
CDOIF

Chemical and Downstream Oil Industries Forum

Collection of Guidance Publications

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Safety and environmental standards for fuel storage sites

Process Safety Leadership Group
Final report



Safety and environmental standards for fuel storage sites

Process Safety Leadership Group
Final report

© *Crown copyright 2009*

First published 2009

ISBN 978 0 7176 6386 6

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

Applications for reproduction should be made in writing to:
The Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU
or e-mail: licensing@opsi.gov.uk

Contents

Foreword	7
Introduction	9
Scope and application	11
Summary of actions required	14
Part 1 Systematic assessment of safety integrity level requirements	22
Part 2 Protecting against loss of primary containment using high integrity systems	25
Part 3 Engineering against escalation of loss of primary containment	37
Part 4 Engineering against loss of secondary and tertiary containment	42
Part 5 Operating with high reliability organisations	62
Part 6 Delivering high performance through culture and leadership	64
Conclusion	66
<i>Appendices</i>	
Appendix 1 Mechanisms and potential substances involved in vapour cloud formation	67
Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage tank	82
Appendix 3 Guidance on defining tank capacity	125
Appendix 4 Guidance on automatic overfill protection systems for bulk gasoline storage tanks	129
Appendix 5 Guidance for the management of operations and human factors	142
Appendix 6 Emergency planning guidance	197
Appendix 7 Principles of process safety leadership	244
Appendix 8 Process Safety Forum: Governance and terms of reference	247
Appendix 9 BSTG report cross reference	249
Appendix 10 Acknowledgements	252
References	256
Abbreviations	264
Further information	267

Foreword

The recent Texas City and Buncefield incidents have moved industry and regulators beyond the pure science and engineering responses to develop ways to prevent a recurrence. They have caused us to also critically examine the leadership issues associated with delivering what has to be excellent operation and maintenance of high-hazard processes.

The responses by industry and regulators to these incidents, and the recommendations arising from their investigations, are essential to ensuring they never happen again. Such responses need to be effective and measured, requiring a dialogue between industry and the community to determine the balance between risk prevention, the viability of the operations and their value to society. In this regard the regulators are the effective representatives and arbiters for society.

The formation of the Process Safety Leadership Group (PSLG) in September 2007 was designed to meet the need for an effective framework for interaction between industry, trade unions and the COMAH Competent Authority (CA); a framework in which they could carry out a dialogue to jointly develop, progress and implement meaningful, effective recommendations and practices that improve safety in our industries.

PSLG membership consisted of senior representatives of the relevant trade associations, the CA and trade unions. It built on the work of the Buncefield Standards Task Group (BSTG), set up in 2006 to translate the lessons learned from that incident into effective and practical guidance that the industry could implement quickly. PSLG expanded the membership to include the Chemical Industries Association and also took on the task of progressing the implementation of the Buncefield Major Incident Investigation Board (MIIB) recommendations. PSLG also saw a need to raise the profile of process safety leadership throughout the petrochemical and chemical industries in response to criticisms by both the Baker Panel (Texas City) and MIIB (Buncefield) that leadership in this area was lacking and a contributory factor to these events.

PSLG has sought to continue the BSTG model of working through the trade associations to measure and encourage progress against the various recommendations. In particular the use of work groups involving the regulator, industry and the trade unions has been key to developing effective, practical guidance and recommendations with buy-in from all involved. To support this work, PSLG developed its Principles of Process Safety Leadership, signed by the trade associations, CA and trade unions, which set out the commitment to the enhancement of process safety. The trade associations will reflect the principles of process safety through their own initiatives and actively share progress as programmes roll out.

The model of industry and the regulator working together on improving our capability to operate safely is, I am convinced, a very effective one. Taking the path chosen by BSTG and PSLG is not an easy option – it requires trust from all parties and a willingness to voluntarily accept measures that require significant investment, both in financial and human terms. The regulator will always, and should always, have the power to act independently to impose change – ‘aligned, but not joined’ was the phrase coined when BSTG set off. However, I am sure we will get better, faster, by jointly finding solutions rather than adopting a prescriptive approach.

This report and its recommendations represent the outcome of a tremendous amount of work by the industry, trade unions and the regulator. I would like to thank them for all their efforts, tenacity and input. Our work can and will make a significant contribution to improving process safety – the challenge for all of us now is to deliver!

Tony Traynor
Chair
Process Safety Leadership Group



Introduction

1 The main purpose of this report is to specify the minimum standards of control which should be in place at all establishments storing large volumes of gasoline.

2 The PSLG also considered other substances capable of giving rise to a large flammable vapour cloud in the event of a loss of primary containment. However, to ensure priority was given to improving standards of control to tanks storing gasoline PSLG has yet to determine the scale and application of this guidance to such substances. It is possible that a limited number of other substances (with specific physical properties and storage arrangements) will be addressed in the future.

3 This report also provides guidance on good practice in relation to secondary and tertiary containment for facilities covered by the CA Control of Major Accident Hazards (COMAH) Containment Policy.¹

4 Parts of this guidance may also be relevant to other major hazard establishments.

5 Taking forward improvements in industry, PSLG built on the developments of the original BSTG using a small, focused, oversight team to provide leadership and support to expert working groups in developing guidance on specific topics. It was chaired by a senior member of industry and involved representatives from the United Kingdom Petroleum Industry Association (UKPIA), the Tank Storage Association (TSA), the United Kingdom Onshore Pipeline Operators' Association (UKOPA), the Chemical Industries Association (CIA), the Trades Union Congress, the Health and Safety Executive (HSE), the Environment Agency and the Scottish Environment Protection Agency (SEPA). PSLG led, developed and promoted improvements to safety and environmental controls, in particular:

- demonstrating effective leadership within the sector;
- developing organisational and technical solutions;
- sharing and learning from incidents and good practice;
- driving forward research;
- monitoring compliance with the Buncefield MIIB's and BSTG's recommendations;
- making further recommendations where appropriate; and
- taking effective account of the findings of the exploration of the explosion mechanism.

