David Raymond Ransome
BA CEng FInstMC

Application for

Functional Safety Expert
(TuV Rheinland)

David R Ransome
P & I Design Ltd
2 Reed Street
Thornaby
TS17 7AF
UK

Telephone +44 7879411444
email: drr@pidesign.co.uk

TÜV Rheinland Functional Safety Program

FS Expert (TÜV Rheinland) - Certificate

Note: Please fill in below table with due diligence. Thank you!

First Name	David
Family Name	Ransome
Email Address	drr@pidesign.co.uk

Company Name (full name as registered)	P & I Design Ltd	
Legal form of company (Ltd., plc., Inc. etc.)	Limited Company	
Invoice address	☒ **Company address** ☐ **Private address**	
Street, Number	2 Reed Street	
ZIP Code	TS17 7AF	
City	Thornaby	
Country	England	
Please consider:	In case the invoicing address is your private address, please consider that VAT (19 %) will be invoiced.	
For companies in EEC Countries:	**VAT ID / Registration No.**	317558836

Application Area	Safety Instrumented Systems, Process Hazard & Risk Analysis Functional Safety Management

☒ I hereby confirm that I wish to apply for the FS Expert (TÜV Rheinland) certificate.

☒ I have attached all necessary application documents.

27.11.2015 DRansome

Date / Signature

THE INSTITUTE
of
MEASUREMENT & CONTROL

FOUNDED

1944

ROYAL CHARTER

1975

This is to certify that

David Raymond Ransome

was admitted as a

FELLOW

of The Institute of Measurement and Control

on the

8th Day of August 2005

President

Secretary

ec uk

Established for the promotion and development
of the knowledge and best practice of engineering

This is to certify that

David Ransome

in membership of

Institute of Measurement and Control

has been registered by the Engineering Council UK and is hereby authorised
to use the style or title of

Chartered Engineer

Kel Fidler
Chairman

Executive Director

Date of Registration 22 August 2005

Date of issue 22 August 2005

Registration No. 555021
This certificate is the property of the Engineering Council UK
Returnable on request or de-registration

The degree of

BACHELOR OF ARTS

has been awarded to

David Raymond Ransome

11th December 1992

The Open University

Vice-Chancellor

Secretary

Shell U.K. Oil Products Limited
Stanlow Manufacturing Complex
PO Box 3
Ellesmere Port
South Wirral CH65 4HB
United Kingdom
Tel +44 (0)151 350 4544
Fax +44 (0)151 350 4525

Dear Colleague

Buncefield Standards Task Group – Final Report

I would like to personally thank you for your hard work, commitment and determination, which has enabled us to produce the accompanying BSTG Final Report.

Together we have achieved a great deal over the last 18 months and I am certain we are a long way towards achieving our aim of ensuring that another Buncefield incident does not occur again. We still have a way to go and I hope that you will continue to contribute and support this aim.

What has really made a difference is the way we have all aligned our individual concerns, interests and determination to deliver a joined up set of recommendations which underpin our aim. As I have expressed in the foreword to the report, how industry responds to such incidents and how the regulators respond on behalf of the public is a measure of our society. The strength and robustness of that response has been extremely impressive.

I would like you, on my behalf, to also thank those within your organisation who have contributed and supported your contribution.

As well as producing new and clearer safety and environmental standards for fuel storage sites we have also achieved something even more remarkable – a change in the way industry and regulators work together. We now have a more mature and effective model with shared commitment to deliver improvements. I am certain we will be able to strengthen this model as we move forward and turn these recommendations into action.

Thank You.

Ken Rivers
Chair, Buncefield Standards Task Group

David R Ransome
BA CENG FInstMC

Application for recognition :

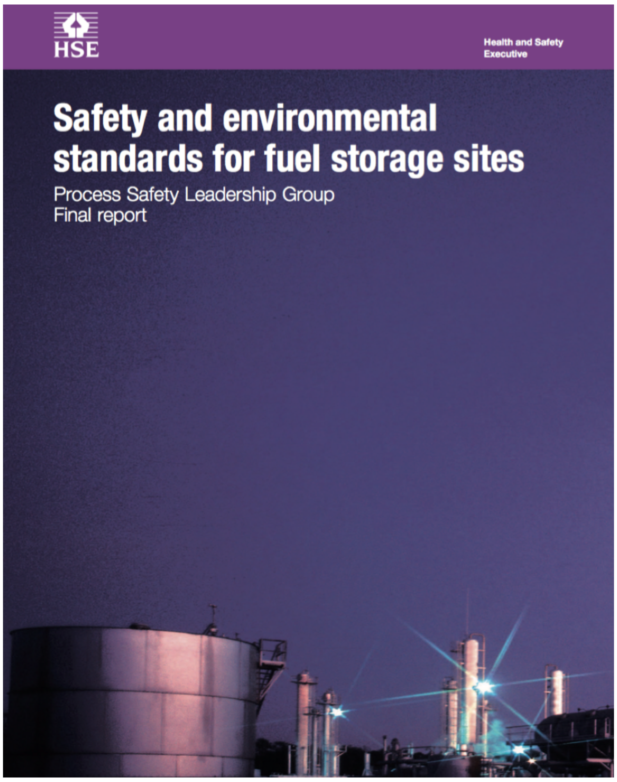
TuV Rheinland Functional Safety Programme

Case Study 1

Developing an Industry/Regulator Acceptable
Layer of Protection Analysis Model for inclusion within PSLG Guidance.

PSLG LOPA Sub-group

2008 – 2009



HSE

Health and Safety
Executive

Safety and environmental standards for fuel storage sites

Process Safety Leadership Group
Final report

INTRODUCTION

On 11th December 2005 one of the largest explosions in peace time Britain occurred as a result of overfilling a gasoline storage tank at the Buncefield depot of the Hertfordshire Oil Storage Ltd. The explosion measured 2.4 on the Richter Scale, the smoke cloud being visible from space. Fortunately, the incident did not result any any fatalities, however there were over 40 casualties, 2 of which were serious. The resulting damage to local property was significant and the storage facility itself was all but destroyed.

Following the incident and in parallel to the judicial enquiries, the Major Accident Investigation Board (MIIB) published a report making recommendations on emergency preparedness, response and recovery for the oil storage sector. In addition, the Buncefield Standard Task Group (BSTG), being the joint Competent Authority / industry standards working group was set up to review safety and environmental protection standards at fuel storage sites following the Buncefield incident.

In July 2007 the BSTG final report was published, I was part of the BSTG working group involved with LOPA and Safety Instrumented Systems.

Following the publication of the BSTG report a second industry / regulator group, Process Safety Leadership Group (PSLG) was formed with the purpose of developing the work produced by the BSTG and providing guidance for the sector in relationship to complying with all of the recommendation produced by the MIIB.

I continued as a part of the PSLG, again in the capacity of assisting in the development of LOPA and Safety instrumented System guidance.

Following the publication of the BSTG report, industry and the regulator felt that the LOPA contained in Appendix 1, a simple order of magnitude example, lacked sufficient complexity and detail. It was therefore a term of reference to the working group that a more detailed example should be developed and guidance produced for the PSLG guidance. The output of this work is Part 1 and Appendix 2 of the PSLG final report published in 2009. ISBN 978 0 7176 6386 6.

PSLG set up several working groups, working group 3 (WG3) – Control & Instrumentation was to produce guidance on LOPA and Safety Instrumented Systems.

A sub-group of WG3, the LOPA sub-group was formed and the group decided that an effective way forward in producing guidance, would be to perform a LOPA at a UK storage facility. This would allow the work of the sub-group to be validated in a true environment.

For my part within the sub-group, I was to liaise with the terminal and chair the LOPA site meetings, together with producing the LOPA calculations and results, together with presenting the findings to the full working group.

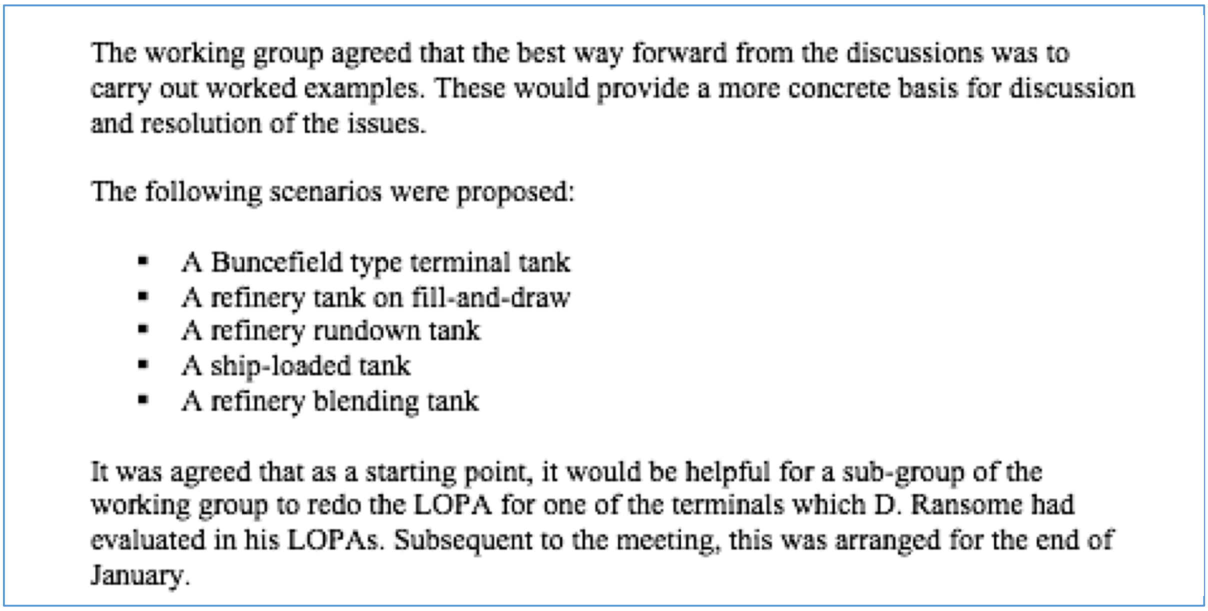
PSLG LOPA SUB-GROUP

Membership

The sub-group comprised a total of 14 delegates with representatives from industry, engineering consultants, the Health & Safety Executive and the Health & Safety Laboratories.

The chair of the group was Richard Gowland, Director of the European Process Safety Centre (EPSC).

At the LOPA sub-group meeting held on 2nd December 2008 at the HSE Offices in London, the following was agreed:



The working group agreed that the best way forward from the discussions was to carry out worked examples. These would provide a more concrete basis for discussion and resolution of the issues.

The following scenarios were proposed:

- A Buncefield type terminal tank
- A refinery tank on fill-and-draw
- A refinery rundown tank
- A ship-loaded tank
- A refinery blending tank

It was agreed that as a starting point, it would be helpful for a sub-group of the working group to redo the LOPA for one of the terminals which D. Ransome had evaluated in his LOPAs. Subsequent to the meeting, this was arranged for the end of January.

Extract from minutes – 2nd December 2008.

The LOPA example working party comprised:

Myself, D R Ransome – as facilitator
Richard Gowland – EPCS
A senior representative from Health & Safety Laboratories
A human factors expert from ABB Consulting

together with five employees of the storage company and an engineer from my company P & I Design Ltd.

PREFACE

Prior to the involvement of the LOPA sub-group, I had conducted a LOPA study for a client with a large storage facility located on the Humber estuary, the study had not been completed, so in discussions with the Terminal Manager, he agreed that we could use his Terminal to facilitate the work of the PSLG.

The LOPA report had been conducted and issued with four revisions:

1. The Original issue
2. Revised with multiple initiating events
3. Clients comments added
4. SIL 2 IPL data added

In February 2009 the LOPA working party visited the site.

SITE VISIT

The members of the working party visited site and re-conducted the LOPA study, the visit involved interviewing terminal operatives to verify that the management procedures claimed with the LOPA were effective and auditable, together with reviewing all the elements of the LOPA, including:

- The Risk Tolerance Criteria
  - Safety
  - Environmental
- The Consequences of the Scenario
- The Initiating Events
  - Calculating the initiating event frequency
- Reviewing the Protection Layers
  - Existing
  - Proposed
- Consideration of Conditional Modifiers
- Human Reliability
  - Operator Error
    - Terminal Specific from Key Performance Indicators
      - During routine operations
      - Response to emergencies
  - Within the LOPA study I also included HEART[1] calculations for sensitivity analysis

The resulting LOPA calculations were conducted and the report updated.

Following the visit, I produced a concise presentation to give to the full LOPA sub-group.

The working party and the sub-group found that the lessons learnt from conducting this exercise assisted greatly in refining the PSLG guidance we developed in:

Part 1 – Systematic assessment of safety integrity level requirements.

together with:

Appendix 2 – Guidance on the application of protection analysis (LOPA) to the overflow of an atmospheric tank

[1] HEART –

Human Reliability Assessment Using the Human Error Assessment and Reduction Technique. http://www.hsl.gov.uk/health-and-safety-training-courses/human-reliability-assessment-using-the-human-error-assessment-and-reduction-technique-(heart)

OUTPUTS

The client’s LOPA study was updated with two further iterations and approved by the regulator.

I presented the findings of the LOPA example to the full LOPA working group, several elements of which developed through into the published report.

The LOPA sub-group continued with our work in developing guidance for conducting Layer of Protection Analysis and the following appendices are included for completeness.

APPENDIX

Appendix 1 – *Presentation to working group*

Appendix 2 – *PSLG Part 1 – Systematic assessment of safety integrity level requirements*

Appendix 3 – *PSLG Part 1 – Guidance on the application of protection analysis (LOPA) to the overflow of an atmospheric tank*

D R Ransome
November 2015

Extract from PSLG Final Report detailing those participating within the working groups.

Paul Jobling	Simon Storage
Allen Ormond	ABB Engineering Services
Craig Garbutt	Vopak
Kevin Shephard	Vopak
Glen Knight	ExxonMobil
Jon Evans	ExxonMobil
Mike Brown	ExxonMobil
Linda Dixon	Chevron
Paul Evans	Chevron
Fiona Brindley	Health and Safety Executive
Peter Mullins	Health and Safety Executive
Ron McLeod	Shell
John Gilbert	Kaneb
Bud Hudspith	UNITE the union

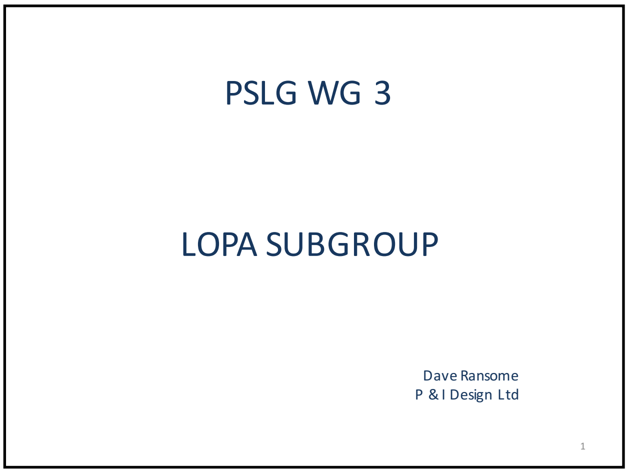
Working Group 2 – Scope

Stuart Barlow (Chairperson)	Health and Safety Executive
James Fairburn	Petroplus
John Galbraith	SABIC
Doug Leach	Chemical Business Association
Neil MacNaughton	INEOS
Kevin Shephard	Vopak
Ian Wilkinson	Total
Stephen Brown	BP

Working Group 3 – Control and instrumentation

Jeff Pearson (Chairperson)	Health and Safety Executive
Chris Newstead	Simon Storage
Dave Ransome	P & I Design Ltd
Ian Neve	Total
John Donald	Total
Joulian Douse	Petroplus
Malcolm Tennant	MHT Technology
Mark Broom	Environment Agency
Martyn Hewitson Griffiths	MHT Technology
Neil MacNaughton	INEOS
Neil Waller	INEOS
Peter Edwards	ConocoPhillips
Richard Gowland	EPSC
Richard Tinkler	ConocoPhillips
Rob Ayton	Petroplus
Robert Nicol	Shell
Stuart Williamson	Petroplus
Terry Lewis	Total
Colin Chambers	Health and Safety Laboratory
David Carter	Health and Safety Executive
Alan King	ABB
Paul Baker	ConocoPhillips

APPENDIX 1

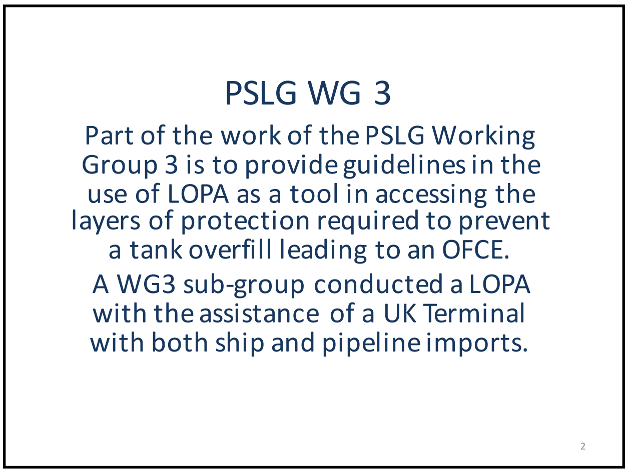


PSLG WG 3

LOPA SUBGROUP

Dave Ransome
P & I Design Ltd

1

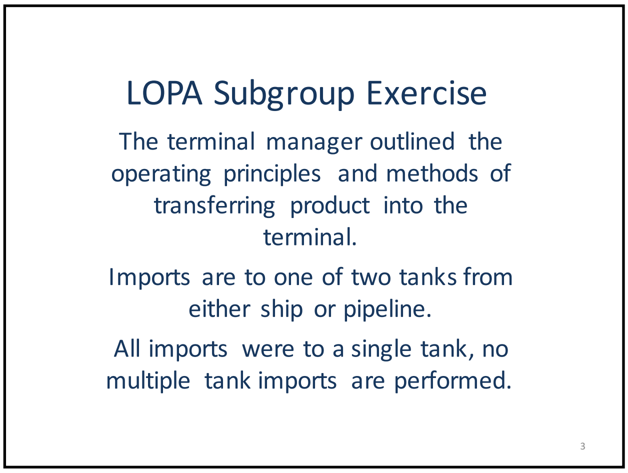


PSLG WG 3

Part of the work of the PSLG Working Group 3 is to provide guidelines in the use of LOPA as a tool in accessing the layers of protection required to prevent a tank overfill leading to an OFCE.

A WG3 sub-group conducted a LOPA with the assistance of a UK Terminal with both ship and pipeline imports.

2



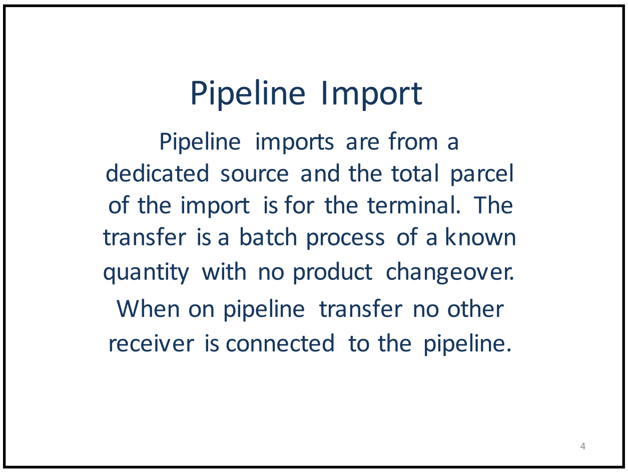
LOPA Subgroup Exercise

The terminal manager outlined the operating principles and methods of transferring product into the terminal.

Imports are to one of two tanks from either ship or pipeline.

All imports were to a single tank, no multiple tank imports are performed.

3

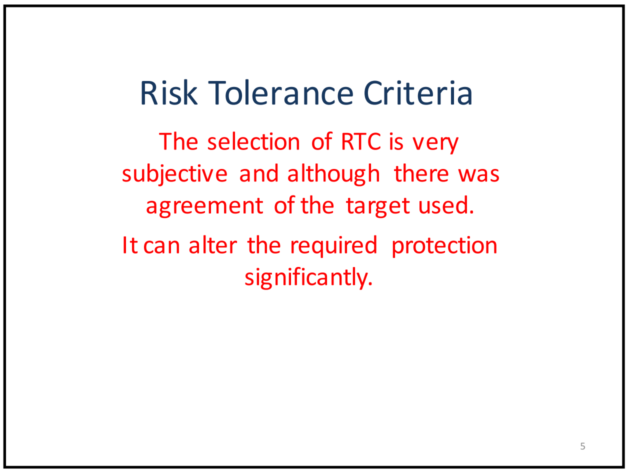


Pipeline Import

Pipeline imports are from a dedicated source and the total parcel of the import is for the terminal. The transfer is a batch process of a known quantity with no product changeover.

When on pipeline transfer no other receiver is connected to the pipeline.

4

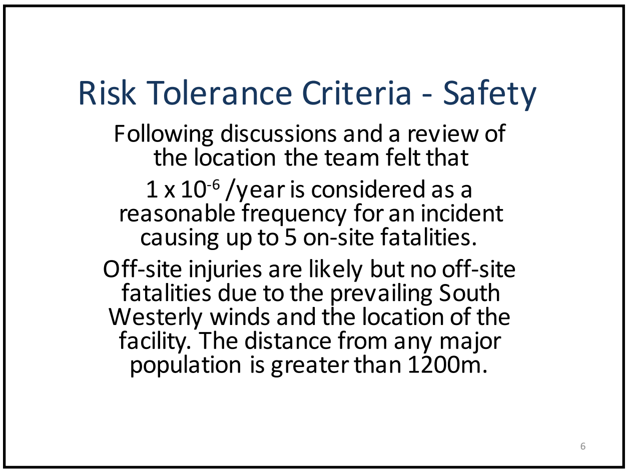


Risk Tolerance Criteria

The selection of RTC is very subjective and although there was agreement of the target used.

It can alter the required protection significantly.

5



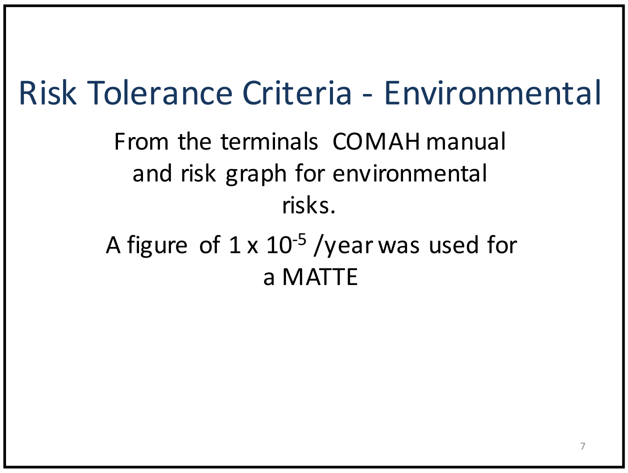
Risk Tolerance Criteria - Safety

Following discussions and a review of the location the team felt that

1 x 10^{-6} /year is considered as a reasonable frequency for an incident causing up to 5 on-site fatalities.

Off-site injuries are likely but no off-site fatalities due to the prevailing South Westerly winds and the location of the facility. The distance from any major population is greater than 1200m.

