figures from the LOPA case analysis

LOPA results presented	Corporate Risk Criteria	Freq of Unmitigated Consequence	Freq of Mitigated Consequence	Freq of Mitigated Consequence with SIL consideration	Target SIL (value if stated)	Calculated SIL Gap
1	1.00E-06	2.12E-07	1.87E-08	already meets criteria	No SIL recommended	No Shortfall
2	1.00E-06	4.63E-03	9.29E-06	3.79E-04	SIL2	1.08E-01
3	1.00E-05	1.90E-03	5.70E-06	report lacking detail	No SIL recommended	No Shortfall
4	1.00E-06	6.92E-05	1.31E-05	3.43E-07	SIL 2	7.65E-02
5	1.00E-06	1.13E-05	2.11E-06	7.06E-08	SIL2	4.74E-01
6	1.00E-06	2.29E-03	1.60E-06	no data presented	SIL1	6.24E-01
7	3.00E-05	1.49E-04	2.24E-03	no data presented	SIL2	1.34E-02
8	1.00E-06	3.80E-02	1.92E-03	See ***Note 1***	SIL2 *(See note 1)*	5.22E-04
9	1.00E-06	6.42E-05	2.92E-05	3.00E-07	SIL2	3.43E-02
10	1.00E-06	8.18E-06	8.07E-07	already meets criteria	No SIL recommended	No Shortfall
11	1.00E-06	2.36E-05	4.44E-06	1.17E-07	SIL2	2.25E-01
12	1.00E-06	4.07E-04	9.16E-05	4.58E-07	SIL2	1.09E-02
13	1.00E-06	1.83E-05	3.43E-06	9.01E-08	SIL2	2.91E-01
14	1.00E-06	1.40E-04	1.39E-04	6.93E-07	SIL2	7.21E-03
15	1.00E-06	8.05E-04	1.53E-04	6.86E-08	SIL2	6.54E-03

Risk Criteria	1.00E-06	3.00E-05
Freq of Unmitigated Consequence	2.12E-07	3.80E-02
Freq of Mitigated Consequence	1.87E-08	2.24E-03

Note 1.
4.8E-05,
Originally non-SIL rated improvements, but company decision revised to SIL2.

12 REFERENCES

1 Buncefield Major Incident Investigation Board, Recommendations on the design and operation of fuel storage sites, 2007

2 Safety and environmental standards for fuel storage sites Buncefield Standards Task Group (BSTG) Final report, July 2007

3 Company A LOPA report

4 BS EN 61511 parts 1 to 3, Functional safety-Safety instrumented systems for the process industry sector, 2004

5 Company B LOPA report

6 Company C LOPA report

7 Company D LOPA report

8 Company E LOPA report

9 A. W. Cox, F.P. Lees and M.L. Ang, Classification of hazardous locations, 1990, IChemE

10 F P Lees, Loss Prevention in the Process Industries, Volumes (1, 2, 3), second edition, Butterworth Heinemann, 1996

11 Company F LOPA report

12 Layer of protection analysis: simplified process risk assessment, Centre for Chemical Process Safety, CCPS, 2001

13 Company G LOPA report

14 HSE research report RR084, Effects of flashfires on building occupants, WS Atkins Consultants Ltd, 2003

15 HSE Books, Reducing risks protecting people: HSE's decision-making process, Her Majesty's Stationery Office, 2001

13 GLOSSARY

ATG	Automatic tank gauge
BPCS	Basic process control system
BSTG	Buncefield Standards Task Group
CBA	Cost benefit analysis
CCF	Common cause failure
CM	Conditional modifier
DCS	Distributed control system
ESD	Emergency Shutdown
FTA	Fault tree analysis
HC	Hydrocarbon
HEART	Human Error Assessment and Reduction Technique
HEP	Human error probability
HID	Hazardous installations directorate
HL	High level
HHL	High-high level
HOSL	Hertfordshire oil storage limited
IE	Initiating event
IPL	Independent protection layer
IR	Individual risk
LOPA	Layers of protection analysis
MOV	Motor operated valve
MTBF	Mean Time Between Failure
PFD	Probability of failure on demand
PL	Protection layer
PLC	Programmable logic controller
SCADA	Supervisory control and data acquisition
SCS	Safety critical system
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
TOR	Tolerability of risk - HSE
VCE	Vapour cloud explosion

Published by the Health and Safety Executive 07/09

HSE

Health and Safety Executive

A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks

In response to the Buncefield incident, the Major Incident Investigation Board (MIIB) made recommendations to improve safety in the design and operation of fuel storage sites. Two of these recommendations were that loss of primary containment (tank overfill) should be prevented by a high integrity system, and that industry should agree to undertake a systematic assessment of safety integrity levels using commonly agreed methods.

The Buncefield Standards Task Group (BSTG), consisting of representatives from industry and the control of major accident hazards (COMAH) Competent Authority, also stated in its final report, Paragraph 16, "Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve." The BSTG report suggests a layer of protection analysis (LOPA) study be used to provide a more consistent approach to safety integrity level (SIL) determination.

Therefore, in response to the MIIB and BSTG recommendations this study aimed to identify common trends and instances of good practice and areas requiring discussion/improvement in the way in which LOPA studies were carried out by operators of sites that bulk store fuels such as petrol.

This study is part of ongoing work to stimulate discussion between concerned parties with the aim of contributing to the development of improved guidance.

Further guidance can be found on the relevant HSE websites.

http://www.buncefieldinvestigation.gov.uk
http://www.hse..gov.uk/buncefield/response.htm

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

RR716

www.hse.gov.uk