6 This report reflects the original scope of BSTG, incorporating the detailed guidance provided by PSLG and its working groups. The report is structured into six parts, addressing all 25 of the recommendations included in the Buncefield MIIB *Recommendations on the design and operation of fuel storage sites*² report:

- Part 1: Systematic assessment of safety integrity level requirements
- Part 2: Protecting against loss of primary containment using high integrity systems
- Part 3: Engineering against escalation of loss of primary containment
- Part 4: Engineering against loss of secondary and tertiary containment
- Part 5: Operating with high reliability organisations
- Part 6: Delivering high performance through culture and leadership

7 This report supersedes and replaces the BSTG final report which was issued in July 2007. A cross reference between the original BSTG report and this final PSLG report is provided in Appendix 9.

8 The structure of this report aligns with the framework of the Buncefield MIIB *Design and operation* report, ensuring a clear cross reference between individual recommendations and the detailed guidance which addresses each of these. Guidance to address a specific issue may be split across multiple MIIB recommendations, so the reader should consider the report as a whole when determining what actions should be taken. For example, when considering the need for additional overfill protection measures, the reader should:

- refer to Parts 1 and 2 and consider the appropriate hazard identification and risk assessment technique outlined in Appendix 5;
- where appropriate follow the guidance in Appendix 2 for the application of the layer of protection analysis (LOPA) technique; and
- where appropriate use the guidance provided in Appendix 4 to determine the architecture and nature of the protection system.

Scope and application

9 This guidance applies to establishments to which the Control of Major Accident Hazards Regulations 1999 (as amended) (COMAH) apply. It relates to the safety and environmental measures controlling the storage of liquid dangerous substances kept at atmospheric pressure in bulk storage tanks. In this guidance liquid dangerous substances are considered to be gasoline, and other hazardous liquids as defined in the COMAH CA Containment Policy. For the purposes of this report gasoline is defined as in paragraph 24. PSLG has not defined the meaning of large storage tanks beyond the definition in paragraph 24 below but rather this guidance should be interpreted in terms of the major accident risks that may arise from an overfill of a tank or other large-scale losses of containment from tanks. Figure 1 provides an overview of the application of this report to existing establishments.

10 This report also provides generic guidance on the storage of bulk hazardous liquids at COMAH establishments covered by Part 1 of the CA Containment Policy. The CA together with industry will determine the extent to which this guidance is relevant to other tanks falling within scope of Part 1 of the Containment Policy and further industry specific guidance will be issued at a later date.

11 This guidance is not an authoritative interpretation of the law, but if you do follow this guidance you will normally be doing enough to comply with the law. Other alternative measures to those set out in this guidance may be used to comply with the law.

12 PSLG considers that these provisions will, in the majority of cases, meet the requirements of COMAH Regulation 4. Regulation 4 requires every operator to take all measures necessary to prevent major accidents and limit their consequences to people and the environment. Regulation 4 requires dutyholders to reduce the risk of a major accident as low as is reasonably practicable (ALARP).

13 Where this report calls for dutyholders to meet this guidance in full, in certain circumstances this may not be reasonably practicable for an existing operation. In the instance of overfill protection, this guidance indicates where such circumstances may arise. However, in such cases the final decision on the degree of compliance to meet the requirements of COMAH will be a matter between the dutyholder and the COMAH CA.

Application to new COMAH establishments and existing COMAH establishments subject to substantial modification

14 All new and substantially modified establishments storing gasoline should follow this guidance in full with respect to tanks meeting the criteria set out in paragraph 24. For establishments falling within the scope of the COMAH CA Containment Policy Part 2, dutyholders should comply with Part 4 of this guidance in full. Other new establishments and modifications falling within the scope of the Containment Policy should take account of this guidance when determining control measures for the bulk storage of liquid dangerous substances.

Application to existing COMAH establishments

15 Figure 1 summarises the application of this guidance to existing COMAH establishments. It should be noted that this figure is to aid decision making rather than to set priorities.

Existing establishments with tanks storing gasoline

16 Establishments storing gasoline in bulk tanks form the highest priority for PSLG. They represent the activities where PSLG expects to see the highest standards of control of risks of both the integrity of plant and equipment and in process safety management. Existing establishments with tanks falling within the definition set out in paragraph 24 should, therefore, meet this guidance in full.

17 PSLG wishes to see a rigorous approach to primary and secondary containment and to on-site emergency arrangements within this category of establishments. This is to ensure that the standards will be, where necessary, significantly higher than before the Buncefield incident.

18 Particular emphasis is given to overfill prevention as this is the primary means by which another major incident can be prevented. Accordingly, Parts 1 and 2 together with Appendix 4 set a rigorous standard with fully automatic overfill protection to safety integrity level 1 (SIL 1) as defined in BS EN 61511 as the benchmark. To limit the environmental consequences of an overfill incident particular attention should be given to standards of secondary and tertiary containment as set out in this guidance. The high standards of on-site emergency arrangements needed to limit the consequence of an incident are also set out.