6

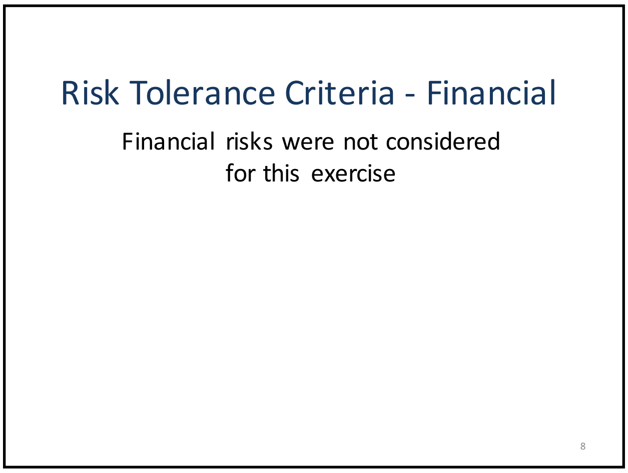


Risk Tolerance Criteria - Environmental

From the terminals COMAH manual and risk graph for environmental risks.

A figure of 1 x 10^{-5} /year was used for a MATTE

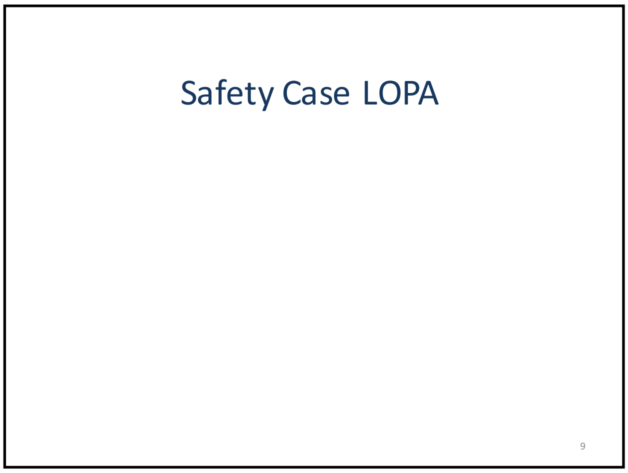
7



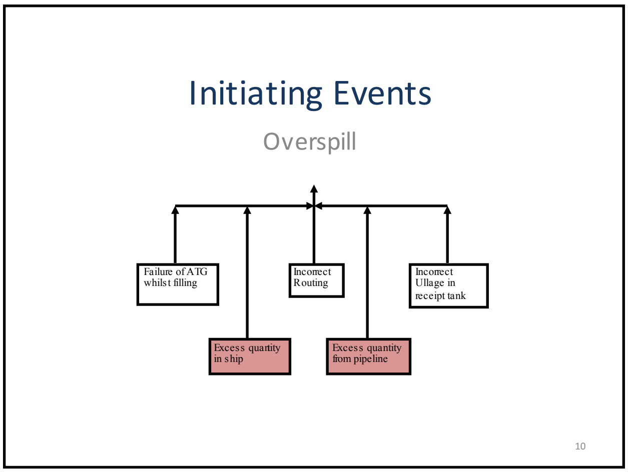
Risk Tolerance Criteria - Financial

Financial risks were not considered for this exercise

8



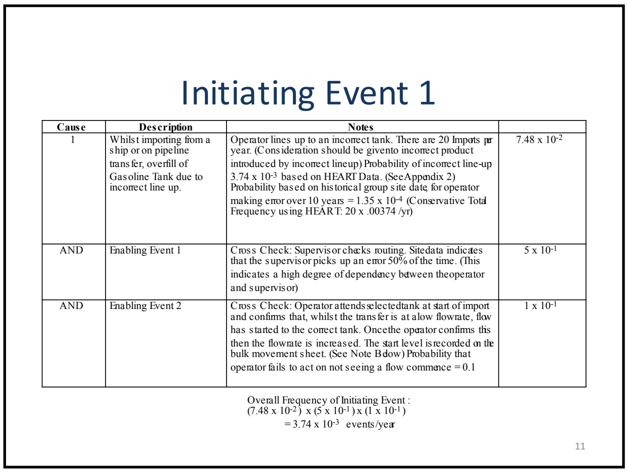
Safety Case LOPA



Initiating Events

Overspill

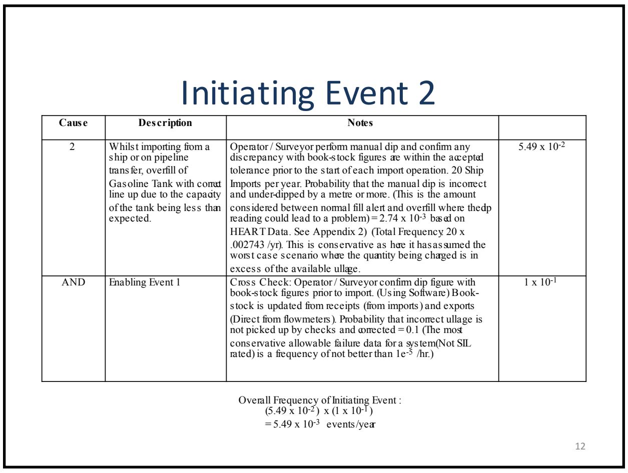
Failure of ATG whilst filling
Incorrect Routing
Incorrect Ullage in receipt tank
Excess quantity in ship
Excess quantity from pipeline



Initiating Event 1

Cause	Description	Notes	
1	Whilst importing from a ship or on pipeline transfer, overfill of Gasoline Tank due to incorrect line up.	Operator lines up to an incorrect tank. There are 20 Imports per year. (Consideration should be givento incorrect product introduced by incorrect lineup) Probability of incorrect line-up 3.74×10^{-3} based on HEART Data. (SeeAppendix 2) Probability based on historical group site date, for operator making error over 10 years = 1.35×10^{-4} (Conservative Total Frequency using HEART: 20 x .00374 /yr)	7.48×10^{-2}
AND	Enabling Event 1	Cross Check: Supervisor checks routing. Sitedata indicates that the supervisor picks up an error 50% of the time. (This indicates a high degree of dependency between theoperator and supervisor)	5×10^{-1}
AND	Enabling Event 2	Cross Check: Operator attends selectedtank at start of import and confirms that, whilst the transfer is at alow flowrate, flow has started to the correct tank. Oncethe operator confirms this then the flowrate is increased. The start level isrecorded on the bulk movement sheet. (See Note Below) Probability that operator fails to act on not seeing a flow commence = 0.1	1×10^{-1}

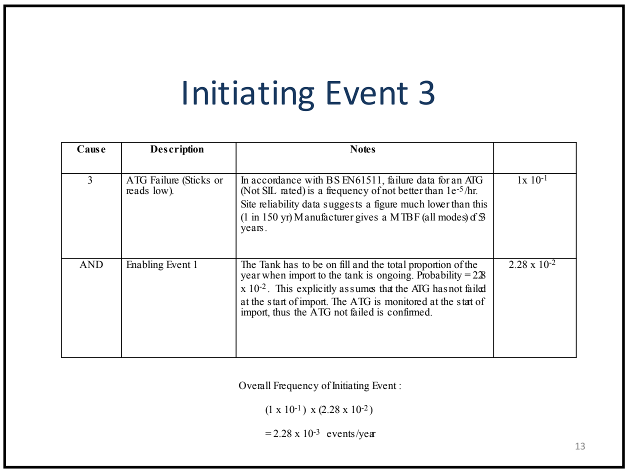
Overall Frequency of Initiating Event :
$(7.48 \times 10^{-2}) \times (5 \times 10^{-1}) \times (1 \times 10^{-1})$
$= 3.74 \times 10^{-3}$ events/year



Initiating Event 2

Cause	Description	Notes	
2	Whilst importing from a ship or on pipeline transfer, overfill of Gasoline Tank with correct line up due to the capacity of the tank being less than expected.	Operator / Surveyor perform manual dip and confirm any discrepancy with book-stock figures are within the accepted tolerance prior to the start of each import operation. 20 Ship Imports per year. Probability that the manual dip is incorrect and under-dipped by a metre or more. (This is the amount considered between normal fill alert and overfill where thedip reading could lead to a problem) = 2.74×10^{-3} based on HEART Data. See Appendix 2) (Total Frequency 20 x .002743 /yr). This is conservative as here it hasassumed the worst case scenario where the quantity being charged is in excess of the available ullage.	5.49×10^{-2}
AND	Enabling Event 1	Cross Check: Operator / Surveyor confirm dip figure with book-stock figures prior to import. (Using Software) Book-stock is updated from receipts (from imports) and exports (Direct from flowmeters). Probability that incorrect ullage is not picked up by checks and corrected = 0.1 (The most conservative allowable failure data for a system(Not SIL rated) is a frequency of not better than $1e^{-5}$ /hr.)	1×10^{-1}

Overall Frequency of Initiating Event :
$(5.49 \times 10^{-2}) \times (1 \times 10^{-1})$
$= 5.49 \times 10^{-3}$ events/year



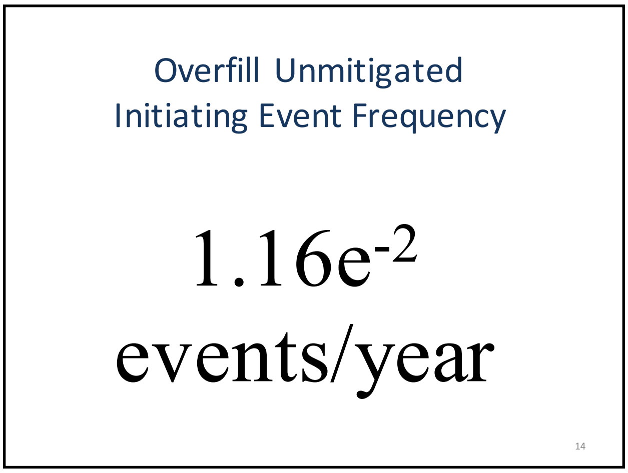
Initiating Event 3

Cause	Description	Notes	
3	ATG Failure (Sticks or reads low).	In accordance with BS EN61511, failure data for an ATG (Not SIL rated) is a frequency of not better than 1e^{-5}/hr. Site reliability data suggests a figure much lower than this (1 in 150 yr) Manufacturer gives a MTBF (all modes) of 53 years.	1x 10^{-1}
AND	Enabling Event 1	The Tank has to be on fill and the total proportion of the year when import to the tank is ongoing. Probability = 2.28 x 10^{-2}. This explicitly assumes that the ATG has not failed at the start of import. The ATG is monitored at the start of import, thus the ATG not failed is confirmed.	2.28 x 10^{-2}

Overall Frequency of Initiating Event :

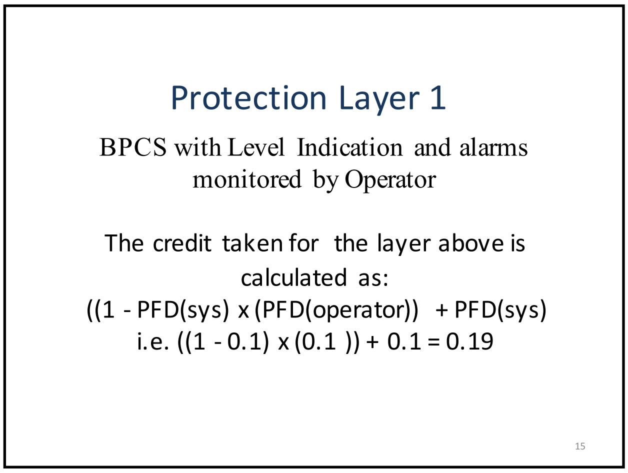
(1 x 10^{-1}) x (2.28 x 10^{-2})

= 2.28 x 10^{-3} events/year



Overfill Unmitigated Initiating Event Frequency

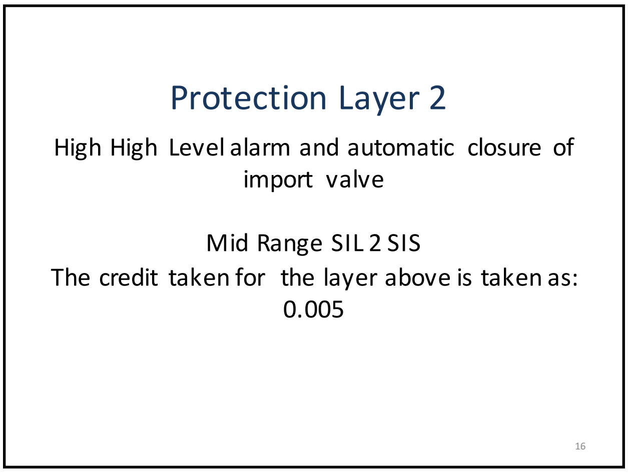
$1.16e^{-2}$ events/year



Protection Layer 1

BPCS with Level Indication and alarms monitored by Operator

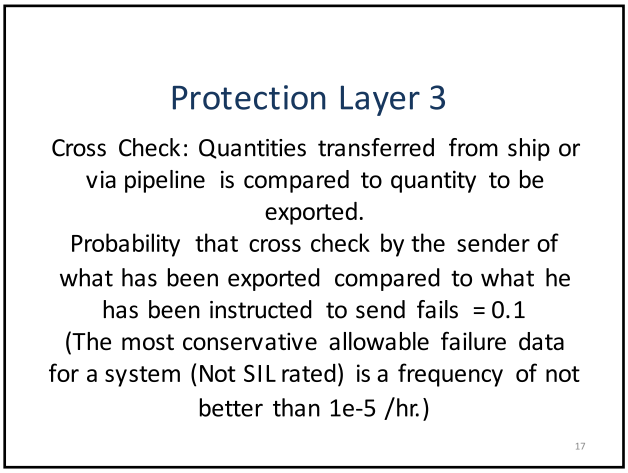
The credit taken for the layer above is calculated as:
((1 - PFD(sys) x (PFD(operator)) + PFD(sys)
i.e. ((1 - 0.1) x (0.1)) + 0.1 = 0.19



Protection Layer 2

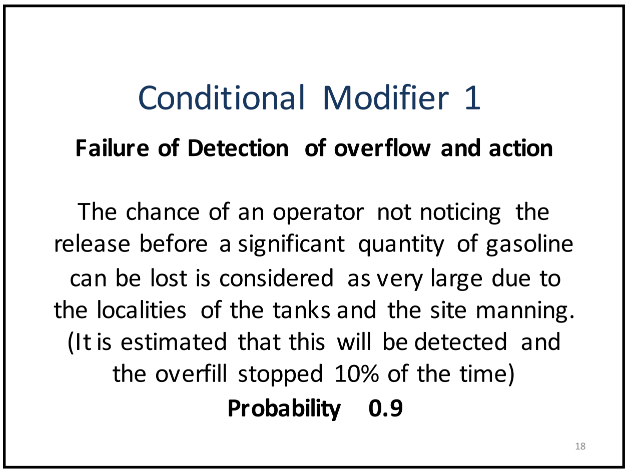
High High Level alarm and automatic closure of import valve

Mid Range SIL 2 SIS
The credit taken for the layer above is taken as:
0.005



Protection Layer 3

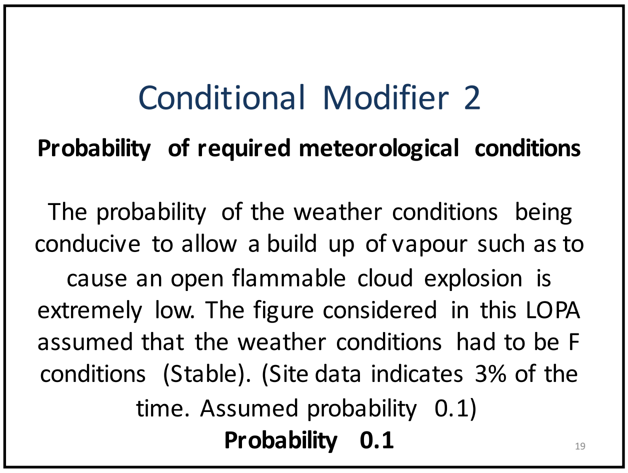
Cross Check: Quantities transferred from ship or via pipeline is compared to quantity to be exported.
Probability that cross check by the sender of what has been exported compared to what he has been instructed to send fails = 0.1
(The most conservative allowable failure data for a system (Not SIL rated) is a frequency of not better than 1e-5 /hr.)



Conditional Modifier 1

Failure of Detection of overflow and action

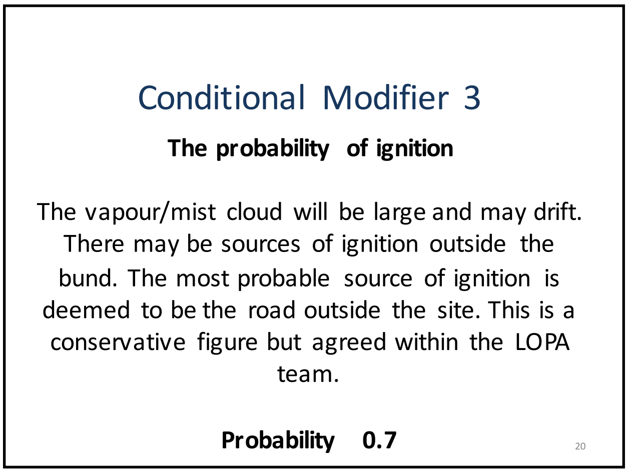
The chance of an operator not noticing the release before a significant quantity of gasoline can be lost is considered as very large due to the localities of the tanks and the site manning. (It is estimated that this will be detected and the overfill stopped 10% of the time)
Probability 0.9



Conditional Modifier 2

Probability of required meteorological conditions

The probability of the weather conditions being conducive to allow a build up of vapour such as to cause an open flammable cloud explosion is extremely low. The figure considered in this LOPA assumed that the weather conditions had to be F conditions (Stable). (Site data indicates 3% of the time. Assumed probability 0.1)
Probability 0.1



Conditional Modifier 3

The probability of ignition

The vapour/mist cloud will be large and may drift. There may be sources of ignition outside the bund. The most probable source of ignition is deemed to be the road outside the site. This is a conservative figure but agreed within the LOPA team.

Probability 0.7

Conditional Modifier 4

Probability of personnel being in affected area

The chance of any personnel being present is considered as 100% as an OFCE as at Buncefield would extend over a large enough area to affect personnel.

Probability 1

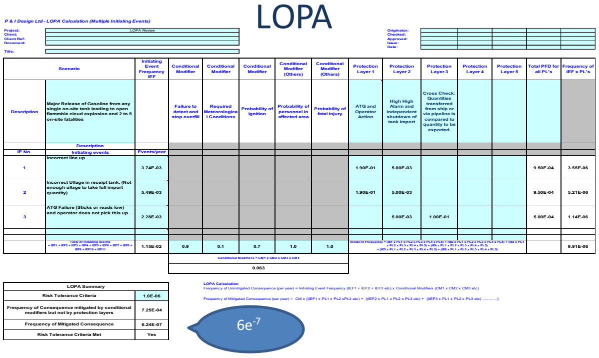
Conditional Modifier 5

Probability of a fatal injury

The likelihood of fatality is considered as absolute. (This figure is felt to be conservative, and is based upon explosion risk as opposed to fire risk).

Probability 1

LOPA



P & I Design Ltd - LOPA Calculation (Multiple Initiating Events)

Project: LOPA Review
Client:
Client Ref:
Document:
Title:

Originator:
Checked:
Approved:
Issue:
Date:

Scenario		Initiating Event Frequency IEF	Conditional Modifier	Conditional Modifier	Conditional Modifier	Conditional Modifier (Others)	Conditional Modifier (Others)	Protection Layer 1	Protection Layer 2	Protection Layer 3	Protection Layer 4	Protection Layer 5	Total PFD for all PL's	Frequency of IEF x PL's
Description	Major Release of Gasoline from any single on-site tank leading to open flammble cloud explosion and 2 to 5 on-site fatalities		Failure to detect and stop overfill	Required Meteorological Conditions	Probability of ignition	Probability of personnel in affected area	Probability of fatal injury	ATG and Operator Action	High High Alarm and independent shutdown of tank import	Cross Check: Quantities transferred from ship or via pipeline is compared to quantity to be exported.				
	Description													
IE No.	Initiating events	Events/year												
1	Incorrect line up	3.74E-03						1.90E-01	5.00E-03				9.50E-04	3.55E-06
2	Incorrect Ullage in receipt tank. (Not enough ullage to take full import quantity)	5.49E-03						1.90E-01	5.00E-03				9.50E-04	5.21E-06
3	ATG Failure (Sticks or reads low) and operator does not pick this up.	2.28E-03							5.00E-03	1.00E-01			5.00E-04	1.14E-06
	Total of Initiating Events = IEF1 + IEF2 + IEF3 + IEF4 + IEF5 + IEF6 + IEF7 + IEF8 + IEF9 + IEF10 + IEF11	1.15E-02	0.9	0.1	0.7	1.0	1.0	Incident Frequency = (IE1 x PL1 x PL2 x PL3 x PL4 x PL5) + (IE2 x PL1 x PL2 x PL3 x PL4 x PL5) + (IE3 x PL1 x PL2 x PL3 x PL4 x PL5) + (IE4 x PL1 x PL2 x PL3 x PL4 x PL5) + (IE5 x PL1 x PL2 x PL3 x PL4 x PL5) + (IE6 x PL1 x PL2 x PL3 x PL4 x PL5)						9.91E-06

Conditional Modifiers = CM1 x CM2 x CM3 x CM4

0.063

LOPA Summary	
Risk Tolerance Criteria	1.0E-06
Frequency of Consequence mitigated by conditional modifiers but not by protection layers	7.25E-04
Frequency of Mitigated Consequence	6.24E-07
Risk Tolerance Criteria Met	Yes

LOPA Calculation
Frequency of Unmitigated Consequence (per year) = Initiating Event Frequency (IEF1 + IEF2 + IEF3 etc) x Conditional Modifiers (CM1 x CM2 x CM3 etc)

Frequency of Mitigated Consequence (per year) = CM x {(IEF1 x PL1 x PL2 xPL3 etc) + {(IEF2 x PL1 x PL2 x PL3 etc) + {(IEF3 x PL1 x PL2 x PL3 etc) ....}

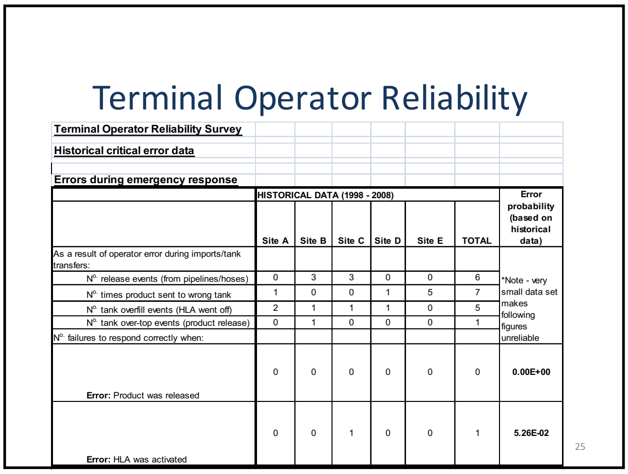
$6e^{-7}$

Terminal Operator Reliability

Historical critical error data

Errors during routine operations

	HISTORICAL DATA (1998 - 2008)						Error probability (based on historical data)
	Site A	Site B	Site C	Site D	Site E	TOTAL	
$N^{o.}$ ship imports in last 10 years	3840	8185	1956	1110	853	**15944**	
$N^{o.}$ pipeline imports (from external sites) in last 10 years	10920	12025	1119	1070	3804	**28938**	
$N^{o.}$ tank-to-tank transfers in last 10 years	3650	5365	1874	2349	1255	**14493**	
Error: $N^{o.}$ imports/tank transfers in which operator failed to rig up transfer line correctly	1	2	3	1	1	**8**	**1.35E-04**
Error: $N^{o.}$ transfers in which supervisor/2nd operator failed to identify operator's error (inadequate check or check not carried out). *Includes failures to check all aspects of the system set-up, not just rigging of transfer line)*	0	2	0	1	1	**4**	**6.74E-05**



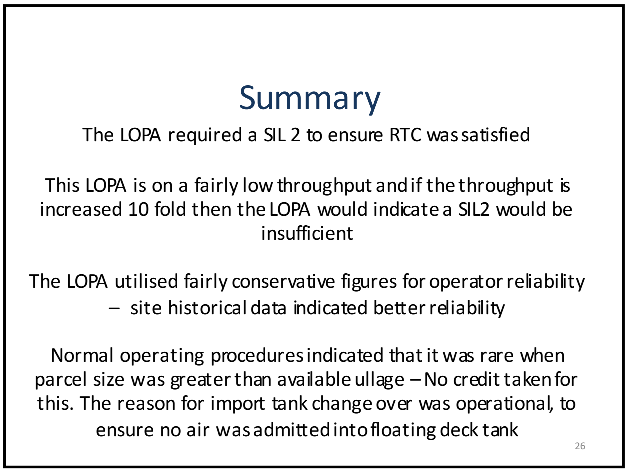
Terminal Operator Reliability

Terminal Operator Reliability Survey

Historical critical error data

Errors during emergency response

	HISTORICAL DATA (1998 - 2008)						**Error probability (based on historical data)**
	Site A	**Site B**	**Site C**	**Site D**	**Site E**	**TOTAL**	
As a result of operator error during imports/tank transfers:							*Note - very small data set makes following figures unreliable
Nº· release events (from pipelines/hoses)	0	3	3	0	0	6	
Nº· times product sent to wrong tank	1	0	0	1	5	7	
Nº· tank overfill events (HLA went off)	2	1	1	1	0	5	
Nº· tank over-top events (product release)	0	1	0	0	0	1	
Nº· failures to respond correctly when:							
Error: Product was released	0	0	0	0	0	0	**0.00E+00**
Error: HLA was activated	0	0	1	0	0	1	**5.26E-02**



Summary

The LOPA required a SIL 2 to ensure RTC was satisfied

This LOPA is on a fairly low throughput and if the throughput is increased 10 fold then the LOPA would indicate a SIL2 would be insufficient

The LOPA utilised fairly conservative figures for operator reliability – site historical data indicated better reliability

Normal operating procedures indicated that it was rare when parcel size was greater than available ullage – No credit taken for this. The reason for import tank change over was operational, to ensure no air was admitted into floating deck tank

APPENDIX 2

Part 1 Systematic assessment of safety integrity level requirements

MIIB Recommendation 1

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

(a) the existence of nearby sensitive resources or populations;
(b) the nature and intensity of depot operations;
(c) realistic reliability expectations for tank gauging systems; and
(d) the extent/rigour of operator monitoring.