Existing establishments storing products that may give rise to a large vapour cloud in the event of an overfill

19 PSLG has undertaken work to determine whether other liquids outside the criteria set out in paragraph 24 have the potential to give rise to a large vapour cloud in similar circumstances to those at Buncefield. The results of this work are given in Appendix 1. This methodology can be used to determine the potential for liquids to form a large vapour cloud in the event of an overfill. An indicative list of such substances is also provided.

20 The CA together with industry will determine the extent to which this guidance should apply to tanks meeting the criteria in Appendix 1. Following the publication of this guidance a programme of work will be started to establish a strategy for compliance taking account of the nature of the risk and severity of the consequence of a major accident. In the meantime, dutyholders should take account of this guidance in complying with their normal legal duties under COMAH.

Existing establishments with tanks falling within scope of Part 2 of the COMAH Competent Authority Containment Policy

21 Dutyholders should comply with the recommendations in Part 4 of this guidance (Engineering against loss of secondary and tertiary containment) so far as is reasonably practicable.

22 Dutyholders should take account of the good practice guidance in other parts of this report when determining control measures for the bulk storage of liquid dangerous substances.

Existing establishments with other tanks falling within scope of Part 1 of the COMAH Competent Authority Containment Policy

23 This report contains generic guidance on the storage of bulk liquids, product transfers and management systems, including competence and human factors. Therefore, dutyholders should take account of the good practice guidance in this report when determining control measures for the bulk storage of liquid dangerous substances.

Definition of in-scope gasoline tanks

24 In-scope gasoline tanks are defined as:

- those storing gasoline (petrol) as defined in Directive 94/63/EC European Parliament and Council Directive 94/63/EC of 20 December 1994 on the control of volatile organic compound emissions resulting from the storage of petrol and its distribution from terminals to service stations;
- vertical, cylindrical, non-refrigerated, above-ground storage tanks typically designed to standards BS 2654,³ BS EN 14015,⁴ API 620,⁵ API 650⁶ (or equivalent codes at the time of construction);
- with side walls greater than 5 m in height; and
- filled at rates greater than 100 m³/hour (this is approximately 75 tonnes/hour of gasoline).

The Containment Policy does not define the meaning of bulk storage, but for the purposes of this guidance the following criteria apply:

- The liquid is stored in an atmospheric storage tank built to a recognised design code as bullet point 2 of paragraph 24.

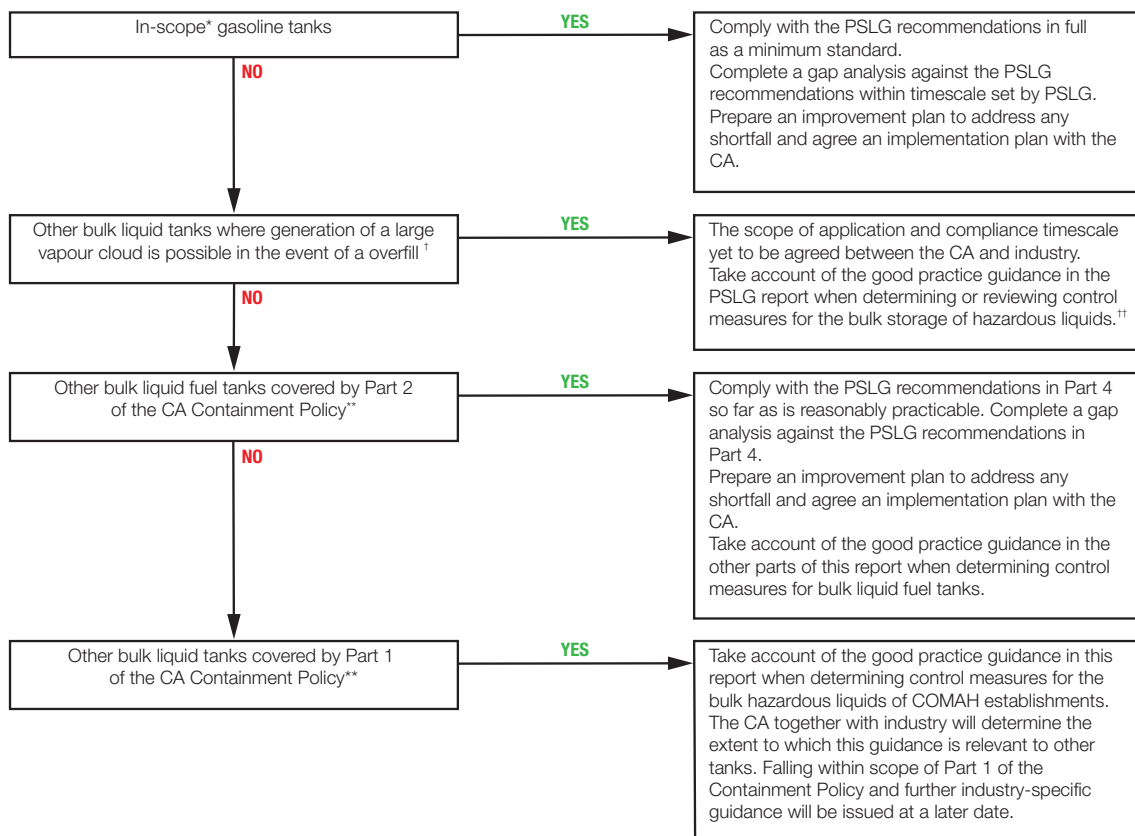


Figure 1 Compliance at existing COMAH establishments

* As defined in paragraph 24.

† As set in Appendix 1.

** CA COMAH Containment Policy www.environment-agency.gov.uk/business/sectors/37107.aspx.

†† Work has yet to be concluded on the extent to which this guidance should be implemented for tanks storing liquids which may give rise to a large vapour cloud in the event of an overfill - as set out in Appendix 1. The CA will agree future proposals on implementation with industry

Summary of actions required

25 Table 1 provides a summary of the MIIB *Design and operation* report recommendations; Parts 1 to 6 of this report provide the guidance to address each of these recommendations. Dutyholders should already have met the recommendations within the BSTG report. The CA has a programme of work to check compliance.

26 The information in Parts 1 to 6 of this guidance is presented in the same order as the recommendations in the MIIB *Design and operation* report.

27 Within six months of the publication of this report, dutyholders should undertake a gap analysis of their compliance with the revised and new guidance contained within this report for in-scope gasoline tanks (as defined in paragraph 24) and record their findings. Within nine months of the publication of this report dutyholders should agree with the CA an improvement plan to comply with this guidance.

28 For a number of recommendations there is a requirement to ensure that any changes are incorporated within the safety report. For lower-tier sites, demonstrating that improvements have been made will be achieved in the normal way by having systems and procedures in place at the establishment to deliver the intended outcome.

Table 1 Recommendations from the MIIB *Design and operation* report

MIIB recommendation		MIIB sub-recommendation		PSLG Report Reference
<i>Systematic assessment of safety integrity level requirements</i>				
1	The CA and operators of Buncefield-type sites should develop and agree a common methodology to determine 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: Application of the methodology should be clearly demonstrated in the COMAH safety report submitted to the CA for each applicable site. Existing safety reports will need to be reviewed to ensure this methodology is adopted.	1(a)	the existence of nearby sensitive resources or populations;	Part 1, paragraphs 29–33 Overfill protection systems for storage tanks, paragraphs 34–38 Application of LOPA to the overflow of an atmospheric tank, paragraphs 39–40 Incorporating the findings of SIL assessments into COMAH safety reports, paragraph 41 Operator responsibilities and human factors, paragraphs 42–43
		1(b)	the nature and intensity of depot operations;	
		1(c)	realistic reliability expectations for tank gauging systems;	
		1(d)	the extent/rigour of operator monitoring.	

MIIB recommendation	MIIB sub-recommendation	PSLG Report Reference
<i>Protecting against loss of primary containment using high integrity systems</i>		
2	2(a)	Part 2, paragraphs 44–46 Management of instrumented systems for fuel storage tank installations, paragraphs 47–68 Probabilistic preventative maintenance for atmospheric bulk storage tanks, paragraph 69
	2(b)	
3		Automatic overfill protection systems for bulk gasoline storage tanks, paragraphs 70–72 Overfill protection standards, paragraphs 73–78 Tank overfill protection, paragraphs 79–103 Fire-safe shut-off valves, paragraphs 104–114 Remotely operated shut-off valves (ROSOVs) paragraphs 106–109
4		Automatic overfill protection systems for bulk gasoline storage tanks, paragraphs 70–73 Overfill protection standards, paragraphs 73–78 Tank overfill protection, paragraphs 79–103 Fire-safe shut-off valves, paragraphs 104–114

MIIB recommendation	MIIB sub-recommendation		PSLG Report Reference
<p>5 All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure the specified SIL is maintained in practice in accordance with the requirements of Part 1 of BS EN 61511.</p>			<p>Automatic overfill protection systems for bulk gasoline storage tanks, paragraphs 70–72 Overfill protection standards, paragraphs 73–78 Tank overfill protection, paragraphs 79–103 Fire-safe shut-off valves, paragraphs 104–114</p>
<p>6 The sector should put in place arrangements to ensure the receiving site (as opposed to the transmitting location) has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) without depending on the actions of a remote third party, or on the availability of communications to a remote location. These arrangements will need to consider upstream implications for the pipeline network, other facilities on the system and refineries</p>			<p>Improving safety of fuel transfers, paragraph 115</p>
<p>7 In conjunction with Recommendation 6, the sector and the CA should undertake a review of the adequacy of existing safety arrangements, including communications, employed by those responsible for pipeline transfers of fuel. This work should be aligned with implementing Recommendations 19 and 20 on high reliability organisations to ensure major hazard risk controls address the management of critical organisational interfaces.</p>			<p>Improving safety of fuel transfers, paragraph 115</p>
<p>8 The sector, including its supply chain of equipment manufacturers and suppliers, should review and report without delay on the scope to develop improved components and systems, including but not limited to the following:</p>	8(a)	<p>Alternative means of ultimate high-level detection for overfill prevention that do not rely on components internal to the storage tank, with the emphasis on ease of inspection, testing, reliability and maintenance.</p>	<p>Improved level instrumentation components and systems, paragraph 116 Overflow detection, paragraphs 117–121</p>
	8(b)	<p>Increased dependability of tank level gauging systems through improved validation of measurements and trends, allowing warning of faults and through using modern sensors with increased diagnostic capability.</p>	
	8(c)	<p>Systems to control and log override actions.</p>	