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

29 The overall systems for tank filling control should be of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow.

30 Dutyholders' systems should meet the latest international standards, ie BS EN 61511:2004.

31 Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve.

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

33 LOPA is one method and is a suitable methodology to determine SILs within the framework of BS EN 61511-1. Note that other methods are available, and are described in BS EN 61511-1.

Overfill protection systems for storage tanks

34 Overfill protection systems, including instrumentation, devices, alarm annunciators, valves and components comprising the shutdown system, should be assessed using BS EN 61511, which sets a minimum performance for SILs. This includes the following considerations:

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

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

36 Shutdown of product flow to prevent an overfill should not depend solely upon systems or operators at a remote location. The receiving site should have ultimate control of tank filling by local systems and valves.

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

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

Application of LOPA to the overflow of an atmospheric tank

39 The dutyholders should review the risk assessment for their installations periodically and take into account new knowledge concerning hazards and developments in standards. Any improvements required by standards such as BS EN 61511 should be implemented so far as is reasonably practicable.

40 LOPA is one of several methods of risk assessment that can be used to facilitate SIL determination; BS EN 61511 Part 3 provides a summary of the method. Other methods described in BS EN 61511, eg risk graphs, are equally acceptable for the determination of SIL. Detailed guidance for the application of LOPA to the overflow of an atmospheric tank is provided in Appendix 2.

Incorporating the findings of SIL assessments into COMAH safety reports

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

- the overall systems for tank filling control are of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow; and
- SIS and management systems should be commensurate with the requirements of BS EN 61511, so far as is reasonably practicable.

Operator responsibilities and human factors

42 Monitoring and control of levels, and protection against overfill, may depend on operators taking the correct actions at a number of stages in the filling procedure. These actions may include, but not be limited to:

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

43 Some of these actions are checks and therefore improve safety; some however are actions critical to safety. The probability of human error increases in proportion to the number of contiguous, critical actions required, so the human factors associated with operator responsibilities need careful consideration. A useful guide is *Reducing error and influencing behaviour* HSG48.[9] Also refer to Annexes 6, 7 and 8 of Appendix 2.

APPENDIX 3

Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric tank

Introduction

1 The scope of this appendix is confined to the filling of atmospheric storage tanks which meet the requirements of the scope defined within this report.

2 Throughout this report reference is made to the British Standard versions of the international standards IEC 61508 and 61511. The British Standards are the official English-language versions of the European Standards approved by CENELEC and are identical with the equivalent IEC standard. The use of British Standard references is because the primary focus of the guidance has been the application of the LOPA technique in the context of United Kingdom health, safety and environmental legislation.

3 This guidance should not be used for occupied building assessments or land use planning purposes due to the current uncertainty in the explosion mechanism.

Overview of LOPA methodology for Safety Integrity Level determination

4 The term 'LOPA' is applied to a family of techniques used for carrying out a simplified- (often referred to as a semi-) quantified risk assessment of a defined hazardous scenario. As originally conceived, the LOPA methodology applied simple and conservative assumptions to make the risk assessment. In this approach, factors are typically approximated to an order of magnitude. Over time, some operating companies have applied greater rigour to the analysis so that the LOPA may now incorporate and summarise several more detailed analyses such as fault trees and human reliability assessments.

5 As a result the LOPA methodology covers analyses ranging from being little different in terms of complexity to a risk graph, to little short of a detailed quantified risk assessment (see Figure 21). Both of these extremes, and everything in between, are legitimate applications of the LOPA methodology. The simple order of magnitude approach is often used as a risk screening tool to determine whether a more detailed analysis should be performed. In some cases, the use of fault tree analysis and event tree analysis, supported by consequence/severity analysis may be more appropriate than using the LOPA methodology.

6 The LOPA technique has been developed and refined over a number of years, and is described more fully in the CCPS concept book *Layer of Protection Analysis*.[57] This appendix draws extensively on the guidance given in the book. However, where the advice in the CCPS BOOK on protection layers claimed for basic process control system (BPCS) functions is not consistent with BS EN 61511; the more conservative approach of BS EN 61511 should be followed. Where relevant, these differences are highlighted, and the requirements of BS EN 61511 should be given precedence.

7 LOPA is often used to identify the shortfall in meeting a predetermined dangerous failure target frequency. For the purposes of this guidance, this shortfall, if it exists, is associated with the average probability of failure on demand of a demand mode safety function required to meet the target dangerous failure frequency. The identified shortfall is equated to the required SIL of a safety instrumented function (SIF), as defined in BS EN 61511.

8 There are several ways of describing a hazardous scenario. The simplest convention is to include in the description:

- the unwanted serious event (the consequence); and
- its potential cause or causes (initiating event(s)).

9 Hazardous scenarios can be derived by a number of techniques, eg Hazard and Operability Studies (HAZOP), Failure Modes and Effects Analysis (FMEA) and What If. These studies will typically provide at least one initiating event, a high level description of the consequences (although details of the severity are rarely provided) and may also provide information on the safeguards.

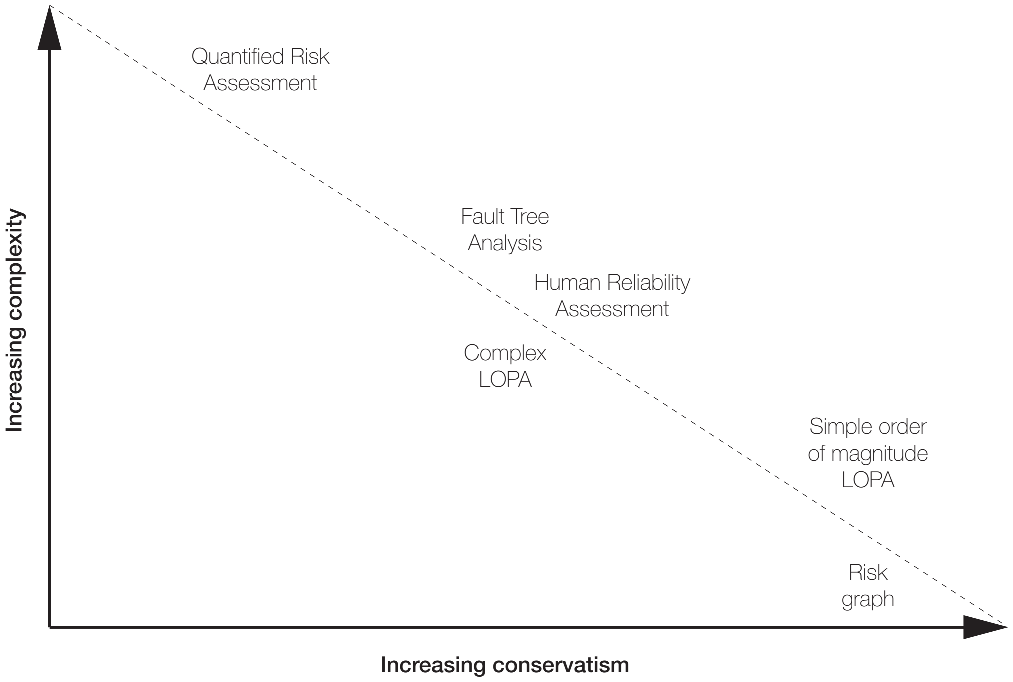


Figure 21 Relationship of LOPA technique to other risk assessment methodologies

10 Once the hazardous scenario has been identified, the LOPA proceeds by defining and quantifying the initiating events (including any enabling events and conditions) more fully and then identifying and quantifying the effectiveness of the protection layers and conditional modifiers which may prevent the scenario from developing or allow it to develop to the defined consequence.

11 It is helpful to adopt a systematic approach to identifying the critical factors which will prevent the initiating event from leading to a loss of containment and those which, once containment is lost, will prevent the undesired consequence from occurring. Essentially, this means considering the analysis in terms of a bow-tie diagram, with the LOPA being the aggregation of a number of individual paths through the bow-tie diagram which result in the same undesired consequence.

12 It is also important to adopt a systematic approach to identifying the consequence of interest for the LOPA from the range of possible outcomes. Annex 2 shows the right-hand side of a bow-tie diagram representing a possible range of consequences to the environment from the overflow of a storage tank.

13 The critical factors can then be divided between prevention protection layers (on the left-hand side of the bow-tie), mitigation protection layers (on the right-hand side of the bow-tie) and conditional modifiers. Further guidance on protection layers and conditional modifiers is given later in this report.

14 In algebraic terms, the LOPA is equivalent to calculating fi^C in the equation below:

$$f^c = \sum_{i=1}^{K} \left(f_i^I \times \left(\prod_{m=1}^{L} P_{im}^{EE} \right) \times \left(\prod_{j=1}^{M} PFD_{ij}^{PL} \right) \times \left(\prod_{k=1}^{N} P_{ik}^{CM} \right) \right)$$

Where:

f^c is the calculated frequency of consequence *C* summed over all relevant initiating failures and with credit taken for all relevant protection layers and conditional modifiers.

f_i^I is the frequency of initiating failure *i* leading to consequence *C*

P_{im}^{EE} is the probability that enabling event or condition *m* will be present when initiating failure *i* occurs.

PFD_{ij}^{PL} is the probability of failure on demand of the *j*th protection layer that protects against consequence *C* for initiating event *i*.

P_{ik}^{CM} is the probability that conditional modifier *k* will allow consequence *C* to occur for initiating event *i*.

15 The calculated value of f^C is then compared with a target frequency. The target frequency may be derived from detailed risk tolerance criteria, or may take the form of a risk matrix. This comparison allows decisions to be made on whether further risk reduction is required and what performance any further risk reduction needs to achieve, including the SIL, if the additional protection layer is a SIS.

16 Some variants of the LOPA methodology determine the harm more precisely in terms of harm caused to people and harm to the environment. This approach, which is required by the tolerability of risk framework for human safety, *Reducing risks, protecting people*,[58] requires consideration of additional factors such as the probability of ignition, the performance of containment systems, and the probability of fatality. For a similar perspective of environmental issues assessors should consult the relevant Environment Agency sector BAT guidance. All of these factors may be subject to considerable uncertainty, and the way the LOPA is carried out needs to reflect this uncertainty. Uncertainties are present in all calculations but sensitivity analysis can be used to help understand the uncertainty.

17 The product of the LOPA should be a report which identifies the hazardous scenario(s) being evaluated, the team members and their competencies, the assumptions made (including any supporting evidence) and the conclusions of the assessment, including the SIL of any SIS identified. The format and detail of the LOPA report should facilitate future internal review by the operating company and should also reflect the likelihood that it may be scrutinised by an external regulator and other third parties.

18 It is important to emphasise that the LOPA methodology is a team-based methodology and its success relies on the composition and competence of the team. The team should have access to sufficient knowledge and expertise to cover all relevant aspects of the operation. In particular, for the risk assessment of an existing operation, the team should include people with a realistic understanding of operational activities and tasks – recognising that this may not be the same as what was originally intended by the designer or by site management. Any LOPA study should be carried out from scenario definition to final result using the knowledge of what is actually done.

19 This guidance supports both simple and more complex applications of LOPA to assess the risks arising from a storage tank overflow. The simpler applications are associated with greater conservatism and less onerous requirements for providing supporting justification. The more complex applications will often require greater amounts of supporting justification and may require specialist input from experts in human factors analysis, risk quantification, dispersion and consequence modelling. Also, as the analysis becomes more complex, it may prove harder to provide long-term assurance that the assumptions in the assessment will remain valid. Users of this guidance should therefore not only consider what factors are currently relevant, but also what is required to make sure that they continue to be relevant.

20 Although this guidance focuses on the LOPA technique, other techniques such as fault tree analysis or detailed quantitative risk assessment, used separately, may be a more appropriate alternative under some circumstances. Quantified methods can also be used in support of data used in a LOPA study. It is common practice with many dutyholders to use detailed quantified risk assessment where multiple outcomes need to be evaluated to characterise the risk sufficiently, where there may be serious off-site consequences, where the Societal Risk of the site is to be evaluated, or where high levels of risk reduction are required.

21 As the LOPA study proceeds, the team should consider whether the complexity of the analysis is still appropriate or manageable within a LOPA or whether a more detailed technique should be used independently of the LOPA technique. Where a more detailed analysis is undertaken, much of this guidance will still be applicable. In all cases the analyst is responsible for ensuring that the appropriate level of substantiation is provided for the complexity of the study being undertaken.

22 To simplify the use of this guidance, a flow chart mapping out the overall process is included (Figure 22).

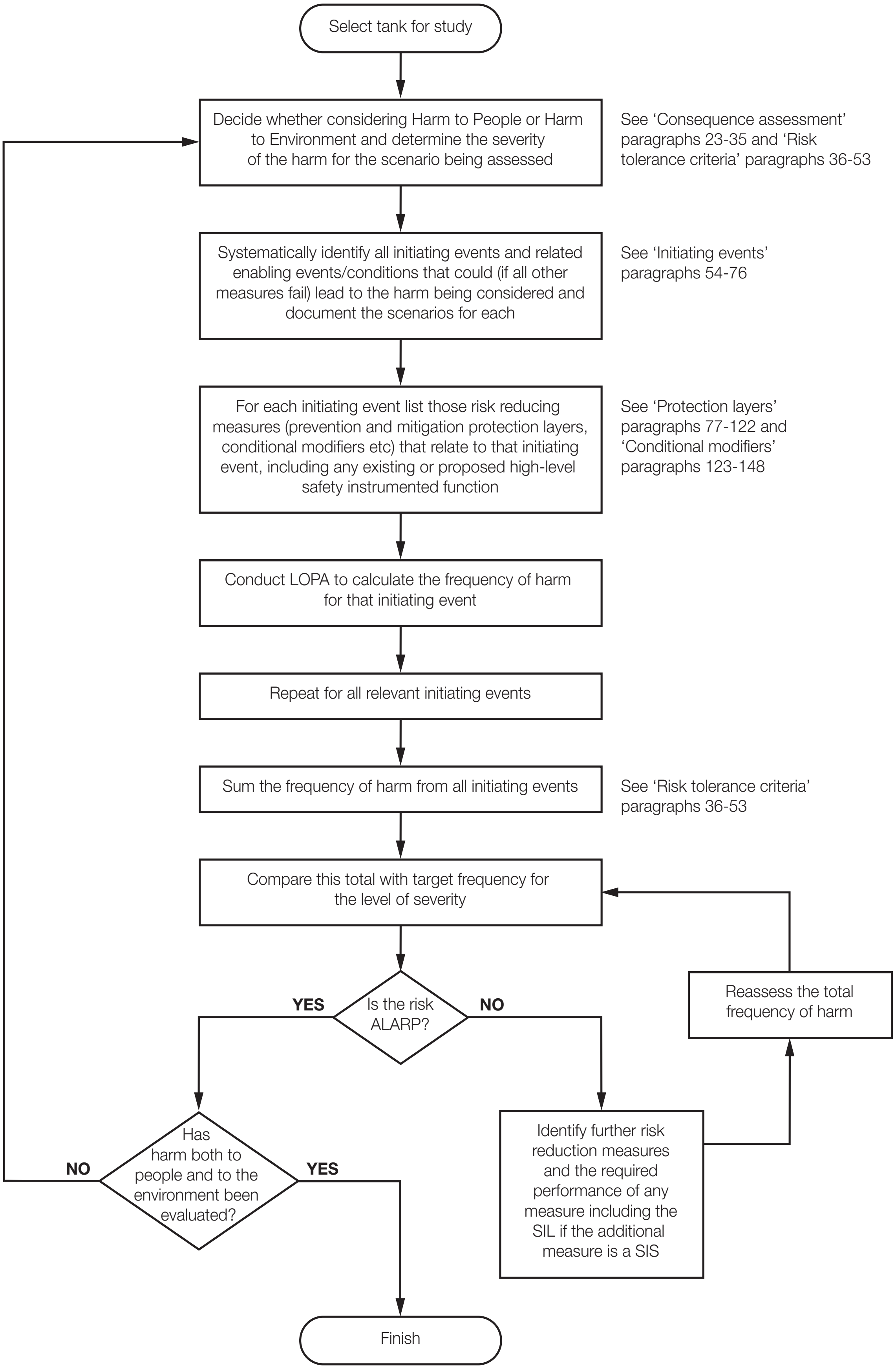

Select tank for study
Decide whether considering Harm to People or Harm to Environment and determine the severity of the harm for the scenario being assessed
See 'Consequence assessment' paragraphs 23-35 and 'Risk tolerance criteria' paragraphs 36-53
Systematically identify all initiating events and related enabling events/conditions that could (if all other measures fail) lead to the harm being considered and document the scenarios for each
See 'Initiating events' paragraphs 54-76
For each initiating event list those risk reducing measures (prevention and mitigation protection layers, conditional modifiers etc) that relate to that initiating event, including any existing or proposed high-level safety instrumented function
See 'Protection layers' paragraphs 77-122 and 'Conditional modifiers' paragraphs 123-148
Conduct LOPA to calculate the frequency of harm for that initiating event
Repeat for all relevant initiating events
Sum the frequency of harm from all initiating events
See 'Risk tolerance criteria' paragraphs 36-53
Compare this total with target frequency for the level of severity
Is the risk ALARP?
YES
NO
Reassess the total frequency of harm
Has harm both to people and to the environment been evaluated?
NO
YES
Identify further risk reduction measures and the required performance of any measure including the SIL if the additional measure is a SIS
Finish

Figure 22 Flowchart for application of LOPA process

Consequence assessment

Overview

23 This guidance is concerned with the prevention of the overflow of an atmospheric storage tank. Such a scenario is only one part of the wider picture of risks associated with storage tank operations. Therefore, the dutyholder of the storage facility should bear in mind that even once the risks of a tank overflow have been addressed, there may be other severe events resulting from (for example) failures of integrity in the tank floor and walls which should also be evaluated before the risk assessment of the facility can be considered complete. For these cases, techniques other than LOPA may be appropriate.

24 In the case of the overflow of a gasoline tank, several outcomes are possible with different safety and environmental consequences:

- Prior to the Buncefield explosion, the most likely consequences from the overflow of an atmospheric storage tank would have been assumed to be a flash fire and/or pool fire. The size of the flash fire would probably have been limited because the influence of vaporisation from an atomised liquid cascade was not recognised and the flash fire would have been associated with evaporation from an assumed quiescent pool in the bund. In either case, the most serious outcome may well have been assumed to be a single fatality somewhere on the operating facility with the off-site consequences being managed through evacuation.
- Following the explosion at Buncefield, the most severe human safety consequence should now be assumed to be an explosion that may cause damage to occupied buildings or places where people may congregate. The explosion will be accompanied by a flash fire and will probably result in multiple pool fires.
- The Buncefield explosion and subsequent fires caused environmental damage due to the contamination of ground and surface water by oil products and firefighting agents. Some of this damage was the result of failures of secondary containment during the fires and insufficient tertiary containment to retain contaminated firefighting water. Experience of leaks from tanks at other sites has been that where the bunds are permeable, ground water contamination can occur.

Individual Risk and scenario-based assessments

25 This guidance addresses four types of assessment for overflow protection: three for safety risk and one for environmental risk. These are as follows:

- Individual Risk assessment, where the calculation is typically performed for a specified individual (often characterised by ‘the person most at risk’ and referenced to a specific job role or a physical location). Typically the calculation takes one of two forms: the risk from a tank overflow is aggregated with contributions from other relevant hazards and then compared with an aggregated risk target; alternatively, the risk from the single overflow scenario may be calculated and compared with a target for the contribution to Individual Risk derived for a single scenario. Individual Risk should aggregate all risks to that individual not just major accident risks. Consideration of Individual Risk is required within the COMAH safety report for an establishment.
- Scenario-based safety risk assessment, where the calculation estimates the frequency with which the hazardous scenario will lead to the calculated consequence (a certain number of fatalities within the total exposed population). The distinction between this calculation and an Individual Risk calculation is that this calculation does not focus on any specific individual but instead considers and aggregates the impact on the whole population. A single scenario-based risk assessment does not account for all the sources of harm to which an individual may be exposed in a given establishment. When scenario-based LOPA is carried out, Individual Risk should also be considered to ensure that Individual Risk limits are not exceeded.
- Societal Risk assessment: Where the scenario contributes significantly to the Societal Risk of the establishment an assessment should be made. For top-tier COMAH sites, consideration of Societal Risk is required within the COMAH safety report and, if applicable, could be more stringent than Individual Risk.
- Scenario-based environmental risk assessment, where the consequence is assessed against a range of outcomes.