MIIB recommendation		MIIB sub-recommendation		PSLG Report Reference
9	Operators of Buncefield-type sites should introduce arrangements for the systematic maintenance of records to allow a review of all product movements together with the operation of the overfill prevention systems and any associated facilities. The arrangements should be fit for their design purpose and include, but not be limited to, the following factors:	9(a)	The records should be in a form that is readily accessible by third parties without the need for specialist assistance.	Maintenance of records, paragraphs 122–123
		9(b)	The records should be available both on site and at a different location.	
		9(c)	The records should be available to allow periodic review of the effectiveness of control measures by the operator and the CA, as well as for root cause analysis should there be an incident.	
		9(d)	A minimum period of retention of one year.	
10	The sector should agree with the CA on a system of leading and lagging performance indicators for process safety performance. This system should be in line with HSE's recently published guidance on <i>Developing process safety indicators</i> HSG254. ⁷			Process safety performance indicators, paragraphs 124–125
<i>Engineering against escalation of loss of primary containment</i>				
11	Operators of Buncefield-type sites should review the classification of places within COMAH sites where explosive atmospheres may occur and their selection of equipment and protective systems (as required by the Dangerous Substances and Explosive Atmospheres Regulations 2002). ⁸ This review should take into account the likelihood of undetected loss of containment and the possible extent of an explosive atmosphere following such an undetected loss of containment. Operators in the wider fuel and chemicals industries should also consider such a review, to take account of events at Buncefield.			Part 3, paragraph 126 Review of area classifications, paragraph 127
12	Following on from Recommendation 11, operators of Buncefield-type sites should evaluate the siting and/or suitable protection of emergency response facilities such as firefighting pumps, lagoons or manual emergency switches.			Siting and protection of emergency response facilities, paragraph 128

MIIB recommendation	MIIB sub-recommendation	PSLG Report Reference	
13	<p>Operators of Buncefield-type sites should employ measures to detect hazardous conditions arising from loss of primary containment, including the presence of high levels of flammable vapours in secondary containment. Operators should without delay undertake an evaluation to identify suitable and appropriate measures. This evaluation should include, but not be limited to, consideration of the following:</p>	<p>13(a) Installing flammable gas detection in bunds containing vessels or tanks into which large quantities of highly flammable liquids or vapour may be released.</p> <p>13(b) The relationship between the gas detection system and the overfill prevention system. Detecting high levels of vapour in secondary containment is an early indication of loss of containment and so should initiate action, for example through the overfill prevention system, to limit the extent of any further loss.</p> <p>13(c) Installing CCTV equipment to assist operators with early detection of abnormal conditions. Operators cannot routinely monitor large numbers of passive screens, but equipment is available that detects and responds to changes in conditions and alerts operators to these changes.</p>	<p>Detection of hazardous conditions, paragraph 129</p>
14	<p>Operators of new Buncefield-type sites or those making major modifications to existing sites (such as installing a new storage tank) should introduce further measures including, but not limited to, preventing the formation of flammable vapour in the event of tank overflow. Consideration should be given to modifications of tank top design and to the safe re-routing of overflowing liquids.</p>		<p>Prevention of the formation of flammable vapour clouds for new or substantially modified sites, paragraphs 130–135</p>
15	<p>The sector should begin to develop guidance without delay to incorporate the latest knowledge on preventing loss of primary containment and on inhibiting escalation if loss occurs. This is likely to require the sector to collaborate with the professional institutions and trade associations</p>		<p>Preventing loss of primary containment, paragraphs 136–138 Internal/out-of-service inspections, paragraphs 139–146 External/in-service inspections, paragraphs 147–149 Deferring internal examinations, paragraphs 150–151 Competency, paragraphs 152–154 Remedial work, paragraphs 155–159</p>

MIIB recommendation	MIIB sub-recommendation		PSLG Report Reference
<p>16 Operators of existing sites, if their risk assessments show it is not practicable to introduce measures to the same extent as for new ones, should introduce measures as close to those recommended by Recommendation 14 as is reasonably practicable. The outcomes of the assessment should be incorporated into the safety report submitted to the CA.</p>			<p>Prevention of the formation of flammable vapour clouds for existing sites, paragraphs 160–165</p>
<i>Engineering against loss of secondary and tertiary containment</i>			
<p>17 The CA and the sector should jointly review existing standards for secondary and tertiary containment with a view to the CA producing revised guidance by the end of 2007. The review should include, but not be limited to the following:</p>	17(a)	<p>Developing a minimum level of performance specification of secondary containment (typically this will be bunding).</p>	<p>Part 4, paragraph 166–169 Bund lining systems, paragraphs 170–185 Pipe penetrations, paragraphs 186–208 Bund wall expansion and construction joints, paragraphs 209–217 Secondary containment systems under tanks, paragraphs 218–220 Basis for bund capacity based on tank capacity, paragraphs 221–232 Firewater management and control measures, paragraph 233 Tertiary containment, paragraphs 234–250</p>
17(b)	<p>Developing suitable means for assessing risk so as to prioritise the programme of engineering work in response to the new specification.</p>		
17(c)	<p>Formally specifying standards to be achieved so that they may be insisted upon in the event of lack of progress with improvements.</p>		
17(d)	<p>Improving firewater management and the installed capability to transfer contaminated liquids to a place where they present no environmental risk in the event of loss of secondary containment and fires.</p>		
17(e)	<p>Providing greater assurance of tertiary containment measures to prevent escape of liquids from site and threatening a major accident to the environment.</p>		
<p>18 Revised standards should be applied in full to new-build sites and to new partial installations. On existing sites, it may not be practicable to fully upgrade bunding and site drainage. Where this is so operators should develop and agree with the CA risk-based plans for phased upgrading as close to new plant standards as is reasonably practicable.</p>			<p>Bund lining systems, paragraphs 170–185 Pipe penetrations, paragraphs 186–208 Bund wall expansion and construction joints, paragraphs 209–217 Secondary containment systems under tanks, paragraphs 218–220 Basis for bund capacity based on tank capacity, paragraphs 221–232 Firewater management and control measures, paragraph 233 Tertiary containment, paragraphs 234–250</p>