26 The distinction between an Individual Risk assessment and a scenario-based safety assessment is important for how the consequence is calculated and for how this is presented in the LOPA. It is of particular relevance to how some protection layers (in particular evacuation, see paragraphs 118–122) and conditional modifiers (probability of presence and probability of fatality, see paragraphs 142–145) are applied.

27 For a scenario-based assessment, there may be no single value for factors such as occupancy or probability of fatality that can be applied across the entire exposed population. If this is the case, it is not appropriate to represent the factor in the LOPA as a protection layer or conditional modifier. Instead the factor should be incorporated into the consequence assessment by subdividing the exposed population into subgroups sharing the same factor value and then aggregating the consequence across all the subgroups.

Estimating the consequences of a Buncefield-type explosion

28 The full details of the explosion at Buncefield are not fully understood at the current time, although the explosion appears to be best characterised by the detonation of at least part of the vapour cloud formed by the overflow (RR718[59]). The available evidence suggests over-pressures of at least 200 kpa within the flammable cloud, but rapidly decaying outside the cloud for the prevailing conditions and Buncefield.

29 Given the limitations on current understanding, it is appropriate to apply the precautionary principle as outlined in *Reducing risks, protecting people* and the policy guidelines published by the United Kingdom Interdepartmental Liaison Group on Risk Assessment: *The Precautionary Principle: Policy and Application*.[60] As described in *Reducing risks, protecting people*, the precautionary principle ‘rules out lack of scientific certainty as a reason for not taking preventive action’. Therefore this guidance offers judgements based on the information currently available in recognition that future developments in modelling and understanding may allow these judgements to be revised.

30 Currently there is no widely available methodology for estimating the size, shape and rate of development of the flammable cloud that could be formed from a storage tank overflow. The behaviour of the explosion and effects cannot be predicted with the more commonly used models such as the multi-energy model. More sophisticated models may be able to estimate the explosion hazards and risks for particular sites. Otherwise it is proposed that consequence assessments are based on the experience of the Buncefield incident.

31 In estimating the spread of the flammable cloud, the simplest assumption is that it spreads in all directions equally. This assumption is conservative and is considered reasonable if there are no topographical factors influencing directionality. At wind speeds of less than 2 m/s, it is assumed that the wind direction is too variable and hard to measure reliably to have a significant directional impact. However, the spread of the flammable cloud at Buncefield was influenced by local topography and the cloud did not spread equally in all directions even under very low wind speed conditions. The influence of topography will need to be considered on a case-by-case basis and should be justified by supporting evidence. This may involve specialised dispersion modelling as standard models cannot reproduce the source term from the plunging cascade and may not be reliable at very low wind speeds. The effort to produce such a justification may only be worth making if the directionality has a significant impact on the consequence.

32 The following distances (Table 7) are considered to be a conservative approximation of the hazard zones for a Buncefield-type explosion and, in the absence of other information, are recommended as a method by which operators can determine relevant hazard zones.

Table 7 Hazardous zones for a Buncefield-type explosion

Zone name	Zone size (measured from the tank wall)	Comment
A	r < 250 m	HSE research report RR718 on the Buncefield explosion mechanism indicates that over-pressures within the flammable cloud may have exceeded 2 bar (200 kPa) up to 250 m from the tank that overflowed (see Figure 11 in RR718). Therefore within Zone A the probability of fatality should be taken as 1.0 due to over-pressure and thermal effects unless the exposed person is within a protective building specifically designed to withstand this kind of event.
B	250m < r < 400 m	Within Zone B there is a low likelihood of fatality as the over-pressure is assumed to decay rapidly at the edge of the cloud. The expected over-pressures within Zone B are 5–25 kPa (see RR718 for further information on over-pressures). Within Zone B occupants of buildings that are not designed for potential over-pressures are more vulnerable than those in the open air.
C	r > 400 m	Within Zone C the probability of fatality of a typical population can be assumed to be zero. The probability of fatality for members of a sensitive population can be assumed to be low.

Note: the distances are radii from the tank wall as this is the location of the overflow (see Figure 23). Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach.

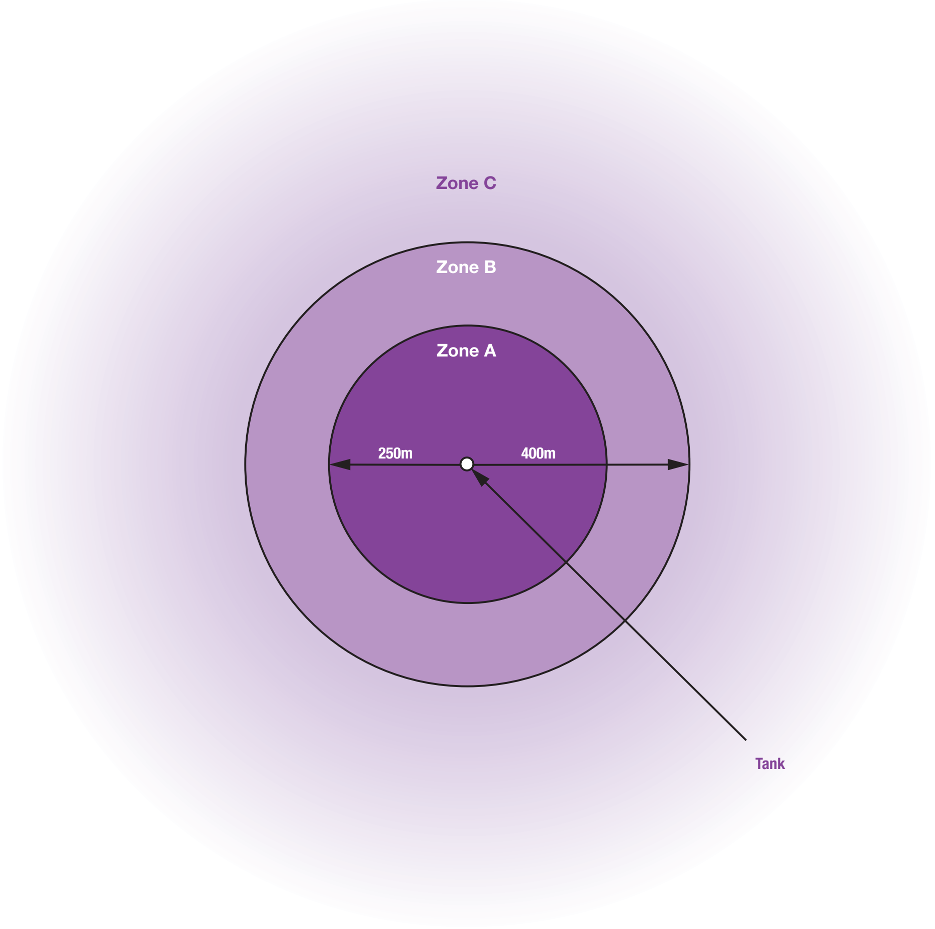


Figure 23 Hazardous zones for a Buncefield-type explosion

33 The zones within Table 7 are provided as a conservative basis. The zones may be adjusted on a case-by-case basis, due to site-specific factors such as:

- Site topography. The Buncefield site is reasonably level other than higher ground to the south. This appears to have affected the spread of the cloud such that it extended 250 m to the north and 150 m to the south. Therefore if a site is not level, distances shorter than Table 7 may be appropriate for the 'uphill' direction. Similarly, if a site has a significant slope, then it would be appropriate to consider distances longer than Table 7 in the 'downhill' direction.
- Significant sources of ignition within Zone A. If there are 'continuous' sources of ignition closer to the tank than 250 m located in a position that could be contacted by the cloud, then it is very likely that the cloud will ignite before it reaches 250 m. This would mean that the distance to the edge of Zone A is less than 250 m and CM2 (Probability of ignition) is likely to be 1. Examples of 'continuous' sources of ignition are boilers, fired heaters and surfaces that are hot enough to ignite the cloud. Typically, automotive, internal combustion engines are not a reliable source of ignition. However, an automotive starter motor is a known ignition source.
- Duration and rate of transfer into the tank. The quantity of petrol that overflowed Tank 912 at Buncefield from initial overflow to ignition was approximately 300 tonnes. If the transfer rate or overflow duration is estimated to be significantly different to that at Buncefield, then this may affect the formation and size of the cloud. An estimate of cloud generation could be made based on modelling such as the 'HSL entrainment calculator' and a 2 m cloud height (for further information see Appendix 1).

34 Other factors that should be considered when estimating the consequence to people are:

- Hazards resulting from blast over-pressure can be from direct and indirect sources. For example, indirect sources of fatal harm resulting from an explosion can be missiles, building collapse or severe structural damage (as occurred at Buncefield).
- People on and off site within the relevant hazard zones should be considered as being at risk. People within on-site buildings such as control rooms or offices that fall within the hazard zones as described above should be considered at risk unless the buildings are sufficiently blast-rated.
- The base case should be 'normal night time occupancy' – see CM1 'Probability of calm and stable weather'. However, a sensitivity analysis should consider abnormally high occupancy levels, eg road tanker drivers, visitors, contractors and office staff who may be present should the calm and stable conditions occur during normal office hours (see paragraph 131). Additionally, sensitive populations just beyond the 250 m, eg a school or old people's home, should also be considered.

Environmental consequences

35 This guidance also covers the environmental risks associated with a storage tank overflow. The consequences may be direct (pollution of an aquifer if the overflowing gasoline penetrates the bund floor) or indirect (pollution arising from firefighting efforts). The consequence will need to be determined on a case-by-case basis after consideration of the site-specific pathways to environmental receptors, the condition of secondary and tertiary containment arrangements, the location and type of specific receptors, and any upgrades planned to meet Containment Policy requirements (*COMAH CA Policy on Containment of Bulk Hazardous Liquids at COMAH Establishments*).

Risk tolerance criteria

General

36 Risk tolerance criteria can be defined for human risk and for environmental risk on the basis of existing guidance. In addition, dutyholders may also have risk tolerance criteria for reputation risk and business financial risk. However, there is no national framework for such criteria and decisions on the criteria themselves and whether to use such criteria in addition to those presented here lie with the dutyholder. No specific guidance is given in this report to evaluating

reputation risk or business financial risk but much of this report will be of assistance in carrying out such evaluations.

37 Regulation 4 of the COMAH Regulations requires dutyholders to 'take all measures necessary (AMN) to prevent major accidents'. This is equivalent to reducing risks to ALARP. HSE's semi-permanent circular *Guidance on ALARP decisions in COMAH*[61] states that:

'The demonstration that AMN have been taken to reduce risks ALARP for top-tier COMAH sites should form part of the safety report as required by regulations 7 and 8 of the COMAH Regulations… For high-hazard sites, Societal Risks/Concerns are normally much more relevant than Individual Risks, but Individual Risk must still be addressed'.

38 See also paragraphs 108 and 109 of *A Guide to the COMAH Regulations* L111.[62]

39 For each 'in scope' tank with the potential of an explosion following an overflow, the tolerability of risk of the major accident hazard scenario must be assessed. A risk assessment should address the categories described in paragraph 25.

Scenario-based safety risk assessment

40 LOPA, like most risk assessment tools, is suitable for this type of risk assessment, using the following approach:

- determine the realistic potential consequence due to the hazardous scenario (in this case the number of fatalities due to an explosion following an overflow from a specific tank);
- estimate the likelihood of the scenario; and
- locate the consequence and likelihood on the following (or similar) risk matrix (Table 8).

Table 8 Risk matrix for scenario-based safety assessments

Likelihood of 'n' fatalities from a single scenario	Risk tolerability		
10^{-4}/yr – 10^{-5}/yr	Tolerable if ALARP	Tolerable if ALARP	Tolerable if ALARP
10^{-5}/yr – 10^{-6}/yr	Broadly acceptable	Tolerable if ALARP	Tolerable if ALARP
10^{-6}/yr – 10^{-7}/yr	Broadly acceptable	Broadly acceptable	Tolerable if ALARP
10^{-7}/yr – 10^{-8}/yr	Broadly acceptable	Broadly acceptable	Broadly acceptable
Fatalities (n)	**1**	**2–10**	**11–50**

41 Table 8 is based on HSE's *Guidance on ALARP decisions in control of major accident hazards (COMAH)* SPC/Permissioning/12. Note that a scenario-based risk assessment with a single fatality is not the same as an Individual Risk calculation.

42 This assessment should be repeated for each 'in-scope' tank in turn. Where there is a large number of in-scope tanks (eg ten or more) the aggregate risk from all of the tanks may be adequately addressed by the individual and societal assessments detailed below, but may require a separate assessment.

Individual Risk assessment

43 The tank overflow scenario may contribute to the risks to individuals, either on-site or off-site. Where the total risk of fatality to any individual (the Individual Risk) from the activities at the hazardous establishment exceeds a frequency of 10^{-6} per year (see *Reducing risks, protecting people* paragraph 130), additional risk reduction measures should be considered, either at the tank or elsewhere, to reduce the risk so far as is reasonably practicable. This exercise should form part of the safety report demonstration for an establishment considering the risk from all major accident hazards.

Societal Risk assessment

44 The scenario of an explosion following a tank overflow may contribute significantly to the societal risk associated with an establishment. If this is the case, then the scenario should be included in the Societal Risk assessment within the safety report for the establishment. As described in the HSE COMAH SPC/Permissioning/12:

> 'Societal Risk is the relationship between frequency of an event and the number of people affected. Societal concern includes (together with the Societal Risk) other aspects of society's reaction to that event. These may be less amenable to numerical representation and include such things as public outcry, political reaction and loss of confidence in the regulator, etc. As such, Societal Risk may be seen as a subset of societal concern.'

45 Assessing a scenario in terms of the numbers of potential fatalities does not address all aspects of societal concern, but is an indicator of the scale of the potential societal consequences. The fatalities may be onsite and/or offsite. Other aspects of societal concern are outside of the scope of this risk assessment guidance.

46 A scenario with the potential for more than ten fatalities may contribute significantly to the level of Societal Risk from the hazardous establishment. Therefore the scenario should also be considered as part of the safety report Societal Risk assessment.

47 A scenario with the potential for ten or less fatalities may not represent a significant Societal Risk and a judgment will need to be taken over its inclusion.

48 *Reducing risks, protecting people* provides one Societal Risk tolerance criterion, that the fatality of '50 people or more in a single event should be regarded as intolerable if the frequency is estimated to be more than one in five thousand per annum' (paragraph 136). This risk criterion is applied to a 'single major industrial activity' as a whole, where a single major industrial activity means an industrial activity from which risk is assessed as a whole, such as all chemical manufacturing and storage units within the control of one company in one location or within a site boundary.

49 There is currently no nationally agreed risk tolerance criterion to determine when the level of Societal Risk is 'broadly acceptable'. This assessment is site-specific, and would therefore need to be performed for the establishment as part of the safety report demonstration and agreed with the CA.

50 LOPA is not normally used to assess Societal Risk because a Societal Risk assessment typically requires the evaluation of a range of scenarios. This is typically carried out using quantified risk assessment techniques such as fault and event trees. There is no universally agreed method of presenting the results of a Societal Risk assessment, but commonly used methods include F-N curves and risk integrals.

Scenario-based environmental risk assessment

51 There are currently no published environmental risk criteria for Great Britain with the same status as those for safety in *Reducing risks, protecting people*. Information on tolerability of environmental risk has also been produced for options assessment in section 3.7 of *Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal of BAT* IPPC H1 Version 6 July 2003.[63] The tolerability criteria from this reference is summarised in matrix form in Table 9 below. Further guidance on environmental risk matrix can be found in Annex 5 of HSE's SPC/Permissioning/11.[64]

52 Dutyholders seeking to demonstrate compliance with the COMAH Regulations should adopt an approach consistent with the information provided in Tables 9 and 10 and with that in their COMAH safety reports and pollution prevention control permit applications.

Table 9 Tolerability of environmental risk

	Category	Acceptable if frequency less than	Acceptable if reduced as reasonably practical and frequency between	Unacceptable if frequency above
6	Catastrophic	10^{-6} per year	10^{-4} to 10^{-6} per year	10^{-4} per year
5	Major	10^{-6} per year	10^{-4} to 10^{-6} per year	10^{-4} per year
4	Severe	10^{-6} per year	10^{-2} to 10^{-6} per year	10^{-2} per year
3	Significant	10^{-4} per year	10^{-1} to 10^{-4} per year	10^{-1} per year
2	Noticeable	10^{-2} per year	~ 10^{+1} to 10^{-2} per year	~10^{+1} per year
1	Minor	All shown as acceptable	–	–

53 For the purposes of this guidance, the categories from Table 9 have been aligned to COMAH terminology as follows:

- 'Acceptable if frequency less than' equates' to the 'Broadly acceptable region';
- 'Acceptable if reduced as low as is reasonably practicable and frequency between' equates to the 'Tolerable if ALARP region';
- 'Unacceptable if frequency above' equates to the 'Intolerable region'.

Table 10 Risk matrix for environmental risk

Category	Definitions	
6	Catastrophic	– Major airborne release with serious off-site effects – Site shutdown – Serious contamination of groundwater or watercourse with extensive loss of aquatic life
5	Major	– Evacuation of local populace – Temporary disabling and hospitalisation – Serious toxic effect on beneficial or protected species – Widespread but not persistent damage to land – Significant fish kill over 5 mile range
4	Severe	– Hospital treatment required – Public warning and off-site emergency plan invoked – Hazardous substance releases into water course with ½ mile effect
3	Significant	– Severe and sustained nuisance, eg strong offensive odours or noise disturbance – Major breach of permitted emissions limits with possibility of prosecution – Numerous public complaints
2	Noticeable	– Noticeable nuisance off site, eg discernible odours – Minor breach of permitted emission limits, but no environmental harm – One or two complaints from the public
1	Minor	– Nuisance on site only (no off-site effects) – No outside complaint

Source From information in IPPC document *Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal of BAT*

Initiating events

54 The next stage of the LOPA is to identify all the significant initiating events that can cause the defined safety or environmental consequence and to estimate the frequency (likelihood) of their occurrence. An initiating event can be considered as a minimum combination of failures and

enabling events or conditions that are capable of generating the undesired consequence – in this case, the overflow of a gasoline storage tank. Initiating events place demands on protection layers.

Identifying initiating events

55 One of the issues identified in the sample review of LOPAs in HSE's research report RR716 was that the identification of initiating events was not comprehensive and therefore that the frequency of demands on protection layers may have been underestimated. It is important that the process for identifying initiating events is comprehensive and that it is carried out with the involvement of those who have to perform the tank-filling operation.

56 Potential causes of tank overflow should be considered in each of the following categories:

- **Equipment failures:** for example failures of level measurement systems (gauges, radar devices, suspended weights), valves and other components; also failures of site services and infrastructure that could affect safe operation (eg loss of power, utilities, communications systems);
- **Human failures:** in particular errors in executing the steps of the filling operation in the proper sequence or omitting steps; and failures to observe or respond appropriately to conditions or other prompts. Possible errors may include but not be limited to:
  - incorrect calculations of the ullage in a tank (leading to an overestimate of how much material can be safely transferred into the tank);
  - incorrect verification of dips or incorrect calibration of level instrumentation;
  - incorrect routing of the transfer (sending material to the wrong tank);
  - incorrect calculation of filling time or incorrect setting of stop gauges;
  - failure to stop the transfer at the correct time (eg missing or ignoring the stop gauge and/or succeeding alarms).
- **External events:** for example:
  - changes in the filling rate due to changing operations on other tanks or due to changes within a wider pipeline network;
  - failure to terminate filling at the source (remote refinery, terminal or ship) on request from the receiving terminal;

One systematic way of identifying initiating events is to prepare a demand tree. This is described in detail and illustrated by example in Annex 3.

Estimating initiating event frequencies

57 The LOPA requires that a frequency is assigned to each initiating event. The frequency may be derived in several ways:

- Where the initiating event is caused by the failure of an item of equipment, the failure rate per year may be derived from the failure-to-danger rate of the equipment item.
- Where the initiating event is caused by the failure of a person to carry out a task correctly and in a timely manner, the initiating event frequency is calculated as the product of the number of times the task is carried out in a year and the human error probability (HEP) for the task. In this case, the time at risk (see Annex 4) is already included in the number of times the task is carried out in a year and no further factor should be applied.
- Where the initiating event is taken to be the failure of a BPCS control loop (when it does not conform to BS EN 61511), the minimum frequency which can be claimed is 1E-5 dangerous failures per hour.

As with any quantitative risk assessment technique, it is important that where probabilities or frequencies are assigned numerical values, these values are supported by evidence. Wherever possible, historical performance data should be gathered to support the assumptions made. Where literature sources are used, analysts should justify their use as part of the LOPA report.

Enabling events/conditions

58 Enabling events and conditions are factors which are neither failures nor protection layers but which must be present or active for the initiating event to be able to lead to the consequence. They can be used to account for features inherent in the way the tank-filling operation is conducted. An example would be that the tank can only overflow while it is being filled, and so certain factors such as instrument failure may only be relevant during a filling operation. This is an example of the 'time at risk', and further guidance on how to include this is given in Annex 4.

59 Enabling events and conditions are expressed as probabilities within the LOPA – ie the probability that the event or condition is present or active when the initiating failure occurs. The most conservative approach would be to assume that enabling events or conditions are always present when an initiating failure occurs (the probability is unity), but this may be unrealistically conservative. The guidance in Annex 4 provides information on how to develop a more realistic figure.

60 Enabling events and conditions are typically operational rather than intentional design features and may not be covered by a facility's management of change process. Therefore caution needs to be taken when the 'time at risk' factor includes operational factors that are likely to change. Examples may include:

- the number of tank-filling operations carried out in a year (which may change as commercial circumstances change);
- the proportion of tank fills which are carried out where the batch size is capable of causing the tank to overflow (it may be that the tank under review normally runs at a very low level and would not normally be able to be filled to the point of overflow by typical batch sizes);
- the tank operating mode (if the tank is on a fill-and-draw operating mode so that the level is more or less static).

While each of these considerations is a legitimate enabling event or condition, caution needs to be taken in taking too much credit for them. It is quite possible that any or all of these circumstances may change as part of normal facility operations without the significance for the validity of the LOPA being recognised in any management of change process.

Special considerations

Failures of the basic process control system (BPCS) as initiating events

61 The term 'basic process control function' (BPCF) was developed to differentiate between the functional requirement for process control (what needs to be done) and the delivery of the functional requirement through the basic process control system (how it is done). The terminology is intentionally analogous to the terms 'safety instrumented function' and 'safety instrumented system'.

62 Although the definitions in BS EN 61511 are not always explicit in this area, a BPCS can include both a fully automated control system and a system that relies on one or more people to carry out part of the BPCF. The BPCS is considered to comprise all the arrangements required to effect normal control of the working level in the storage tank, including operational controls, alarms through the BPCS and the associated operator response. For the purposes of the LOPA and the type of scenario under consideration, the BPCS would typically include several of the following:

- a level sensor on the tank;
- field data marshalling and communications systems;
- input/output cards;
- central processing units (logic controller, processing cards, power supplies and visual displays);
- operators and other workers required to perform the normal control function required to control the level of the storage tank;
- communication arrangements between operators if more than one operator is required to carry out the control function;
- final elements (which may be a remotely or locally operated valve or pump).

63 Refer to Annex 5 for a more detailed discussion about the treatment of the BPCS in the LOPA for the overflow of an atmospheric storage tank.

64 BS EN 61511 sets a limit on the dangerous failure rate of a BPCS (which does not conform to IEC 61511) of no lower than 1E-5/hr. This limit is set to distinguish systems designed and managed in accordance with BS EN 61511 from those that are not. For example minor modifications to hardware and software elements in a BPCS may not routinely be subject to the same rigour of change control and re-evaluation required for a SIS that complies with BS EN 61511. The 1E-5 dangerous failures per hour performance limit should be applied to the system(s) that implement the BPCF taken as a whole, whether operating as a continuous closed-loop system or whether relying on the intervention of a process operator in response to an alarm.

65 The performance claimed for the BPCS should be justified, if possible by reference to actual performance data. For the purposes of analysis, the performance of a given BPCS may be worse than the 1E-5 dangerous failures per hour performance limit but cannot be assumed to be better (even if historical performance data appears to show a better standard of performance) unless the system as a whole is designed and operated in accordance with BS EN 61511.

66 The elements comprising the BPCS may be different for different filling scenarios. In particular, while the tank level sensor may be the same, the human part of the BPCS may change (if multiple people and/or organisations are involved) and also the final element may change (eg filling from a ship may involve a different final element from filling from another tank). In each case, the elements of the BPCS should be defined for each mode of operation of the tank and should be consistent with what is required by operating procedures.

67 There are two main approaches when dealing with initiating events arising from failures in the BPCF within the LOPA:

- In the first and most conservative approach, no credit is taken for any component of the BPCS as a protection layer if the initiating event also involves the BPCS. The failures involving the BPCS may be lumped into a single initiating event or may be separately identified. This approach is consistent with simple applications of LOPA. See Annex 5 for further discussion. This approach fully meets the requirements of BS EN 61511.
- The second approach is to allow a single layer of protection to be implemented where there is sharing of components between the BPCS as an initiator and the BPCS as a layer of protection. Where credit for such a layer is claimed, the risk reduction factor is limited to ten and the analysis must demonstrate that there is sufficient independence between the initiating event and the protection layer (see Annex 5 for further details). For example, a failure of an automatic tank gauge would not necessarily prevent consideration of the same operator who normally controls the filling operation responding to an independent high level alarm as a protection layer, whereas a failure of the operator to stop the filling operation at the required fill level may preclude consideration of their response to a subsequent alarm. This approach meets the requirements of BS EN 61511 providing all the associated caveats are applied and adequate demonstrations are made.

68 It is always preferable to base performance data on the actual operation under review, or at least one similar to it. Care needs to be taken in using manufacturer's performance data for components as these may have been obtained in an idealised environment. The performance in the actual operating environment may be considerably worse due to site- and tank-specific factors.

Additional aids to tank filling operations

69 Operators may be able to configure their own alarms to advise when a tank filling operation is nearing its programmed stop time ('stop gauges'). Software systems may also help with scheduling tasks by keeping track of all the tank movement operations being carried out and ordering the required tasks.

70 Some tank monitoring systems include alarms and systems which monitor for 'stuck' tank gauges and 'unscheduled movement'.

71 While these are useful aids to operation, neither the systems themselves nor the human interface with them are designed or managed in accordance with BS EN 61511. Therefore the credit to be taken for them should be limited. As they also typically rely on the same operator who has to bring the transfer to a stop, it is not appropriate for them to be considered as a protection layer. Instead they may be considered as a contributing factor to the reliability claimed for the operator, for example in relation to error recovery, in carrying out the basic process control function, and are therefore part of the basic process control system.

72 Care needs to be taken to identify situations where the operator has come to rely on the 'assist' function to determine when to take action. It is important to identify this type of situation to avoid making unrealistic reliability claims.

The role of cross-checking

73 Many tank-filling operations include a number of cross-checking activities as part of the operation. These may include checks before the transfer starts (eg routing valve line-up, tank dips, available ullage) and periodic checks during the filling operation (eg to confirm the filling rate, carry out tank dips or check for unusual instrument behaviour).

74 Depending on the circumstances, cross-checks may be represented in the LOPA as modifiers to the initiating event frequency or as part of a protection layer. If the initiating events include a contribution for misrouting, then the frequency of misrouting may be adjusted if a suitably rigorous cross-check is carried out. If the tank filling operation requires an initial tank dip to be carried out, the frequency of the dip being incorrectly carried out or recorded may be affected by a suitable cross-check. If the tank filling operation requires periodic checks of the level to be carried out, this may provide an opportunity to identify that a level gauge has stuck or that the wrong tank is being filled.

75 Cross-checks can provide an opportunity to detect and respond to an error condition, whether the condition has been caused by a human error or an equipment failure. The amount of credit that can be taken for the cross-check will depend on the specifics of what is being checked and the degree of independence of the check. This is discussed in more detail in Annex 6.

76 Various human reliability assessment techniques may be used to evaluate the effectiveness of cross-checking activities – eg THERP (Technique for Human Error Rate Prediction) and HEART (Human Error Assessment and Reduction Technique). It is important that any assessment is made by a competent human reliability specialist and that it is based on information provided by the operators who actually carry out the filling operation.

Protection layers

General principles

77 The LOPA methodology relies on the identification of protection layers, and in specifying protection layers it is important that all the rules for a protection layer are met. A valid protection layer needs to be:

- effective in preventing the consequence; and
- independent of any other protection layer or initiating event; and
- auditable, which may include a requirement for a realistic functional test.

78 Note that the requirement for all three criteria to be met for each protection layer is a stronger requirement than in the Informative Annex D to BS EN 61511-3, where these requirements are only applied to so-called 'independent layers of protection'. The approach adopted in this guidance is consistent with the approach in the CCPS book *Layer of Protection Analysis*.

Effectiveness

79 Care needs to be taken in ensuring that each of these requirements for a protection layer is met and avoid the type of errors described in Annex 1.

80 A protection layer must be effective. This requires that the layer has a minimum functionality that includes at least:

- a means of detection of the impending hazardous condition;
- a means of determining what needs to be done; and finally
- a means of taking effective and timely action which brings the hazardous condition under control.

81 If any of these elements are missing from the protection layer, the layer is incomplete or partial and the elements should be considered an enhancement to another protection layer. For example, the presence of a level detection instrument with a high level alarm which is independent of the normal level instrument used for filling control is not a complete protection layer in its own right. A full protection layer would require consideration of the arrangements for determining what action is required and the means of making the process safe, for example an independent valve/ pump shut-off.

82 For the layer to be effective, it must be capable of bringing the hazardous condition under control and prevent the consequence from developing without the involvement of any other protection layer or conditional modifier. The requirement for timeliness may require careful consideration of the dynamics of the scenario and when any response from a protection layer may be too late to be effective. Where people are involved, care needs to be taken over the human factors of the response.

Independence

83 A protection layer needs to be independent of other protection layers and of the initiating event. This is a requirement of clause 9.5 in BS EN 61511-1 and is a key simplifying feature of LOPA. To ensure that protection layers are independent, it is vital that they are clearly identified. (See Annex 5 for further details.)

84 The simplest application of LOPA requires absolute independence between protection layers, as well as between protection layers and initiating events. Therefore, if a proposed protection layer shares a common component with another protection layer or initiating event (eg a sensor, human operator, or valve), the proposed protection layer could not be claimed as a separate protection layer. Instead, the proposed protection layer would have to be included as part of the initiating event or other protection layer.

85 A more detailed application of LOPA requires ‘sufficient’ rather than absolute independence between protection layers or between a protection layer and an initiating event. The principles within BS EN 61511-1 and 61511-2 (eg clauses 9.4, 9.5 and 11.2) present the requirements on the BPCS when used as a protection layer. For example a detailed evaluation would need to be performed of the possible failure modes of each element of the protection layer – typically involving techniques such as Failure Modes and Effects Analysis, Human Reliability Assessment and Fault Tree Analysis. Great care needs to be taken in using this approach to ensure that consistent assumptions about the condition of equipment or people are made throughout the analysis.

Auditability

86 Protection layers need to be auditable. In this context, audit means far more than simply a management system audit. In broad terms, auditing refers to the continued assessment of system performance, including all the necessary supporting arrangements. The process of testing is required to ensure that a layer of protection will continue to function as originally intended and that the performance has not degraded. The details of this will vary with the details of the protection layer, and may require programmed functional tests. Formal auditing of management systems will also be required to ensure that not only do technical components of the protection layer

continue to perform at the right level, but also that the overall performance of the management system remains at the right level. Whatever the details, the auditing needs to address the following questions:

- How can the performance of this protection layer be degraded?
- What needs to be checked to make sure that the performance has not degraded?
- How often do the checks need to be carried out?
- How can it be confirmed that all the required audits are being carried out with sufficient rigour?

87 For example, routine inspection, testing and maintenance of a level sensor may provide assurance that the sensor will continue to operate, and likewise for the final element. Where people are involved in the protection layer, an ongoing means of demonstrating their performance against defined criteria will need to be developed. This may involve a combination of management system checks (eg by verifying training records and confirming that key documents are available and up-to-date) and observed practical tests (eg carrying out emergency exercises, testing communications arrangements and reviewing the presentation of information by instrumentation systems). Additionally, some form of testing that is analogous to the functional test required for hardware systems should be developed. Regardless of the details for a specific protection layer, it is essential that records of the various 'audits' are retained for future examination and reference.

Prevention layers

General process design

88 An underlying assumption is that the storage tanks being studied by the LOPA are capable of producing the hazard in question by complying with the scope requirements. This does not mean that tanks outside the scope present no risk, but these other risks have not been specifically considered in developing this guidance. For example, if the tank is equipped with an overflow arrangement which precluded the formation of a vapour cloud, this would take the tank outside the scope of this guidance. However, even if the tank has an overflow arrangement which prevents the formation of a large vapour cloud from a liquid cascade, significant safety hazards may still arise from the evaporation and ignition of a liquid pool in the bund, and significant environmental hazards may arise if the liquid leaks through the walls or floor of the bund. The guidance in this report may assist in the assessment of these scenarios.

89 Issues to do with the mode of operation of the tank (eg typical parcel sizes for filling, normal operating levels) are accounted for as enabling events and conditions forming part of the initiating event (see paragraphs 54–76).

The basic process control system as a protection layer

90 It may be possible to take credit for the BPCS as a protection layer if sufficient independence can be demonstrated between the required functionality of the BPCS in the protection layer and any other protection layer and the initiating event. Clauses 9.4 and 9.5 of BS EN 61511-1 and BS EN 61511-2 present the requirements on the BPCS when used as a protection layer. In particular, BS EN 61511-1 9.5.1 states:

> 'The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirement of the protection layers. This assessment may be qualitative or quantitative.'

91 The demonstration of independence is most straightforward if the initiating event does not involve a failure of the BPCS, eg if the initiating event involves misrouting flow to the storage tank and there is sufficient independence between the person making the routing error and the person controlling the filling of the tank.

92 If the initiating event involves a failure of part of the BPCS, the simplest approach under a LOPA would be to discount any further protection layer operating through the BPCS. Some analysts may consider this approach excessively conservative for their situation. However, other analysts and some operating companies are known to apply this approach because of the difficulties associated with making the required demonstrations. Annex 5 gives further guidance on the level of independence required where more than one function is delivered through the BPCS.

93 Claims for risk reduction achieved by the BPCS should meet the requirements of BS EN 61511-1 and 61511-2 (eg clauses 9.4, 9.5 and 11.2).

Response to alarms

94 Dutyholders should review and where necessary revise the settings of the level alarms on their tanks in accordance with Appendix 3. Where the alarm settings meet the requirements, it is considered legitimate to consider operator response as a protection layer under suitable conditions.

95 Where process alarms are delivered through the BPCS, consult Annex 5 for further guidance on independence when credit is being claimed for more than one function implemented through the BPCS. The analysis should meet the requirements of BS EN 61511-1 (for example clauses 9.4, 9.5 and 11.2).

96 The wider considerations of operator response to alarms are discussed in Annex 8. Where the alarm is delivered through the BPCS, the risk reduction factor of the alarm layer should be limited to at best 10 in accordance with BS EN 61511-1 clause 9.4.2.

97 As with other protection layers, the alarm itself is only part of the protection layer. The full protection layer needs to include the alarm, the operator, the machine-operator interface, any communications systems (if communications between operators is required to deliver the required alarm function) and a final element. For the response to the alarm to be included as a protection layer, the following requirements should be met:

- The alarm protection layer should not include any failed component of it which is part of an initiating event. Therefore:
  - if the initiating event is due to a failure of the tank gauge, it would not be legitimate to rely on an alarm generated by the same tank gauge;
  - if the initiating event involves the failure of a valve or pump to stop on demand, the alarm protection layer cannot rely on the same valve or pump to bring the transfer to a stop.
- There must be sufficient time for the transfer to be brought safely to a halt.
- Where the initiating event is a failure within the BPCS and the alarm system uses the same BPCS, credit for the alarm may only be taken if sufficient independence can be shown between the alarm function and the failed BPCS elements (see Annex 5).

Safety instrumented systems

98 In LOPA studies, the normal convention is that the need for SIS is determined when all other protection layers have been considered. If an existing SIS complies with BS EN 61511 then a reliability performance consistent with the SIL-rating of the SIS and its design and operation can be claimed. If any ‘instrumented protection’ does not comply with BS EN 61511 then a risk reduction factor of no greater than 10 can be claimed for it. However, experience has shown that it is unlikely that an instrumented protection system that does not comply with BS EN 61511 would have a reliability assessment associated with it, and therefore an assessment would have to be made to determine the performance level that could be claimed.

Other safety-related protection systems

99 It is possible to argue that some other protection layers can be considered so long as they meet the requirement for a protection layer set out in paragraphs 77–87 of this appendix. Such protection layers are referred to as ‘other technology’ in BS EN 61511 and are not subject to the performance limits required by BS EN 61511, eg pressure relief valves.

Mitigation layers

100 Mitigation layers are protection layers representing intentional design or operational measures which become effective once primary containment has been lost. They must be relevant to the hazardous scenario under consideration and must prevent the consequence from developing. The same mitigation layer may be effective against some consequences but ineffective against others. For example, bunding will not prevent the development of a vapour cloud from a storage tank overflow, but may be effective in preventing certain kinds of environmental consequence. Possible mitigation measures which may have an impact on the overflow of a gasoline storage tank include:

- overflow detection (including gas detection, liquid hydrocarbon detection and direct observation);
- fire protection (to the extent which this may reduce escalation or environmental consequences from a tank overflow, although this was not the case at Buncefield);
- bunding or dyking;
- emergency warning systems and evacuation.

101 For all these, it needs to be recognised that these mitigate the consequence but do not prevent a release and incident. If their effect is included in a LOPA study, it is important to make sure that they are:

- independent of other protection layers, especially where positive action is to be taken;
- properly designed to prevent the undesired consequence;
- effective in preventing the undesired consequence; and
- tested periodically to assure continued effectiveness.

102 When included in a LOPA study, the function of the mitigation layers need to be described in terms of how they meet a demand and their reliability.

Overflow detection

103 Overflow detection may take several forms. It may be automatic, using suitably located gas/liquid detectors to operate valves or pumps, or it may be manual, relying on operator response to various forms of detection (including alarms raised by suitable instrumentation, visual indications such as direct observation or via CCTV, or smell). The details of overflow detection measures will be site-specific, and a number of factors need to be taken into consideration.

104 Where reliance is placed on operators to detect (as opposed to respond to) the overflow, the following factors should be considered:

- site manning levels;
- procedures detailing required checks and appropriate actions;
- other duties performed by the operator.

105 Detection may be adversely affected where the personnel present on site have a number of tasks to do which limit their opportunities for regular and scheduled checks of the storage area. Any checks that are occasional and ad hoc should not be credited in the LOPA. Conversely, when operators have sufficient time formally set aside to check the storage tanks at pre-determined intervals during filling operations, detection becomes more likely. If regular site checks are cited as a mitigation measure these should be set out in a formal procedure and be subject to verification.

106 Where hydrocarbon gas or liquid detection equipment is used the following factors should be considered:

- the type of detection, which should be determined on a case-by-case basis and be specific to the tank under consideration; and
- the location of the detector(s), and the kind of releases which can and cannot be detected; and
- whether the detector is connected to an alarm or provides an input for an automated shutdown, or both.

107 On sites where hydrocarbon gas or liquid detection is used as a means of overflow detection, the detector type, operation, maintenance and detector location are critical factors. Historically, hydrocarbon detection systems have been found not to be highly reliable because their ability to detect gas or liquid depends not only on the reliability of the instrument but also on their positioning in a suitable location and their robust maintenance. Therefore, claims made for the performance of an overflow detection system should include sufficient supporting evidence.

108 Care also needs to be taken to be realistic in specifying the required performance of an overflow detection system because it is only a partial protection layer if it simply detects that the storage tank is overflowing. For the protection layer to be complete and effective, it must also be possible to take action which will stop the overflow before any vapour cloud formed can reach a source of ignition. There are several important elements to this:

- It must be possible for the overflow to be detected and stopped safely (ie without expecting an individual to approach close to the vapour cloud).
- The means of stopping the overflow must be independent of other layers of protection – ie reliance cannot be put on closing valves or stopping pumps which form part of another protection layer.
- The time to stop the overflow requires careful consideration given the assumption of a very low wind speed. Under low wind speed conditions, any large vapour cloud may be persistent and may be capable of being ignited and exploding for some time after the overflow has stopped. Different considerations for response time would apply for an environmental consequence where, for example, the consequence requires that the gasoline penetrates the floor of the bund.
- For any detection system relying on direct observation, careful consideration needs to be given to the human factors of the process, including the time taken for diagnosis, communication, determination of the condition of any other failed protection layers and for the correct action to be taken.
- The human–machine interface, in particular the means of alerting the operator that an overflow has occurred and the human factors affecting the response of the operator.
- Where relevant, the reliability and quality of the communications arrangements, including the presence of any radio ‘blind spots’ and areas of high background noise or distraction.
- Where direct observation is assumed, consideration needs to be given to the means of observation. While the sense of smell may alert a knowledgeable person to the presence of gasoline vapour and to the fact that the situation is abnormal, it is unlikely to allow the source to be localised without further investigation. Even visual observation may not be sufficient if the vapour cloud is large.
- Where the operating procedures for the facility require operators to investigate potential leaks, a failure of the overflow detection protection layer may result in increased numbers of people being vulnerable should the vapour cloud ignite. This may result in worse consequences than would be expected from simple time-averaged observation of where people are and when.
- Where the response to an indication of a tank overflow requires operator intervention, consideration needs to be given to:
  - the expected role of an operator on receipt of a signal from the gas or liquid detection system. (How will the operator be alerted? Will it be obvious which tank is overflowing? Which operator is expected to respond? Where will the operator be when the alert is received? How long will it take to diagnose the situation? Are there clear instructions on what to do? Has the situation been rehearsed?);
  - their ability to take action (which valve needs to be closed? How is the valve identified? Is it accessible safely? How long will it take to close? How is the valve closed?);
  - the effectiveness of the action (will closing the valve in the required response time make much of a difference? Will the gas cloud already have reached a large size?).

Fire protection

109 Fire protection systems are not a relevant mitigation layer for safety because they cannot realistically be expected to prevent a tank overflow from igniting and exploding (as would be expected from a prevention layer). Nor can they mitigate the damage caused by an explosion in such a way as to protect vulnerable people who might otherwise be killed by an explosion.

110 Fire protection systems may be a relevant mitigation layer for environmental damage, but this would depend very much on the environmental consequence being assessed and whether the fire protection system is a critical factor in preventing the consequence from developing. It will also be closely related to the effectiveness of the secondary and tertiary containment and therefore may not be considered a fully independent layer. The relationship of the fire protection system to other layers of protection and the effectiveness it is assigned should be judged on a case-by-case basis.

Bunding/secondary and tertiary containment

111Secondary and tertiary containment are not relevant protection layers against an explosion, but are relevant to minimising the environmental consequences of a tank overflow. The significance of secondary and tertiary containment will depend on the pathways by which the gasoline from the tank (or any products such as contaminated firewater which may be an indirect consequence of the overflow) may enter the wider environment.

112 If secondary containment fails, ground water may be affected. A number of incidents in recent years have involved secondary containment failures resulting in ground water impacts. The use of a low probability of failure on demand for ground water impacts due to secondary containment failures should be justified.

113 Care is particularly required over paths to the environment that may not be immediately obvious. These may include:

- bund floor penetrations for groundwater monitoring bore holes or pipework that may present an easier route to groundwater than through the bulk of the bund floor;
- drainage arrangements for the collection and removal of rainwater and/or water that is drained from the storage tank, especially if these rely on an operator to keep a bund drain valve closed, or to close it after heavy rainfall. Also, if the bund includes rubble drains these may reduce the effective thickness of the bund floor;
- penetrations of the bund wall, where these are inadequately sealed;
- degradation of the condition of earth bund walls, eg due to slumping, settlement and burrowing animals. Also, where access arrangements into the bund result in a reduced effective bund wall height.

114 A LOPA considering the level of reduction of risk provided by secondary and tertiary containment requires a realistic case-by-case assessment which may take into account the extent to which measures comply with current good practice, the means of recovery of spilt material (if it is safe to do so) and the extent to which loss of integrity may occur for the event being considered.

115 The performance of the tertiary containment systems cannot be separated from the emergency response arrangements and their effectiveness. For sites where excess contaminated fire water is piped directly to a suitably sized and designed treatment plant and then to the environment a low probability of failure on demand for the tertiary containment systems would be appropriate. Where such excess fire water would be released directly into surface water or allowed to spill onto the ground and hence pass to ground water, a high probability of failure on demand would be expected to be used. The use of a high risk reduction factor for surface water and/or ground release of excess fire water should be fully justified.

116 Where secondary and tertiary containment arrangements fully meet the requirements for bund permeability, a low probability of failure on demand can be assigned to the protection layers. Where there are gaps against best practice, a higher probability of failure on demand may be warranted.

117 General guidance cannot be given beyond the need for a realistic case-by-case assessment which may take into account environmental remediation and the rate at which penetration of the ground takes place. These considerations will be site-specific and possibly specific to each tank.

Emergency warning systems and evacuation procedures
118 Emergency warning systems and evacuation procedures may allow people to escape in the event of a storage tank overflow, and therefore avoid harm. However, great care is required in taking credit for such systems in the LOPA because in their own right they only constitute a means of, possibly, making a hazardous situation 'safe' (by preventing the consequence from being realised). To be a complete protection layer they need to be combined with a means of detecting an overflow, and therefore emergency warning systems and evacuation procedures are better considered part of an overflow detection protection layer as an alternative to (or in combination with) closing a valve or stopping a pump.

119 In judging the effectiveness of the emergency warning system and evacuation procedures, the following should be considered:

- The time it takes to activate the emergency warning system.
- The coverage of the emergency warning system – can it be heard in all relevant parts of the facility, including in noisy workplaces and inside vessels, vehicles and tanks?
- Have the required emergency response actions been defined clearly and are they communicated to all personnel at risk, including visitors and contractors?
- How is assurance gained that personnel have understood their training and that they continue to remember what to do?
- Is it absolutely clear what needs to be done and how in responding to the alarm?
- Do any decisions need to be made on how to respond to the alarm to deal with specific site conditions at the time?
- Are muster points clearly signed?
- Is at least one muster point located in a safe place for foreseeable site conditions?
- Can personnel access at least one muster point safely regardless of local conditions and will it be obvious which muster point to go to and which route to use even in conditions of poor visibility?
- How long will it take personnel to escape the hazardous area and how does this compare with the time available before ignition might occur?
- Are the evacuation procedures regularly tested by field tests, and what do the test results show?