MIIB recommendation	MIIB sub-recommendation	PSLG Report Reference	
<i>Operating with high reliability organisations</i>			
19	<p>The sector should work with the CA to prepare guidance and/or standards on how to achieve a high reliability industry through placing emphasis on the assurance of human and organisational factors in design, operation, maintenance, and testing. Of particular importance are:</p>	<p>19(a) understanding and defining the role and responsibilities of the control room operators (including in automated systems) in ensuring safe transfer processes;</p> <p>19(b) providing suitable information and system interfaces for front line staff to enable them to reliably detect, diagnose and respond to potential incidents;</p> <p>19(c) training, experience and competence assurance of staff for safety critical and environmental protection activities;</p> <p>19(d) defining appropriate workload, staffing levels and working conditions for front line personnel;</p> <p>19(e) ensuring robust communications management within and between sites and contractors and with operators of distribution systems and transmitting sites (such as refineries);</p> <p>19(f) prequalification auditing and operational monitoring of contractors' capabilities to supply, support and maintain high integrity equipment;</p> <p>19(g) providing effective standardised procedures for key activities in maintenance, testing, and operations;</p> <p>19(h) clarifying arrangements for monitoring and supervision of control room staff;</p> <p>19(i) effectively managing changes that impact on people, processes and equipment.</p>	Part 5, paragraphs 251–258
20	<p>The sector should ensure that the resulting guidance and/or standards is/are implemented fully throughout the sector, including where necessary with the refining and distribution sectors. The CA should check that this is done.</p>		Part 5, paragraphs 251–258
21	<p>The sector should put in place arrangements to ensure that good practice in these areas, incorporating experience from other high hazard sectors, is shared openly between organisations.</p>		Part 5, paragraphs 251–258

MIIB recommendation	MIIB sub-recommendation		PSLG Report Reference
22 The CA should ensure that safety reports submitted under the COMAH Regulations contain information to demonstrate that good practice in human and organisational design, operation, maintenance and testing is implemented as rigorously as for control and environmental protection engineering systems.			Part 5, paragraphs 251–258
<i>Delivering high performance through culture and leadership</i>			
23 The sector should set up arrangements to collate incident data on high potential incidents including overfilling, equipment failure, spills and alarm system defects, evaluate trends, and communicate information on risks, their related solutions and control measures to the industry.			Part 6, paragraphs 259–265
24 The arrangements set up to meet Recommendation 23 should include, but not be limited to, the following:	24(a)	Thorough investigation of root causes of failures and malfunctions of safety and environmental protection critical elements during testing or maintenance, or in service.	Part 6, paragraphs 259–265
	24(b)	Developing incident databases that can be shared across the entire sector, subject to data protection and other legal requirements. Examples exist of effective voluntary systems that could provide suitable models.	
	24(c)	Collaboration between the workforce and its representatives, dutyholders and regulators to ensure lessons are learned from incidents, and best practices are shared.	
25 In particular, the sector should draw together current knowledge of major hazard events, failure histories of safety and environmental protection critical elements, and developments in new knowledge and innovation to continuously improve the control of risks. This should take advantage of the experience of other high hazard sectors such as chemical processing, offshore oil and gas operations, nuclear processing and railways.			Part 6, paragraphs 259–265

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 overflow 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 overflow, 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.

Part 2 Protecting against loss of primary containment using high integrity systems

44 The MIIB's third progress report¹⁰ indicated that there was a problem with the tank level monitoring system at Buncefield.

45 Overfill protection systems using high-level switches or other two-state detectors may be inactive for long periods and may develop unrevealed faults. Such faults cause the system to fail to danger. Therefore, overfill protection systems should be tested periodically to identify and correct unrevealed faults.

46 These systems should be designed, implemented, documented, and have a regime of safety lifecycle management necessary to achieve the required SIL in compliance with BS EN 61511.

MIIB Recommendation 2

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

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

Management of instrumented systems for fuel storage tank installations

47 This guidance does not replace or detract from the requirements of BS EN 61511, but is a summary of some of the main requirements that are relevant to in-scope tanks. It does not cover all the requirements of BS EN 61511 – for more detail refer to the standard.

48 The suitability and continuing integrity of instrumented systems is essential to ensure the safety of an installation and in particular the primary containment system. The functional integrity of overfill protection systems is critical to primary containment. Overfill protection systems may be in a dormant state without being required to operate for many years. For this reason periodic testing is an essential element in assuring their continuing integrity.

49 BS EN 61511 requires that for all SIS implementing safety instrumented functions of SIL 1 or higher there is a management system in place for the whole of the lifecycle of the SIS, which will manage all appropriate measures.

50 BS EN 61511 does not cover requirements for systems providing a risk reduction of less than ten; however, they may still provide a contribution to the safety function and where these systems are part of the risk reduction they should comply with the management systems requirements of BS EN 61511 so far as is reasonably practicable.

51 Additional general guidance on operating high reliability organisations and the management of general operations human factors is in Part 5 and Appendix 5 of this guidance. Dutyholders should also consult broader human factors guidance when reviewing or implementing the human elements of their safety management systems.

Management of SIS

52 A SIS management system should include the following elements specific to safety instrumented systems. The management system may be part of an overall site-wide safety management system but the following elements should be in place for each phase in the SIS lifecycle:

- safety planning, organisation and procedures;
- identification of roles and responsibilities of persons;
- competence of persons and accountability;
- implementation and monitoring of activities;
- procedures to evaluate system performance and validation including keeping of records;
- procedures for operation, maintenance, testing and inspection;
- functional safety assessment and auditing;
- management of change;
- documentation relating to risk assessment, design, manufacture, installation and commissioning;
- management of software and system configuration.