120 Any credit taken for warning and evacuation systems should be fully justified in the LOPA report.

121 While an overflow detection system combined with a warning alarm and evacuation procedures may meet the requirements for an effective protection layer in considering the risk to an individual, it may not do so for the overall exposed population.

122 Where the risk to a population is being considered, an overflow detection system with a warning alarm and evacuation procedures may only be partially effective. Therefore such a system would not meet the requirement of effectiveness for a LOPA layer of protection. In this case, the contribution of any evacuation system should be considered in the determination of the consequence and not as a protection layer.

Conditional modifiers

123 In this guidance, the term conditional modifiers is applied to risk reduction factors which are either external to the operation of the facility (eg weather) or are part of the general design of the facility without being specific to the prevention of a tank overflow (eg shift manning patterns, on-site ignition controls). Conditional modifiers are represented in the LOPA by probabilities of occurrence, as opposed to the probability of failure on demand used to represent a protection layer.

124 The same principles of independence, effectiveness and auditability which apply to protection layers also apply to conditional modifiers. It is important to make sure that the conditional modifier, as defined in the LOPA, is effective in its own right in preventing the consequence without relying on the performance of another conditional modifier or protection layer. Where the performance of a proposed conditional modifier is conditional on the performance of a protection layer or another conditional modifier, it cannot be considered independent. Instead it should be considered part of another protection layer or conditional modifier. The risk reduction should only be claimed once and the LOPA team will need to decide where best to include it.

125 The use of a given conditional modifier may not be appropriate in all circumstances depending on the type of calculation being performed. See paragraphs 25–27 of this appendix.

126 In many cases there may be uncertainty over what value to use for a given conditional modifier because the factors which influence it cannot all be defined or characterised, eg where the role of human behaviour is uncertain or where the underlying science is itself uncertain. Under these circumstances a conservative approach should be taken, consistent with the application of the precautionary principle (see paragraphs 23–24 of this appendix).

127 The presentation of conditional modifier probability ranges in guidance is problematic because of the number of site- and situation-specific factors that need to be considered. Experience has shown that any values cited in literature are often used without consideration of any accompanying caveats and without due consideration of site- and situation-specific issues. Therefore this guidance aims to describe the relevant factors to be considered rather than proposing specific values. These can then be addressed as part of a reasoned justification to support the probability used for a given conditional modifier.

CM 1 – Probability of calm and stable weather

128 The Buncefield explosion occurred during calm and stable weather conditions. There is insufficient evidence currently available to say with certainty whether the weather needed to be both calm and stable, whether only one of these conditions was required (and if so which), and what wind speed limit should be applied to the 'calm' condition. The basis of this guidance is that the development of a large vapour cloud with the kind of compositional homogeneity that is believed to have existed at Buncefield required both low wind speed and stable atmospheric conditions.

129 It is not certain from the available data what limiting value should be used to define a low wind speed condition. This guidance recommends that a value of 2 m/s is used. Analysts are cautioned against trying to differentiate between wind speeds lower than 2 m/s because of the difficulties in obtaining reliable measurements under such conditions (see CRR133[65]). Noticeably higher wind speeds will disperse the vapour cloud more rapidly and may make it more likely that an ignition would lead to a fire rather than to an explosion.

130 It is also unclear at present what level of atmospheric stability is required for the development of the kind of large vapour cloud formed at Buncefield. The release at Buncefield occurred under inversion conditions which promote the formation of ground-hugging vapour clouds. Given the present state of knowledge, it is recommended that the weather conditions are confined to classes E and F on the basis that these correspond to inversion conditions and are most likely to be associated with low wind speeds.

131 The occurrence of Pasquill classes E and F is between the hours 1600–0800 (see Table 4.1.10 in CRR133) and therefore mainly but not exclusively outside normal office hours. Note that weather conditions associated with the Buncefield explosion are affected by seasonal variations and should be accounted for by the analyst.

CM 2 – Probability of ignition of a large flammable cloud

132 This conditional modifier represents the probability that the ignition of the vapour cloud from a storage tank overflow is delayed until it is sufficiently large to cause a widespread impact. Alternative outcomes are an earlier ignition that causes a localised flash fire, or safe dispersal of the cloud without ignition.

133 As a general rule, as the size and duration of a Buncefield-type release increases the probability of ignition will increase, eventually tending towards 1.0. For shorter duration large releases, some available data has been quoted in LOPA studies by operators based on Lees' Loss Prevention in the Process Industries[66] suggesting a probability of ignition of 0.3 although this value is based on offshore blowouts and is not directly applicable to Buncefield-type events.

134 The bulk of available literature on ignition probabilities is pre-Buncefield and is based on scenarios and circumstances that differ significantly from the Buncefield incident. This can in many cases make their adoption for Buncefield-type scenarios inappropriate. Therefore, a number of factors need to be taken into consideration when determining the probability of ignition for gasoline and other in scope substances. These include, but are not necessarily limited to the following:

- Size and duration of release – which may require an estimate of how long an overflow might persist before it is discovered, how big the cloud can get and how long it might take to disperse. In the absence of better information, the size and duration of release should be based on the Buncefield incident.
- Site topography, which can lead to a flammable cloud drifting either towards or away from an ignition source.
- The potential ignition sources present that could come into contact with the flammable cloud such as a vehicle, a pump house or a generator. This assessment should include any off-site sources within the potential flammable cloud.
- Immediate ignition is likely to produce a flash fire, delayed ignition may produce a flash fire or explosion.

135 The significance of area classification in preventing ignition should be considered carefully. While area classification will limit the likelihood of ignition of a flammable cloud in the zoned areas, it will not stop it completely (eg see section 1.6.4.1 of I*gnition probability review, model development and look-up correlations*[67] and section 8.1.3 of *A risk-based approach to hazardous area classification*[68]), and the type of release being considered in this report is outside the scope of conventional area classification practice. 'Classified' hazardous areas are defined by the probability of flammable or explosive atmospheres being present in 'normal' operations or when releases smaller than those at Buncefield occur due to equipment failure. Most major hazard releases would go beyond the 'classified' hazardous areas.

136 Even if a dutyholder chooses as a matter of policy to purchase Zone 2 minimum electrical equipment throughout their facility, this may not apply to every type of equipment (for example, street-lighting). Also, normal site layout practice may allow uncertified electrical equipment (such as electrical switchgear and generators), 'continuous' sources of ignition such as boilers or fired heaters, and hot surfaces, to be present close to Zone 2 boundaries, increasing the chance of ignition.

137 It is also possible that the operation of emergency response equipment (including switchgear and vehicles) may act as an ignition source. The operation of such equipment may be initiated directly or indirectly by the tank overflow and therefore cannot be assumed to be independent of the overflow event.

138 Where a more detailed estimate of ignition probabilities is required further information is given in the HSE's research report CRR203[69] and the Energy Institute's *Ignition probability review, model development and look-up correlations*. The assessment should take into account the spread of the cloud over the facility and its environs and should identify all credible sources of ignition within the area.

CM 3 – Probability of explosion after ignition

139 The reasons why the vapour cloud at Buncefield exploded as opposed to burning as a flash fire are not fully understood. The latest understanding is contained in the report 'Buncefield explosion mechanism Phase 1: Volumes 1 and 2 RR718 HSE Books 2009'. Factors such as ambient temperature; cloud size, shape, and homogeneity; congestion (including that from vegetation); droplet size; and fuel properties may have a significant effect on the probability of an explosion compared to a fire.

140 This conditional modifier is intended to represent such factors. However, there is insufficient information available at present to know which of the above factors, if any, are relevant to the probability of explosion. Nor is it clear whether commonly used generic probabilities of explosion (typically derived from onshore and offshore process data and applied to a wide range of leak sizes with some or no relationship to leak size) can be applied to the type of event considered in this report.

141 Given the present state of knowledge about the Buncefield explosion mechanism this report tentatively proposes that the value of this modifier should be taken as unity in the stable, low wind-speed, conditions that are the basis of this hazardous scenario. A much lower, and possibly zero, probability might be appropriate. It is possible that an improved understanding of the explosion mechanism may allow a better basis for determining the value of this factor in the future.

CM 4 – Probability that a person is present within the hazard zone

142 This conditional modifier can be used to represent the probability of a person being present in the hazardous area at the time of a tank overflow. Care should be taken with this conditional modifier to avoid double-counting factors which have already been taken into account elsewhere (eg in other protection layers or in the calculation of the consequence) and in particular to avoid double-counting any credit taken for evacuation (see paragraphs 118–122). The following occupancy factors may be appropriate for a given scenario:

- For workers at the facility (including contractors and visitors), it is legitimate to take credit if the normal pattern of work associated with the job role means that they would only reasonably be expected to be in the hazardous area for part of their time at work. For example, a worker may have a patrol route that means that they are outside the predicted hazardous area for part of their shift. Maintenance crews may work over a whole facility and may only be present in the hazardous area for a portion of the time they spend at work.
- Outside the facility, residential accommodation should be assumed to be fully occupied given that the hazardous scenario is assumed to happen during night-time conditions. Industrial and office facilities may only be occupied for a portion of the time, but care should be taken to include security, janitorial and cleaning staff who may be present outside normal hours.

143 Where individual risk is being considered, an additional factor can be applied to the occupancy to take account of the fact that the individual only spends part of the year in the work place and therefore there is a chance that if the hazardous event occurs the individual may not be at work and therefore is not exposed to harm. The equivalent factor for a scenario-based assessment would be if the job role being considered is only required on site for part of the year and at other times is not required.

144 Care needs to be taken in using this conditional modifier that it is truly independent of the initiating event, any enabling event or condition, or any protection layer. If normal tank-filling operations require the presence of an operator, or if part of the emergency response to an overflow event requires operators to investigate the incident, this conditional modifier will not be independent.

145 If night-time occupancy is used in the LOPA (see conditional modifier on stable weather), then a sensitivity analysis should be performed for daytime occupancy combined with the low probability of stable, low wind speed, conditions occurring during the daytime. Such an analysis would need to balance the factors such as increased exposed population and the higher probability that an overflow would be seen and remedial action taken to prevent an explosion.

CM 5 – Probability of fatality

146 This conditional modifier is often referred to as 'vulnerability'.

147 This conditional modifier may only be used if a single value can be specified for the hazardous scenario – most likely in an Individual Risk calculation. Otherwise it should be incorporated in the calculation of the consequence. The value to be used will have to be determined on a case-by-case basis.

CM6 – Probability of the environmental consequence

148 This conditional modifier is included to account for any factors additional to those considered elsewhere in the LOPA (eg seasonal factors, if not implicitly included in other factors within the LOPA) that may influence whether the hazardous scenario can cause the defined environmental consequence.

Completing the study of the scenario

149 The process should be repeated for the other scenarios as shown in Figure 22. It must be remembered that the resulting predicted unmitigated frequency of the overflow event is aggregated over all relevant initiating events. This sum, combined with existing control, protection and mitigation risk reduction factors applicable to each initiating event must be compared with the target frequency for the specified consequence defined in the risk tolerance criteria (see paragraphs 36–53).

150 It is important that a sensitivity analysis should be carried out to explore the sensitivity of the predicted risk levels to the assumptions made. It is important to be able to identify the key assumptions and to provide justification that the analysis is based on either realistic or conservative assumptions. Sensitivity of assumptions on initiating events and consequence side of a risk assessment are also required.

Concluding the LOPA

151 The conclusions of the LOPA should be recorded. The record should include sufficient information to allow a third-party to understand the analysis and should justify the assumptions made and the choice of values for parameters such as human reliability, equipment failure rates and conditional modifiers. Where assumptions are made about the mode of operation of the facility (such as the proportion of the time tanks are being filled, or the number of tanks on gasoline duty) these should be documented so that their continuing validity can be checked.

152 The LOPA should provide the basis for the safety requirements specification of the SIS (where required). This should include:

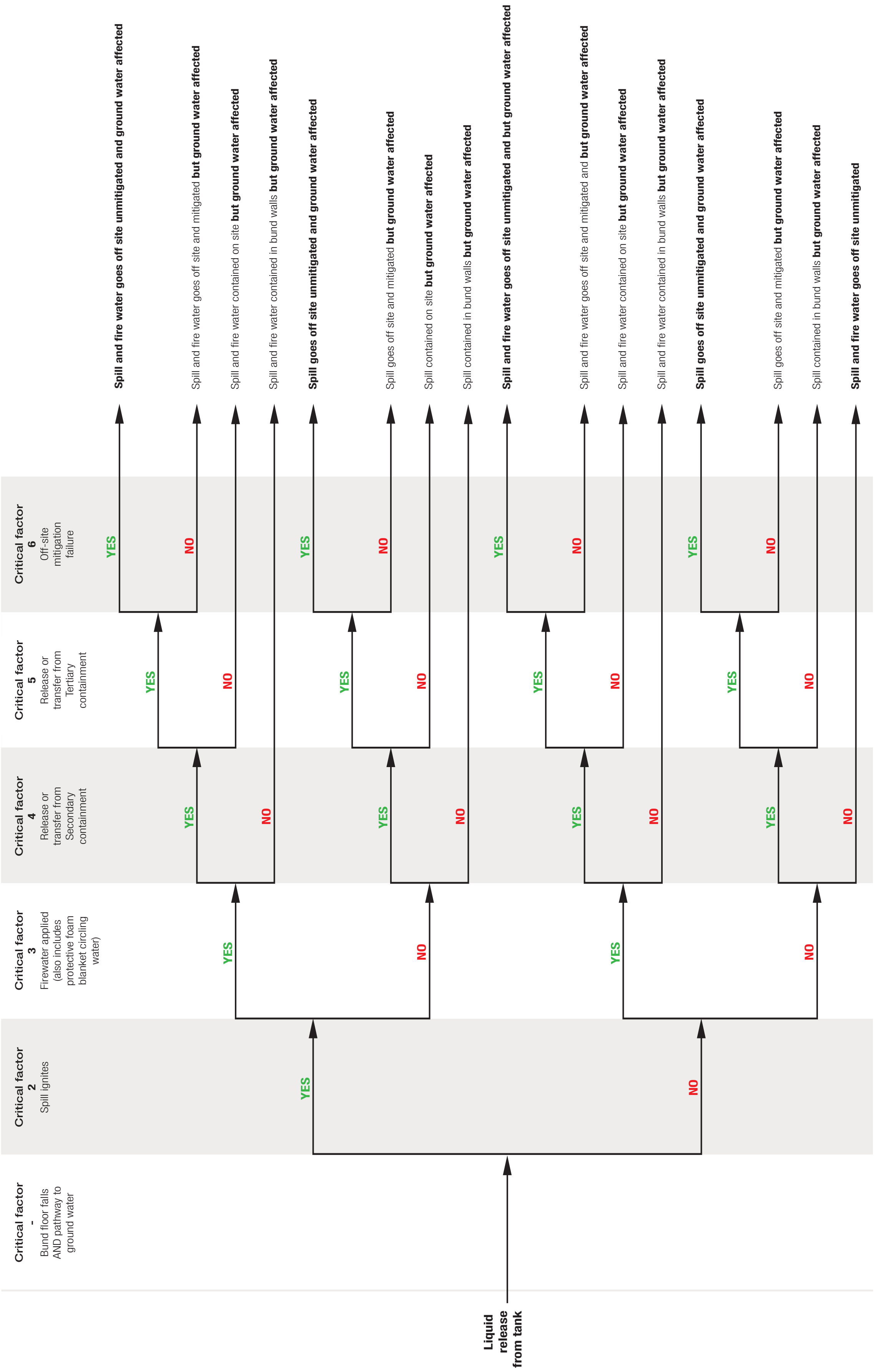
- clear definition of the SIL required for the safety instrumented system in terms of reliability level, eg PFD;
- it should also provide the basis of the functional specification of the SIS.

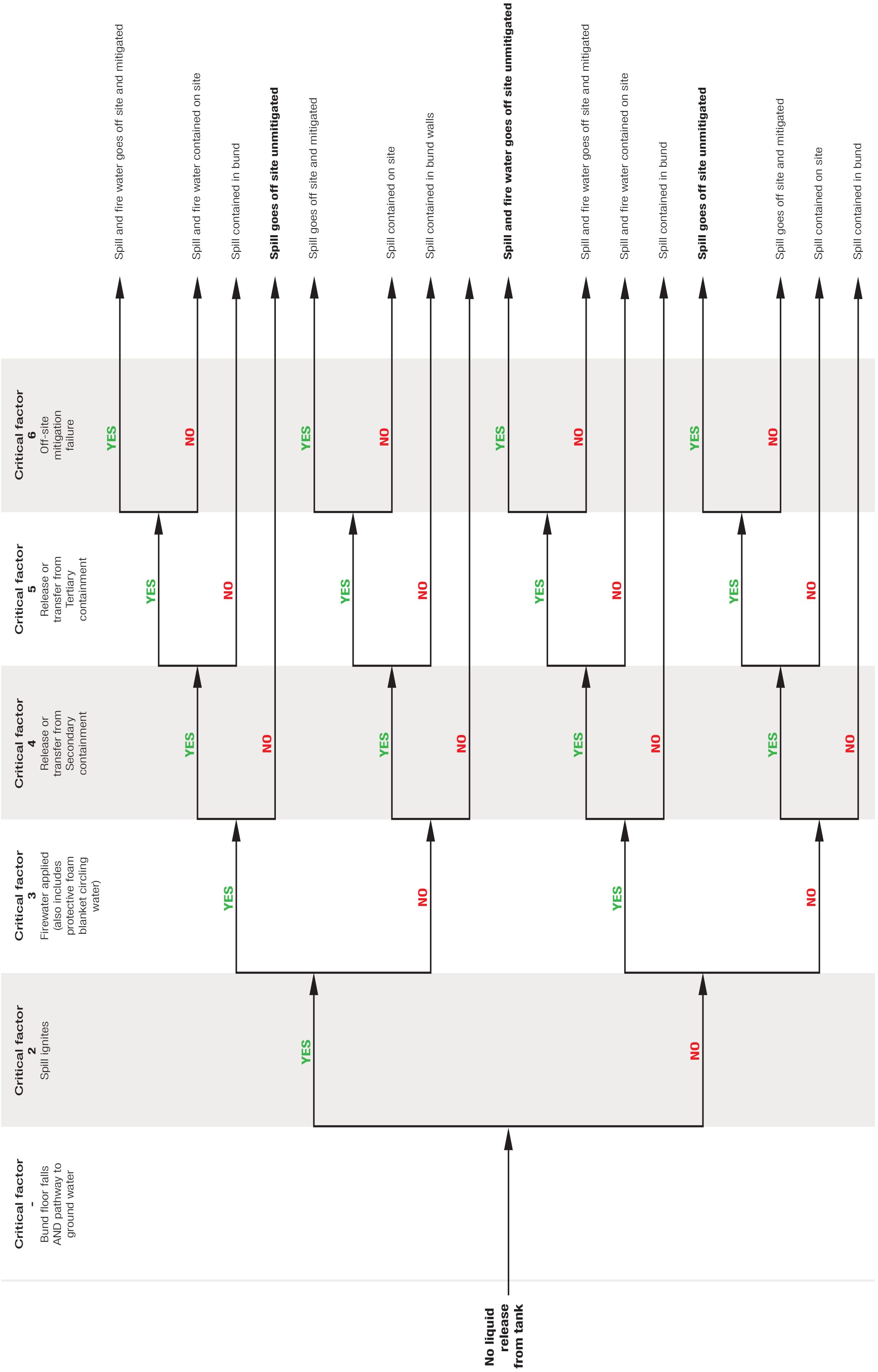
Annex 1 Summary of common failings in LOPA assessments for bulk tank overflow protection systems

153 HSE reviewed a number of early LOPA studies of overfill protection completed following the Buncefield incident (see RR716[70]). A number of errors and problems, listed below, were identified:

- human error probability too optimistic;
- independence of human operators (double counting of benefit from human tasks);
- risk factors due to the number of tanks on any particular site;
- little available data on ATG errors and failures;
- incorrect logic used to combine various factors;
- incorrect handling of number of filling operations;
- difficulty in analysing time at risk ie filling duration;
- uncertainty of ignition probability;
- uncertainty of probability of fatal injury;
- uncertainty of occupancy probability;
- uncertainty of probability of human detection of overflow;
- unjustified valve reliability;
- data not justified by site experience;
- no consideration of common cause failures of equipment;
- inappropriate risk targets;
- all hazard risk targets applied to single events;
- incorrect handling of risk targets eg sharing between tanks;
- difficulty in estimating probability of vapour cloud explosion; and
- difficulty in establishing and verifying all initiating events (causes).

Annex 2 Critical factors for environmental damage from a tank overflow


Critical factor
-
Bund floor fails AND pathway to ground water
Critical factor
2
Spill ignites
Critical factor
3
Firewater applied (also includes protective foam blanket circling water)
Critical factor
4
Release or transfer from Secondary containment
Critical factor
5
Release or transfer from Tertiary containment
Critical factor
6
Off-site mitigation failure
Liquid release from tank
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
Spill and fire water goes off site unmitigated and ground water affected
Spill and fire water goes off site and mitigated but ground water affected
Spill and fire water contained on site but ground water affected
Spill and fire water contained in bund walls but ground water affected
Spill goes off site unmitigated and ground water affected
Spill goes off site and mitigated but ground water affected
Spill contained on site but ground water affected
Spill contained in bund walls but ground water affected
Spill and fire water goes off site unmitigated and but ground water affected
Spill and fire water goes off site and mitigated and but ground water affected
Spill and fire water contained on site but ground water affected
Spill and fire water contained in bund walls but ground water affected
Spill goes off site unmitigated and ground water affected
Spill goes off site and mitigated but ground water affected
Spill contained in bund walls but ground water affected
Spill and fire water goes off site unmitigated


Critical factor
-
Bund floor fails AND pathway to ground water
Critical factor
2
Spill ignites
Critical factor
3
Firewater applied (also includes protective foam blanket circling water)
Critical factor
4
Release or transfer from Secondary containment
Critical factor
5
Release or transfer from Tertiary containment
Critical factor
6
Off-site mitigation failure
No liquid release from tank
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
YES
NO
Spill and fire water goes off site and mitigated
Spill and fire water contained on site
Spill contained in bund
Spill goes off site unmitigated
Spill goes off site and mitigated
Spill contained on site
Spill contained in bund walls
Spill and fire water goes off site unmitigated
Spill and fire water goes off site and mitigated
Spill and fire water contained on site
Spill contained in bund
Spill goes off site unmitigated
Spill goes off site and mitigated
Spill contained on site
Spill contained in bund

Annex 3 Demand tree methodology for systematic identification of initiating causes

154 The purpose of this annex is to provide an example of an outline methodology for the systematic identification of initiating events that can lead to hazardous events. This methodology can be used with any SIL determination (such as LOPA, fault tree analysis) or other techniques used for identification of the initiating events leading to a specific hazardous event.

Description of process example

155 Figure 24 shows the simplified schematic for part of a process sector plant. It has the incoming flow from the left, with a flow controller (FIC210) setting the flow rate into the separator vessel shown.

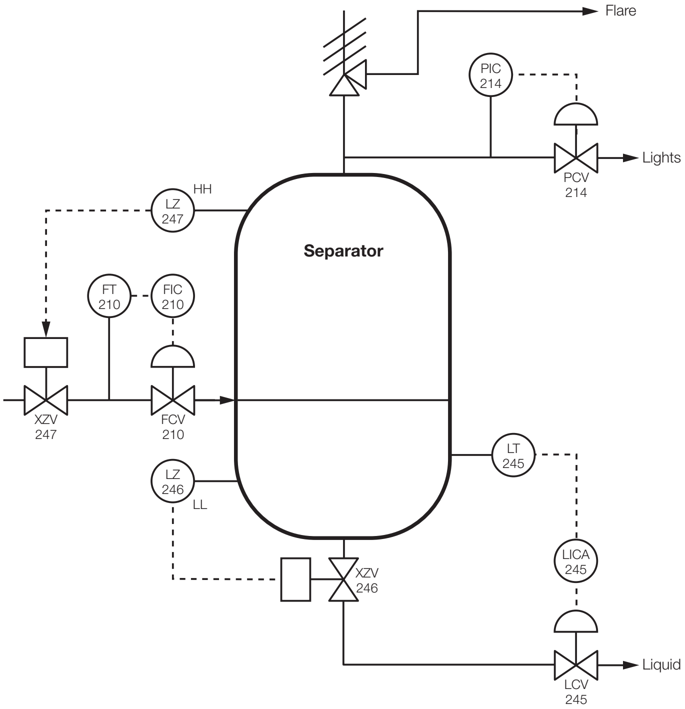


Figure 24 Simplified process schematic

156 The incoming flow is separated in the vessel into two streams: a light vapour phase, which exits the top of the vessel, and a liquid phase, which exits the bottom of the vessel. The liquid level in the vessel is maintained by the level controller (LICA245) that adjusts the liquid flow out of the vessel. The pressure in the vessel is maintained by a pressure controller (PIC214) in the vapour line. Over-pressure protection is provided by a pressure relief valve on the top outlet from the vessel.

157 Two instrumented protective measures are shown: (a) a low level trip (LZ246) protects against loss of level in the vessel and vapour entering the liquid line and (b) a high level trip (LZ247) which protects against liquid entering the vapour line.

158 The specific process concern in this example is associated with an uncontrolled high level in the vessel and the consequences that would result from that. Detailed consequence analysis is not necessary for illustration of the method for demand identification and so for the illustration the hazardous event will be taken as ‘high level in the separator with flow into the vapour line’.

Methodology 'rules'

159 The use of this methodology requires the application of some simple rules:

- No protective measures, which would protect against the hazardous event of concern, are considered at this stage. That is to say in this example, no alarms, trips or interlocks or actions protecting against high level.
- Thinking is not limited to the diagram boundary but is extended as required beyond what is on the diagram.
- All modes of operation are considered: (a) normal operation, (b) start-up, (c) shutdown, etc.

160 The hazardous event is put at the top of a page and the initiating events (demands) are then developed in a systematic manner by asking the question 'how?' at each level of detail.

Mode of operation

161 When developing the demand tree and considering the question 'how?' it is important that the different modes of operation are reviewed for failures that could lead to the hazardous event. Table 11 may be used as a prompt to assist the systematic process.

Table 11 Modes of operation and initiating events

Mode of operation	Class of initiating event			
	Equipment failure	Failure of services	Human failure	External events
Normal operation				
Start-up				
Shutdown				
Abnormal modes				
Maintenance				

162 In Table 11 services could include any or all of the following:

- Loss of electrical power.
- Loss of steam.
- Loss of instrument air.
- Loss of cooling water.
- Other.

Example demand tree

163 Figure 25 shows an example demand tree. The top of the demand tree is the hazardous event of concern. This is expressed as clearly and precisely as possible to assist with development of the rest of the tree.

164 The next level down may relate to modes of operation (eg start-up, shutdown, normal, catalyst regeneration etc) or composition ranges (eg 'high' ethylene, 'high' methane, 'high' hydrogen concentration etc). The important requirement at this level is to keep the description as generic as possible so that it can be developed in more detail further down the tree.

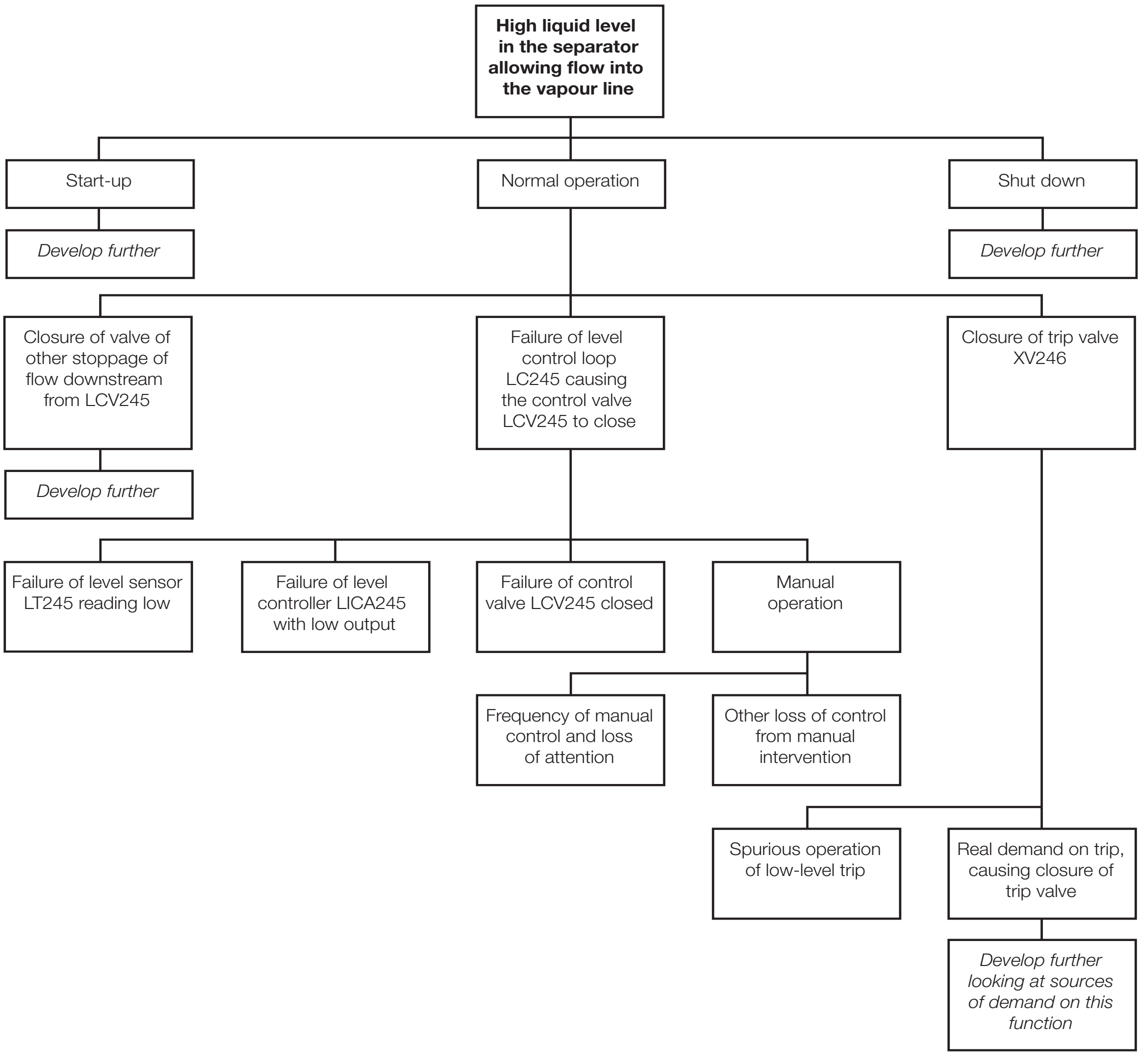

High liquid level in the separator allowing flow into the vapour line
Start-up
Normal operation
Shut down
Develop further
Develop further
Closure of valve of other stoppage of flow downstream from LCV245
Failure of level control loop LC245 causing the control valve LCV245 to close
Closure of trip valve XV246
Develop further
Failure of level sensor LT245 reading low
Failure of level controller LICA245 with low output
Failure of control valve LCV245 closed
Manual operation
Frequency of manual control and loss of attention
Other loss of control from manual intervention
Spurious operation of low-level trip
Real demand on trip, causing closure of trip valve
Develop further looking at sources of demand on this function

Figure 25 Demand tree illustration

165 The tree is developed to a level of detail at which the initiating events (demand failures) can have some frequency assigned to them.

166 It is very important that protective measures do not appear on the demand tree. This has at least three benefits: (a) there is clarity of thinking without the complication of worrying about the protective measures, (b) you get a smaller diagram and (c) it helps you to consider the causal failures on a wider basis and may include some for which there are no protective measures.

Next stages

167 Having identified a number of initiating events, the demand tree can be used as an input to other analysis techniques to carry out a more detailed risk assessment. This further stage would typically use either a fault-tree analysis or a layer of protection analysis (so long as the LOPA methodology used has sufficient flexibility to treat each cause separately and then combine them when assessing the frequency of the hazardous event).

Annex 4 Discussion of ‘time at risk’

168 The concept of ‘time at risk’ is used to account for periodic, discontinuous, operations. Where operations are essentially continuous, the hazards associated with the operation will be present continuously. In contrast, where operations are carried out as batch operations, the hazards associated with the batch operation will only be present while the batch is being carried out.

169 This discussion of time at risk relates to the context of tank filling operations. The context assumes that the storage facility is operational throughout the year and that periodically during the year tank filling occurs.

Failure of equipment

170 During the tank filling operation, there is reliance on items of equipment such as a tank level measurement gauge. Failure of the gauge is one of the potential initiating causes of over filling.

171 For the purpose of this example, failure of the gauge is assumed to be possible at any time, whether the tank is being filled or not. It is also assumed that the fail-to-danger rate of the gauge is a constant, whether the tank is being filled or not (and therefore that failures of the transmitter head or servo-mechanisms may occur with equal likelihood at any time). **Note that this assumption may not be true for all failure modes and would need consideration on a case-by-case basis.**

172 Figure 26 shows the storage facility as operational throughout the year. It also shows one period of tank filling. This is to make the diagram easier to follow. However, the line of argument will still apply to the situation of multiple tank filling periods during the year.

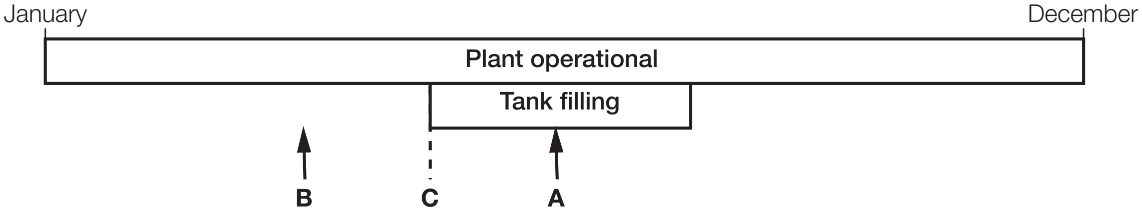


Figure 26 Equipment item failure

173 It is assumed that failure of the level gauge can occur at any time. If it occurs at time A, then it can clearly affect the control of the filling operation. If it occurs at time B then it can only affect the filling operation if it is not detected before tank filling starts at time C and the filling operation proceeds with a faulty gauge.

174 If detection at time C is carried out with a high degree of reliability by some form of checking operation (eg independent gauging or stock checks) then it can be assumed that only gauge failures that occur during tank filling can affect the filling operation. The checking activity fulfils a similar function in this case to a trip system proof-test.

175 If the failure rate of the level gauge is λ per year and the total duration of filling during a calendar year is t hours, then the proportion of time (there being 8760 hours in a year) for which failures are significant is t/8760. This proportion of time may be used with the failure rate to calculate the rate at which failures occur during the tank filling operation. This is then λ x t/8760 in units of per year.

Human failure

176 Another potential cause of over filling is some form of human failure. This can be associated with a failure to control the filling operation or failure to select the correct tank or one of a number of other possibilities, depending on the details of the operation and what tasks people are involved in carrying out.

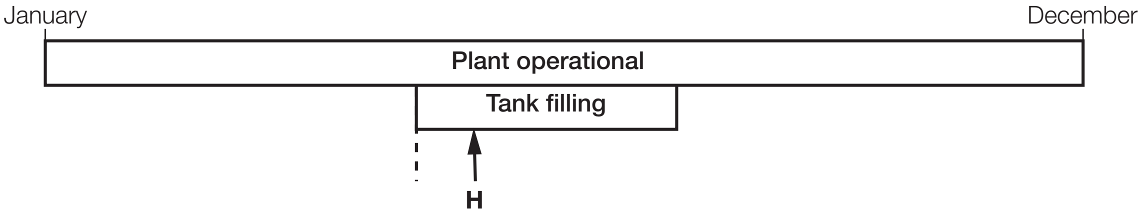


Figure 27 Human action

177 The human task of controlling the filling operation to stop at the intended level is represented in Figure 27 by the letter 'H'. This task by definition only occurs when the tank is being filled. Therefore, the opportunity for the error of allowing the tank to overflow can only occur while the tank is filling. This means that as the task is directly associated with the time when the filling operation occurs, the concept of time at risk does not apply. The occurrence of the filling operation and the possibility of error are not independent but are linked.

178 Note that an important distinction between human failure in carrying out a task and the failure of equipment described is that human failure is characterised by a probability per event (and is therefore dimensionless). Equipment failure is characterised by a failure rate (typically with dimensions of (per year)).

Conclusion

179 Thus there is the generalisation, that 'time at risk' (the proportion of the year for which the filling operation is happening) is relevant to equipment failure that can occur at any time during the year – subject to the caveat of detection of any failure that occurs prior to the filling operation before it causes over filling. Conversely, for any failure such as human error that is directly related to a task that only occurs in relation to the tank filling operation, then the 'time at risk' factor should not be used.

Annex 5 The BPCS as an initiating event and as a protection layer

180 The authoritative requirements and guidance on initiating events and the independence of BPCS-based layers of protection are given in BS EN 61511. The CCPS guidance on LOPA presents two approaches for the application of LOPA. Approach 'A' generally meets the requirements of BS EN 61511. The following guidance emphasises that the normative requirements for assessing independence are those described in BS EN 61511 and that this guidance is intended to indicate the issues involved in making such an assessment.

181 In a simple LOPA using a conservative approach, unless there is complete independence in how basic process control functions are implemented through the BPCS, no credit can be taken for any risk reduction provided by a control or alarm function implemented through the BPCS as a protection layer if a BPCS failure also forms part of an initiating event. However, this conservative approach may be relaxed if it can be demonstrated that there is sufficient independence to allow credit to be taken for both. This issue is discussed in Sections 9.4 and 9.5 of BS EN 61511-1 and BS EN 61511-2. The reader is referred to these sources for a more detailed discussion. Systematic factors such as security, software, design errors and human factors should also be considered.

Programmable electronic systems

182 Credit can be given to more than one control function implemented through the BPCS where there is sufficient rather than complete independence between each function. With regard to any programmable electronic systems that are part of the BPCS the following requirements, which may not be exhaustive, should be met.

- There should be formal access control and security procedures for modifying the BPCS. The access control procedures should ensure that programming changes are only made by trained and competent personnel. The security procedures should prevent unauthorised changes and should also ensure software security, in particular by minimising the potential to introduce a virus to infect the BPCS.

- There should be an operating procedure which clearly defines the action to be taken if the control screen goes blank, a workstation 'freezes', or there are other signs that the programmable device has stopped working correctly during a filling operation.
- A back-up power supply should be available in case the main power supply is lost. The back-up system should give a clear indication when it is being used. The capacity of the back-up supply should be sufficient to allow emergency actions to be taken and these actions should be specified in a written procedure. The back-up power supply must be regularly maintained in accordance with a written procedure to demonstrate its continuing effectiveness.
- The sensors and final elements should be independent for credit to be given to more than one control function. This is because operating experience shows that sensors and final elements typically make the biggest contribution to the failure rate of a BPCS.
- BPCS I/O cards should be independent for credit to be given to more than one control function unless sufficient reliability can be demonstrated by analysis.
- The credit taken for control and protection functions implemented through the BPCS should be limited to no more than two such functions. The following options could be permitted:
  - If the initiating event involves a BPCS failure, the BPCS may only then appear once as a protection layer – either as a control function or as an alarm function, and only if there is sufficient independence between the relevant failed BPCS control or protection functions.
  - If the initiating event does not involve a BPCS failure, the BPCS may perform up to two functions as protection layers (eg a control function and an alarm function) so long as other requirements on independence are met.
- Claims for risk reduction achieved by the BPCS should meet the requirements of BS EN 61511-1 and 61511-2 (eg clauses 9.4, 9.5 and 11.2).

183 Figure 28 illustrates what the application of these principles could require in practice.

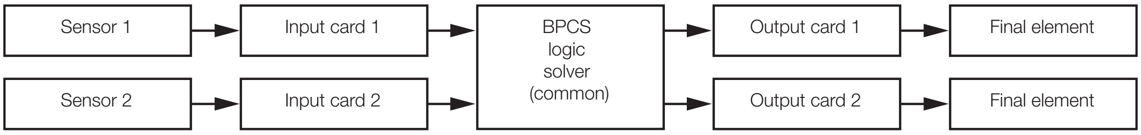


Figure 28 Possible structure of sufficient independent control functions within the BPCS

184 Where credit is taken for more than one function being implemented through the BPCS, this should be supported by a detailed analysis and the analysis should form part of the LOPA records. Determination of the degree of independence between two functions that share a common logic solver, as depicted in Figure 28, is not a trivial task and great care should be taken not to underestimate the level of common cause, common mode and dependent failures. Where an operating company considers that they cannot support the level of analysis required, the BPCS should be limited to a single function in the LOPA. It should be noted that some operating companies preclude taking credit for more than one function from the same logic solver as a matter of policy.

185 Where the implementation of two functions involves a human operator there is evident potential for a common cause failure due to human error affecting the performance of both functions. This may have an impact on whether any credit can be taken for any protection layer involving the operator if an error by the same operator is the initiating event.

186 The simplest and most conservative approach is to assume that if an error made by an individual is the initiating event, the same individual cannot be assumed to function correctly in responding to a subsequent alarm. Therefore, if human error is the cause of failure of a BPCS credit cannot then be taken for the same individual responding correctly to an alarm. This approach is equivalent to taking no credit for error-recovery even if suitable means of error recovery can be identified.

187 A more complex approach would attempt to identify and quantify the possibility of error recovery. This approach would need to consider the type of error causing the initiating event, the information and systems available to warn of the error, the effectiveness of the warning systems in

helping the diagnosis of the error and the time available for diagnosis and recovery before effective recovery is impossible. Where credit is taken for error recovery, this should be supported by detailed analysis by a person competent in appropriate human reliability assessment techniques.

Annex 6 Cross-checking

Discussion

188 Many tank-filling operations include a number of cross-checking activities as part of the operation. These may include checks before the transfer starts (eg routing valve line-up, tank dips, available ullage) and periodic checks during the filling operation (filling rate, tank dips, unusual behaviour of instruments).

189 The risk reduction that can be claimed for checking activities varies greatly with the kind of check being carried out. Experience shows that the risk reduction due to checking is frequently not as great as might be expected. Operators asked to 'check' each other may be reluctant to do so, or the checker may be inclined to believe that the first operator has done the task correctly because they are known to be experienced. Therefore the intended independence of the checking process may not in fact be achieved.

190 This report distinguishes between self-checking activities and those carried out by a third party. Self-checking activities, such as those carried out by the operator responsible for monitoring the filling operation, should be considered as part of the basic reliability of the operator in carrying out the filling operation and hence included in the risk reduction claimed for that activity. The extent and nature of the self-checks may legitimately be considered a factor in the reliability claimed, but they would not warrant separate identification, and hence a claim for risk reduction, within the study unless an error recovery assessment is performed and fully supports any claims made.

191 Third party checks, which may offer risk reduction include: third party verification of tank dips prior to transfer; verification of tank dips for customs purposes. Supervisor verification of valve line-ups prior to transfer may suffer from similar dependencies to that of a second operator as described above. The following guidance applies under these circumstances.

General requirements

192 It can be claimed that an 'independent' cross check will affect the frequency of the initiating event and the demand on any layer of protection if the cross check can be shown to be a formal requirement of a standard operating procedure and the cross-check is:

- independent;
- effective; and
- proper auditable records kept.

193 Note that management system and standard operating procedures cannot be claimed as a protection layer in their own right. On their own, procedures do not meet the requirement of effectiveness for a protection layer because they cannot identify a hazard or perform an action. Instead, procedures are incorporated in the performance claimed for a protection layer because they define requirements for the conduct of activities and therefore are included implicitly rather than explicitly within the analysis.

194 An important task for a LOPA team is to distinguish between those checks that are formally required and those that are carried out as a matter of custom and practice. Checks which are not part of a formal procedure cannot be considered to offer significant risk reduction. For example, where field operators carry out informal checks on tank levels from time to time, the check cannot be considered a valid cross-check because there is no formal requirement to carry it out even though it may offer some risk reduction. Additionally, they may vary over time without requiring any change control.

195 It will also be necessary for the LOPA team to review the checking activities in detail to confirm exactly what is done and how, compared with the requirements of the procedure. Where the procedure requires something to be confirmed visually, the team should verify that this actually happens, as opposed to the checker relying on what they are told by the person carrying out the task.

196 The LOPA team need to be alert to hidden dependencies between the person carrying out the task and the person checking. For example, the visual confirmation that a specific valve has been closed may correctly verify that a valve has been closed, but not necessarily that the correct valve has been closed. The checker may implicitly have relied on the person carrying out the task to select the correct valve.

Quantifying the benefit from checking

197 The key to appropriate checking is the identification of what error is to be highlighted by the check and the action that is taken following identification of the error. The analyst must ask the question 'If the person who has carried out the original action has not spotted the error, what is the justification that the person checking will be able to spot the error?'

198 For example, when considering a check on opening a manual valve, there is a need to consider each of the types of error separately; this is because the validity or benefit of checking is likely to be different for each type of error.

199 The error may be:

- omission of valve opening;
- opening the wrong valve;
- only partially opening the correct valve;

200 For the error of omission, the LOPA team need to ask the question as to whether the checker will even be requested to check that the valve has been opened. Review of the procedure may reveal that the checking part may be triggered by the completion of the original action. Hence with an omission checking may not occur and so a claim for checking would not be appropriate.

201 For the error of opening the wrong valve, the LOPA team need to ask the question as to how the checker knows which valve is to be checked. If the actual procedure involves the person carrying out the original action telling the checker which valve is to be checked, then again a claim for checking would not be appropriate. Equally if the checker uses the same information source as the person carrying out the original action and an error in that information is the cause of the original error, then the checker can be expected to make the same error as the person carrying out the original action; the check has no benefit.

202 For the failure to open fully the valve, then the question arises 'what is it that will alert the checker to the error and yet it was not able to alert the person carrying out the original action?' Again the LOPA team needs to question whether the checker can see anything different from the person carrying out the original action. If there is nothing that the checker will be able to see differently, it is difficult to justify that there is any risk reduction benefit from the checker.

203 There is another aspect in which checking needs careful thought. If the person carrying out the original action knows that there will be checking, then there is a possibility that there may be a level of reliance on the checker: the person carrying out the original action may take less care, secure in the belief that any errors will be detected and corrected by the checker.