Safety planning and organisation

53 Safety planning should identify all the required tasks that need to be performed at various stages and allocate roles and responsibilities of people (departments, individuals, staff or contractors) to perform those tasks.

54 The organisation and planning should be documented and reviewed as necessary when changes occur throughout the operational life of the system.

Responsibilities and competence

55 The roles and responsibilities associated with the SIS (such as design, operation, maintenance, testing etc) should be documented and communicated. This should include a description of the tasks and who is responsible for performing the tasks.

56 People with responsibilities should be competent to perform their tasks consistently to the required standard. The required knowledge, understanding and skills for the competences can be wide ranging and depend on the role and the type of task, and these may be for design, engineering, system technology, hazard and safety engineering, regulations, management, leadership, maintenance and testing.

Performance evaluation

57 Arrangements should be in place to evaluate the performance and validation of a safety instrumented system. This should include validation that the system design meets the requirements of BS EN 61511 and the system operation fulfils the design intent.

58 Failures of the system or of any component should be investigated and recorded along with any modifications and maintenance performed.

59 The details of any demands on the system, and system performance on demand, should be recorded including data on any spurious trips, any revealed failures of the system or its components and, in particular, any failures identified during proof testing.

60 Records of all these events should be kept for future analysis. Records may be paper or electronic.

Operation, maintenance and testing

61 Arrangements should be in place for the operation, maintenance and system testing and inspection for the whole system and subcomponents. Written procedures should be agreed by those the dutyholder has identified as responsible and competent for these functions. Procedures and competency arrangements should be based on adequate consideration of human failure potential in carrying out inspection, maintenance and testing activities. Reference should be made to Appendix 5 for general guidance on procedures and competence assurance.

62 The initial test interval should be determined by the calculation of probability of failure on demand during the design process, and this should be assessed and amended periodically based on real operational data.

Functional safety assessment

63 Functional safety is the part of the overall safety arrangements that depends on a system or equipment operating correctly in response to its inputs (BS EN 61508).¹¹ Procedures for functional safety assessment and auditing should be in place. A functional safety assessment is an independent assessment and audit of the functional safety requirements and the safety integrity level achieved by the SIS.

64 At least one functional safety assessment should be performed on each system, typically at the design stage before the system is commissioned. The functional safety assessment process should be performed by an assessment team which includes at least one competent person independent of the project design team. A functional safety assessment should be performed and revalidated after any modifications, mal-operation or failure to deliver the required safety function (a spurious trip which caused the safety system to action its functions successfully would not be considered a failure). The depth and scope of the functional safety assessment should be based on the specific circumstances, including the size of the project, complexity, SIL and the consequences of failure. Further guidance is given in BS EN 61511 Section 5.

Modifications

65 Where changes or modifications to an SIS are planned then the changes should be subject to a management of change process. The procedure should identify and address any potential safety implications of the modification.

66 Software changes and system configuration changes should also be subject to a management of change process.

Documentation

67 The associated documentation should be maintained, accurate and up-to-date with all necessary information available to allow operation and lifecycle management.

68 The documentation should include but not be limited to process and instrumentation diagrams, system design and testing requirements, and a description of maintenance activities for the various components of the SIS from sensors to final elements inclusive. Documentation of the design should include risk assessment for SIL determination, design specification, factory acceptance testing, installation specification, and commissioning tests.

Probabilistic preventative maintenance for atmospheric bulk storage tanks

69 EEMUA 159¹² probabilistic preventative maintenance approach, or a suitable and demonstrable risk-based system, when referenced together with the standards signposted for integrity management of atmospheric bulk storage tanks, provides the benchmark standard which will enable the dutyholder to have a suitable maintenance strategy and policy underpinning their systems and procedures. Dutyholders should assess their current tank integrity management systems against EEMUA 159, or equivalent, and draw up an improvement plan, as necessary, to ensure arrangements meet this standard.

MIIB Recommendation 3

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

Such systems should meet the requirements of Part 1 of BS EN 61511 for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1). Where independent automatic overfill prevention systems are already provided, their efficacy and reliability should be reappraised in line with the principles of Part 1 of BS EN 61511 and for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1).

MIIB Recommendation 4

The overfill prevention system (comprising means of level detection, logic/control equipment and independent means of flow control) should be engineered, operated and maintained to achieve and maintain an appropriate level of safety integrity in accordance with the requirements of the recognised industry standard for 'SIS', Part 1 of BS EN 61511.

MIIB Recommendation 5

All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure the specified safety integrity level is maintained in practice in accordance with the requirements of Part 1 of BS EN 61511.

Automatic overfill protection systems for bulk gasoline storage tanks

70 Appendix 4 provides guidance on good practice on overfill protection for new and existing in-scope tanks. It covers the design, implementation, lifecycle management, maintenance and proof testing for an automatic system on tank overfill protection to achieve the required SIL in compliance with BS EN 61511 so far as is reasonably practicable. It includes annexes on probability of failure on demand (PFD) calculations, hardware reliability, configuration requirements for fault tolerance and redundancy.

71 The following items are not covered:

- mechanical integrity of pipelines and delivery systems;
- the effects of automatic shutdown on continuous processes;
- the integrity of manual response to alarms where automatic shutdown is not provided.

72 This guidance is not intended to replace BS EN 61511 but to supplement it specifically in relation to tank overfill protection SIS. It does not cover all the requirements of BS EN 61511. Where guidance is not given on any requirement, such as protection against systematic failures, then reference should be made to the standard.