204 Making risk reduction claims for checking requires clear written discussion to say what is being checked and how the checker will be successful when the person carrying out the original action has not been successful.

205 Table 12 suggests some levels of checking to consider. The first level of checking would give a low level confidence in the effectiveness of the cross check and the last level of checking in

Table 12 would give a higher level of confidence in the effectiveness of the checking. No figures for the probability of error are given because these should be determined and justified on a case-by-case basis by a specialist in human error quantification.

Table 12 Levels of cross-checking effectiveness

Level of dependency	Level of checking
Complete	No justifiable reason why the checker should identify the failure when the person carrying out the original action has not.
High	The checker can determine the correct course of action independently of the first person. However, checker either has a common link with the first person or there is good reason to believe that the checker will make the same error as the first person.
Moderate	Checker has a weak link to the first person or there is moderate likelihood that the checker will will make the same error as the first person.
Low	Checker has sufficient independence from the person carrying out the original action and the check is designed to highlight errors that may have occurred.

206 **If in doubt, or if a suitable justification cannot be given, no claims should be made for risk reduction due to checking**.

Annex 7 Incorporating human error in initiating events

Identification of potential human error

207 The first step is to identify which tasks are critical tasks in relation to the overflow event. In this context, a critical task is one in which human error can trigger a sequence of events leading to an overflow. The identification of critical tasks is best achieved during the development of a demand tree, as described in Annex 3.

208 When doing so, there should be coverage of all modes of tank operation: filling, emptying, maintenance, transfers, and any other abnormal modes of operation etc. A 'critical (human) task list' can then be created. Table 13 shows an example.

Table 13 An example 'critical (human) task list'

Mode of operation	Task	Potential adverse outcome
Transfers between tanks	Opening manual routing valve between the transfer pump discharge and a designated receiving tank	Opening the wrong valve and thereby transfer to the tank under review which has too little ullage and causing the tank to overflow

Review of each critical task

209 For each critical task it is important to gain a good overview of the task and its context. There are a number of task analysis techniques that can be used.

- Create a timeline with input from a person who does the activity.
- Review timeline against operating instructions and process engineering input for anomalies.
- Consider creating a hierarchical task analysis for the activity to identify the key tasks.

210 This is followed by a review of the key tasks to identify the potential errors within each task that could lead to the hazardous event under consideration. Techniques for this include (among others):

- Tabular Task Analysis.
- 'Human HAZOP'.

The output of this can be summarised in a critical task list (Table 14):

Table 14 Critical task list

Critical activity and/or task	Nature of the error leading to the hazardous event of tank overflow	Performance shaping factors relating to the task that could influence the probability of error
Opening manual routing valve between the transfer pump discharge and a designated receiving tank	Opening the wrong valve and thereby transfer the tank under review	– Poor labelling of valves – All communication by single channel radio from the control room – Significant proportion of new process operators with little on-site experience

Human error probability assessment

211 Figure 29 illustrates the process of assessing the human error probability (HEP) for the critical task or key step within the task.

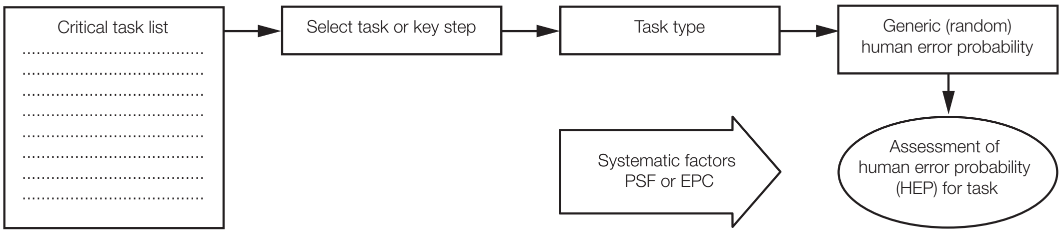

Critical task list
Select task or key step
Task type
Generic (random) human error probability
Systematic factors PSF or EPC
Assessment of human error probability (HEP) for task

Figure 29 Process for assessing human error probability

212 The steps in the assessment process are as follows:

- Select an appropriate 'generic' human error probability, based on the task type and/or the nature of the error.
- This human error probability could then be modified based on the performance shaping factors or error producing conditions relating to the people carrying out the task and the conditions under which they are working.

213 There are a number of standard methods such as APJ (Absolute Probability Judgment), HEART, THERP etc to assess the potential error probability. However, these require a level of training and specialist understanding to use and those new to the assessment of human error probability should seek assistance.

Initiating event frequency calculation

214 The frequency for each human initiating event is based on two parameters:

- Task frequency (/yr).
- HEP – as assessed using an appropriate method or selected from a table of generic task error probabilities, with suitable account taken for any conditions that could impact on the operator's ability to consistently and reliably perform their task, eg error producing conditions used in the HEART method.

215 For each human initiating event, the initiating event frequency would be calculated by:

Initiating event frequency (/yr) = Task frequency (/yr) x HEP

For example, a task carried out once a week, with an assessed human error probability for a specific error of 0.01; the initiating event frequency can be calculated:

Initiating event frequency (/yr) = Task frequency (/yr) x HEP
= 52 x 0.01
= 0.52 per year

Note that enabling events or conditions can be included in the task frequency (the number of times the activity is carried out under operational conditions which could lead to the undesired consequence) and do not require separate identification.

216 For initiating events, the error probability should be conservative.

Annex 8 Response to alarms

217 When considering the alarm function as a protection layer it is helpful to have a mental model along the lines of that shown in Figure 30.

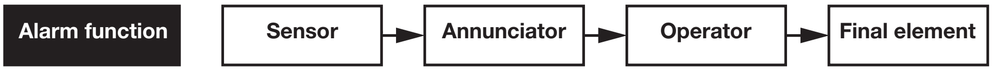


Figure 30 Alarm function

218 This shows four elements: the sensor, the annunciator, the operator and the final element. For complete independence, each of these four elements must be different from those used by other protection layers and from the initiating event for the hazardous scenario in question. Should any of these elements not be independent for the situation being considered then the alarm function should not be included in a simple LOPA analysis.

219 Where there is some commonality of elements between the alarm function and the initiating event or other protection layers, inclusion of the alarm function should be supported by a more detailed analysis. Typically this will require that an initiating event caused by the BPCF is broken down into individual failures of the constituent elements. Credit for the alarm function could only be claimed if there is a means of carrying out the function which is independent of the failed component, and if the person carrying out the function has sufficient knowledge, time and training to carry out any tasks correctly. The factors outlined below for operator response need to be considered.

Definition of the required performance of the alarm function

220 Before proceeding with the analysis of the performance of the alarm function, the required function should be carefully defined. It is not enough simply to identify an instrument and consider that as a protection layer. The protection layer will need to make up a complete loop and should therefore include:

- the operator who is to respond to the alarm;
- the means by which the alarm situation is detected and communicated to the operator; and
- the means of making the situation safe in the available time, given that this cannot include the equipment which has been assumed to have failed.

Operator response

221 Operator response to an alarm contains four sub-tasks as illustrated in Figure 31.

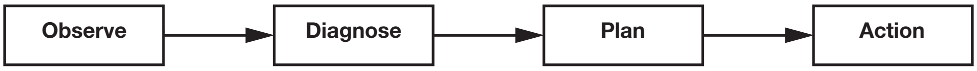


Figure 31 Sequence of operator sub-tasks

- **Observe:** The first of these sub-tasks, observing the indication, is relatively quick to do, so long as an operator is present to hear or observe the indication. However, it does rely on the indication of the alarm being clear and not being hidden by other alarms or information being communicated at the same time. Any assessment of reliability of this sub-task depends on a review of the human-instrumentation interface and the potential for confusion or masking of the key information. It also needs to consider how the alarm is prioritised because this will influence the importance that the operator attaches to the response.
- **Diagnose and plan:** Diagnosis of the problem and planning what to do are two closely coupled sub-tasks. The time required for these sub-tasks will depend on the situation, the clarity of any procedures or instructions given on the correct response, the training of the operator, and how well practised and easy the required response is within the time available. If the operator has not met the situation before – and this may be the case on a well-run facility – it is possible that the operator will not be familiar with the correct response unless the scenario is covered by regular training or by periodic drills or exercises. Where the operator may not be able to make a decision on the correct course of action without referring to a supervisor, caution should be taken before claiming any credit for the alarm function.
- **Action:** Carrying out the necessary action could be a relatively quick thing to do (such as closing a remotely operated valve) or it could require the use of a radio to reach another operator who is then required to go to a specific part of the plant to operate a manual valve.

Time for response

222 The key consideration relating to ‘time for response’ is an understanding of the actual time available from when the alarm is activated until the process goes ‘beyond the point of no return’. This is illustrated in Figure 32.

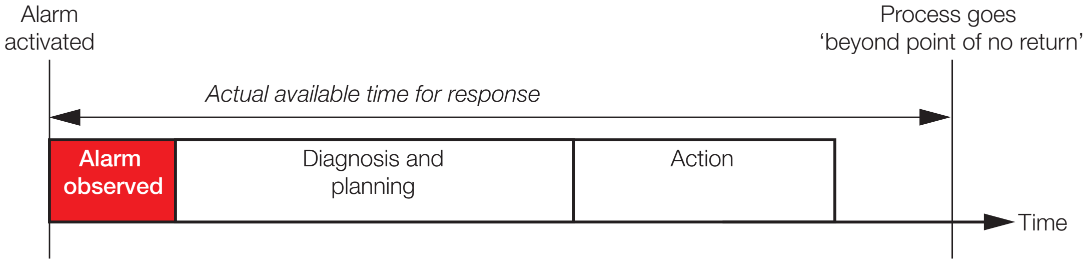


Figure 32 Time for response to alarm

223 All four sub-tasks must be able to be completed effectively within this time. Shortage of time available is one of the key factors that influence the probability of failure for operator response. (See HEART methodology.)

224 The actual total time available for response (see Figure 32) should be evaluated on a case by case basis taking into account all the relevant circumstances of the installation, for example distances, means of taking action and operator experience.

225 It is important that the issue of worst-case time needed is considered. In many instances, the LOPA team will consider it obvious what the response should be and feel that minimal time is required for successful action. However, thinking about the less experienced operators, those new to the operation, and even the experienced operators who have not seen this particular alarm before, should trigger a more considered view of what length of time could be required for overall success.

Probability of failure

226 For a non-SIL alarm function (in this context, a function that does not conform to the requirements of BS EN 61511-1 for a safety instrumented function) an overall PFDavg of no less than 0.1 (see BS EN 61511-1 Table 9) may be used. If, however, there is a view that there could be some increased time pressure on the operators, or other factor making the task conditions less favourable then a higher overall probability of failure may be considered. Note that a component of the protection layer may have a PFD lower than 0.1, but when combined with the rest of the system, it cannot result in an overall PFD lower than 0.1.

227 Any claim for a PFDavg less than 0.1 for an alarm function would by definition mean that it is a SIF and must meet the requirements of BS EN 61511. This would require formal assessment to demonstrate conformance to the requirements of BS EN 61511-1 for SIL 1. The human component of that SIF would need to be included within the assessment using a recognised method for human error probability prediction covering each of the four sub-task elements: ‘Observation’, ‘Diagnosis’, ‘Planning’, and ‘Action’; this is a specialist activity.

228 One method for calculating the overall PFDavg for the Alarm Function is as follows:

$$\textbf{PFDavg}_{\text{(Overall)}} = \textbf{PFDavg}_{\text{(Sensor to Annunciator)}} + \textbf{PFDavg}_{\text{(Means of Action (including final element))}} + \textbf{HEP}_{\text{(Observe)}} + \textbf{HEP}_{\text{(Diagnosis)}} + \textbf{HEP}_{\text{(Planning)}} + \textbf{HEP}_{\text{(Action)}}$$

For each hardware assessment of PFDavg, there should be some consideration of dependent failure (ie common cause or common mode types of dependent failure) with other layers. For each of the human error probability assessments there should again be some consideration of dependent failure. Further guidance on this may be found in *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* NUREG/CR-1278.[71]

Additional notes

229 PSLG support the recommendation of EEMUA 191[72] in that it considers that SIL 2 or higher cannot be claimed for a SIF that includes operator response. (EEMUA 191 table 5, p14.)

230 If an alarm protection layer is not a complete (ie having all four elements shown in Figure 31) and fully independent layer (satisfying the requirements of not sharing elements with the initiating event or other protection layers), the simplest approach is to be conservative and not to claim any risk reduction for the alarm layer. If the analyst wishes to include partial sharing between protection layers, this should be carefully substantiated (eg by using fault tree analysis to model the actual arrangement).

231 For any alarm function, the following factors should be addressed:

- the correct response is documented in operating instructions;
- the response is well-practised by operators;
- the alarm sensor is independent from the initiating event and other protection layers;
- the operator uses action independent from initiating event and from other protection layers;
- an operator is always present and available to respond to the alarm;
- the alarm is allocated a high priority and gives a clear indication of hazard;
- the alarm system and interface is well designed, managed and maintained so that it enables the operator to detect a critical alarm among potentially many other alarms;
- any analysis should bear in mind that under emergency conditions, the probability of failure could foreseeably deteriorate further.

232 Further guidance may be found in EEMUA 191.

AEL

AMSTERDAM PROCESS SAFETY SEMINAR SERIES

LESSONS LEARNED FROM THE BUNCEFIELD INVESTIGATION

March 2–3, 2010 | Amsterdam

LESSONS LEARNED FROM THE BUNCEFIELD INVESTIGATION

The Process Safety Leader Group Final Report, issued 11.12.2009 on site safety at fuel storage sites What can we learn from it?
One year after the Buncefield Investigation Board issued its final report and four years after the Buncefield accident, the Process Safety Leader Group issued its final report: 11.12.2009. The lessons learned in this report go beyond the site safety at fuel storage sites. It contains recommendations valid for those sites, but also very useful for chemical plants. This is an early opportunity to hear first hand the lessons learned from the participants of this Process Safety Leader Group and other persons directly involved in the Buncefield accident and its investigation. This seminar is a great learning opportunity!

Reasons to attend

- Learn first hand the latest lessons learned from key members of the Process Safety Leader Group
- Review the lessons learned based on the final report of the Buncefield Investigation Board
- Learn what are the practical consequences for fuel terminal management
- Learn the latest insights about the explosion mechanism, to be able to review: can this happen to us?
- Human Factors: what are reasonable assumptions for human intervention, what not?
- Instrumented systems: how reliable are they? How can they fail? How to ensure reliability? How to ensure Safety Integrity Level (SIL)?
- The Emergency Response to the Buncefield accident
- Lessons Learned: how can we improve on management of operations and people?
- Layer Of Protection Analysis (LOPA), how can it be applied to fuel storages, chemical plants and other types of operations?
- How can the Lessons Learned from Buncefield be applied to my operations?
- Learn about the effect of Buncefield on UK Land Use Planning

During the event there will ample opportunity for debate and feedback during the breaks, workshops and panel discussions.

The Amsterdam Process Safety Seminar Series is endorsed by the European Process Safety Centre (EPSC) and the Dutch Association for Safety Science (NVVK).

AEL is non profit organisation.

Who should attend

Tank Farm Managers, Process Plant Managers, Site Managers, Safety and Risk Professionals, HAZOP Leaders, Process Engineers, Mechanical Engineers, Project Managers, Process Control & Instrumentation Engineers, Risk Managers, Safety Managers, Maintenance Managers, HSE Directors. Business and operations leaders accountable for storage, transportation and distribution of flammable materials.

nvvk
veiligheidskunde

An AIChE Technology Alliance
CCPS
Center for Chemical Process Safety

epsc
EUROPEAN PROCESS SAFETY CENTRE
CENTRE EUROPÉEN DE SÉCURITÉ DES PROCÉDÉS
EUROPAISCHES ZENTRUM FUR ANLAGENSICHERHEIT

EHSQ Elite

Day 1
TUESDAY, 2 MARCH, 2010

In the Chair: Richard Gowland, Technical Director, European Process Safety Centre

9.00 Registration and Coffee

9.30 **Welcome and Introduction to the Subject**

9.40 **The Bu ncefield Incident. Fire and Explosion**
Technical Director Richard Gowland,
European Process Safety Centre

10.10 **Human Factors initiating the event**
Dr. Alan King, ABB, UK

10.55 Coffee

11.15 **Equipment failures**
Managing Director Dave Ransome, P & I Design Ltd.

The level gauge for Tank 912 recorded an unchanged reading. However, filling of Tank 912 continued.

The protection system which should have automatically stopped the transfer, preventing further filling, didn't operate.

11.45 **Assessment of damage from severe low lying vapour cloud explosions**
Dr. Technical Director Kees van Wingerden, GexCon AS

Damage to buildings and other structures. Decay of overpressure outside the edge of the cloud. Practical methods of risk assessment.

12.45 Lunch

13.15 **The emergency response**
Divisional Officer Mark Samuels
Essex County Fire & Rescue Service, UK

14.00 **The aftermath – what actions were required and initiated?**
Richard Gowland

14.20 **Systematic assessment of safety integrity level requirements**
Richard Gowland

14.50 Coffee

15.10 **Guidance for the management of operations and human factors**
Dr. Alan King

16.10 **Guidance on automatic overfill protection systems for bulk gasoline storage tanks**
Dave Ransome

This presentation will give assistance into the life cycle elements of design, installation and testing of automatic protection systems, to the required Safety Integrity Level (SIL) and to comply with the relevant International Standards and PSLG Guidance.

16.40 **Comments from the Chairman**

17.00 Participation to dinner,
Additional fee is EUR 50/person

Day 2
WEDNESDAY, 3 MARCH, 2010

9.00 **Wrap-up of Day 1**
Chairman

9.15 **Layer Of Protection Analysis**
Richard Gowland and Dave Ransome

How does it apply to Buncefield type facilities?

What needs to be considered?

What does the Buncefield experience and guidance mean for similar AND other facilities?

10.45 Coffee

11.05 **A simplified approach to the use of LOPA – how the guidance can it be applied to other operations?**
Richard Gowland

11.45 **Managing a fuel terminal in the real world**
Environmental and Technical Manager
Chris Newstead, Simon Storage Ltd.

12.30 Lunch

13.30 **Facilitated Discussion groups: An opportunity to compare participant practices with what has been presented at the lectures.**
- Explosion effects
- Human Factors
- Managing people and the hardware

Presenters working to a prepared pattern of questions and sample answers
Directed by Richard Gowland, Dave Ransome and Alan King

14.15 **Presentation of workshop results**
Participants

14.45 Coffee

15.05 **Effect on U.K. Land Use Planning – Health and Safety Executive Policy report**
Richard Gowland

15.15 **The Netherlands Regulator´s response**
Peter Kers and Robert Ruigrok,
DCMR Milieudienst Rijnmond

15.45 **Concluding words**
All speakers + chairman

This program is subject to changes.

FURTHER INFORMATION

please contact

MR RAINER PALONIEMI
Training Manager
AEL, tel. +358 (0)50 547 2724
rainer.paloniemi@ael.fi

REGISTRATION

Please register yourself using the registration form (www.ael.fi/ehs).

The registration deadline is February 15, 2010.

CONFIRMATION

Your registration will be confirmed by e-mail before the event.

REGISTRATION FEE

EUR 985 (VAT 0 %), covers study material in folder form, meals, coffee and other refreshments mentioned in the programme.

EUR 885 (VAT 0 %), members of NVVK.

The registration fee will be invoiced by AEL.

SEMINAR VENUE

Westcord Fashion Hotel Amsterdam
Hendrikje Stoffelstraat 1, 1058 GC, Amsterdam,
The Netherlands, tel. +31 (0) 20 8100 800,
fax +31 (0) 20 6810 802, www.westcordhotels.nl

HOTEL ACCOMMODATION

The participants should make their reservations and pay the accommodation themselves.

A number of hotel rooms are reserved for the seminar delegates at the Westcord Fashion Hotel Amsterdam.

Please quote the allotment code "AEL" when making a booking. Reservation can be made until 2 January 2010; after this date the mentioned rates are no longer guaranteed. Please be informed that a limited number of rooms is available. Make your reservation using the reservation form (download from www.ael.fi/ehs). Please return it to banqueting.fashion@westcordhotels.nl, or fax +31 (0) 20 8100 810.

CANCELLATION POLICY

If for some reason you are unable to attend, let us know no later than 14 days before the seminar begins. If a cancellation is made after that date, 50 % of the seminar fee will be collected. If no notification of cancellation is received, the participation fee will be charged in full.

AEL.fi
ACTION EXPERIENCE LEARNING

AEL – HOUSE OF SOLUTIONS

AEL is Finland's leading provider of technical training. We supply efficient solutions for developing companies' operations, even on a global level. Our service range includes solutions tailored for companies, open and company-specific courses, seminars, qualifications and vocational training. Our strengths include extensive industry know-how, customer-specific solutions and well-designed learning environments.

CERTIFIED BY inspecta
ISO 9001
ISO 14001
OHSAS 18001

AEL, Kaarnatie 4, FI-00410 Helsinki, tel. +358 (0)9 530 71, fax +358 (0)9 5663 278, www.ael.fi

Health and Safety Executive

Safety and environmental standards for fuel storage sites

Process Safety Leadership Group
Final report

Applicants Notes:

Following on from the Buncefield Standards Task Group, I became a member on the Process Safety Leadership Group and contributed in developing the guidance contained in the PSLG Final Report.

I was a member of the working parties which produced the guidance in:

Part 1 Systematic Assessment of Safety Integrity requirements and
Appendix 2 - Guidance on the application of LOPA

Part 2 - Protecting against loss of containment using high integrity systerms and
Appendix 4 - Guidance on Automatic Overfill Protection Systems

Paul Jobling	Simon Storage
Allen Ormond	ABB Engineering Services
Craig Garbutt	Vopak
Kevin Shephard	Vopak
Glen Knight	ExxonMobil
Jon Evans	ExxonMobil
Mike Brown	ExxonMobil
Linda Dixon	Chevron
Paul Evans	Chevron
Fiona Brindley	Health and Safety Executive
Peter Mullins	Health and Safety Executive
Ron McLeod	Shell
John Gilbert	Kaneb
Bud Hudspith	UNITE the union

Working Group 2 – Scope

Stuart Barlow (Chairperson)	Health and Safety Executive
James Fairburn	Petroplus
John Galbraith	SABIC
Doug Leach	Chemical Business Association
Neil MacNaughton	INEOS
Kevin Shephard	Vopak
Ian Wilkinson	Total
Stephen Brown	BP

Working Group 3 – Control and instrumentation

Jeff Pearson (Chairperson)	Health and Safety Executive
Chris Newstead	Simon Storage
Dave Ransome	P & I Design Ltd
Ian Neve	Total
John Donald	Total
Joulian Douse	Petroplus
Malcolm Tennant	MHT Technology
Mark Broom	Environment Agency
Martyn Hewitson Griffiths	MHT Technology
Neil MacNaughton	INEOS
Neil Waller	INEOS
Peter Edwards	ConocoPhillips
Richard Gowland	EPSC
Richard Tinkler	ConocoPhillips
Rob Ayton	Petroplus
Robert Nicol	Shell
Stuart Williamson	Petroplus
Terry Lewis	Total
Colin Chambers	Health and Safety Laboratory
David Carter	Health and Safety Executive
Alan King	ABB
Paul Baker	ConocoPhillips