Overfill protection standards

73 All in-scope tanks should be fitted with a high integrity overfill prevention system that complies with BS EN 61511-1 (Appendix 4 provides further guidance for new and existing installations). Dutyholders should conduct a risk assessment to determine the appropriate SIL to meet the requirements of BS EN 61511-1. The outcome of that risk assessment should demonstrate that the risk arising from a tank overflowing in a way that may give rise to a major accident is ALARP. Appendix 2 provides guidance on the use of LOPA as a means of undertaking a suitable risk assessment.

74 A high integrity overfill prevention system should, as a minimum, provide a level of SIL 1 as defined in BS EN 61511-1. To reduce risk as low as reasonably practicable the overfill prevention system should preferably be automatic and should be physically and electrically separate from the tank gauging system. Automatic overfill prevention may include, but not be restricted to, measures such as automatic shutdown of the supply line or automatic diversion of the flow to another tank.

75 Where the installation of such an independent automatic overfill prevention system at an existing tank is demonstrated to give rise to other more serious safety or environmental risks elsewhere then other alternative measures may be adopted to achieve the same ALARP outcome.

76 Dutyholders will need to prepare a robust demonstration that alternative measures are capable of achieving an equivalent ALARP outcome to an overfill prevention system that is automatic and physically and electrically separate from the tank gauging system.

77 Alternative measures:

- should include an overfill prevention system to at least BS EN 61511-1 SIL 1, combined with other measures to provide high integrity and reliability; and
- those that include an operator(s) as part of the overfill prevention system should demonstrate that the reliability and availability of the operator(s) can be adequately supported to undertake the necessary control actions to prevent an overfill without compromising the ALARP outcome. Operator involvement should be properly managed, monitored, audited and reviewed on an ongoing basis. It is unlikely that an operator can be included in an overfill prevention system rated above SIL 1 as defined in BS EN 61511-1.

Proof testing

78 Appendix 4 paragraphs 23–33 give guidance on proof testing of overfill protection systems in accordance with BS EN 61511-1.

Tank overfill prevention: Defining tank capacity

79 To prevent an overflow, tanks should have headspace margins that enable the filling line to be closed off in time. The set points of high level trips and alarms requiring operator action should allow sufficient time for the action to be taken to deal with the developing situation.

Overfill level (maximum capacity)

80 A vital element of any system to prevent overfilling of a storage tank is a clear definition of the maximum capacity of the vessel. This is the maximum level consistent with avoiding loss of containment (overfilling or overflow) or damage to the tank structure (eg due to collision between an internal floating roof and other structures within the tank, or for some fluids, overstressing due to hydrostatic loading).

Tank rated capacity

81 Having established the overfill level (maximum capacity), it is then necessary to specify a level below this that will allow time for any action necessary to prevent the maximum from being reached/exceeded. This is termed the 'tank rated capacity', which will be lower than the actual physical maximum. Reference should be made to Appendix 3, 'Guidance on defining tank capacity' for a definition of these terms.

82 The required separation between the maximum capacity and the tank rated capacity is a function of the time needed to detect and respond to an unintended increase in level beyond the tank rated capacity. The response in this case may require the use of alternative controls, eg manual valves, which are less accessible or otherwise require longer time to operate than the normal method of isolation.

83 In some cases, it will be necessary to terminate the transfer in a more gradual fashion, eg by limiting the closure rate of the isolation valve, to avoid damaging pressure surges in upstream pipelines. Due allowance should be made for the delay in stopping the transfer when establishing the tank rated capacity. For some fluids, the tank rated capacity may also serve to provide an allowance for thermal expansion of the fluid, which may raise the level after the initial filling operation has been completed.

High-high level shutdown

84 The high-high level device provides an independent means of determining the level in the tank and is part of the overfilling protection system. It provides a warning that the tank rated capacity has been (or is about to be) reached/exceeded and triggers a response:

- The high-high level should be set at or below the tank rated capacity.
- The function of the LAHH is to initiate a shutdown.
- The outcome of LAHH activation may be limited to a visible/audible alarm to alert a human operator to take the required action. The actions required by the operator to a high-high level warning should be clearly specified and documented.
- The response may be fully automatic, via an instrumented protective system including a trip function that acts to close valves, stop pumps etc to prevent further material entering the tank. The trip function should include an audible/visual alarm to prompt a check that the trip function has been successful. Different devices can be employed to provide the trip function; these may range from a simple level switch (level switch high-high) to more sophisticated arrangements including duplicate level instrumentation.

Level alarm high

85 Providing an additional means of warning that the intended level has been exceeded can reduce the demand on the high-high device. It is anticipated that the LAH will be derived from the system used for determining the contents of the tank ATG:

- The position of the LAH should allow sufficient time for a response following activation that will prevent the level rising to the tank rated capacity (or the high-high level activation point if this is set lower).
- It is very important that the LAH is not used to control routine filling (filling should stop before the alarm sounds).

Normal fill level (normal capacity)

86 This level may be defined as the level to which the tank will intentionally be filled on a routine basis, using the normal process control system. The normal fill level will be dependent on the preceding levels and should be sufficiently far below the LAH to avoid spurious activation, eg due to level surges during filling or thermal expansion of the contents.

Other applications

87 In other applications, the primary means of determining the level may not involve an automatic gauging system. Depending on the detailed circumstances, the LAH may be a separate device, eg a switch.

Operator notifications

88 Some ATG systems include the facility for the operator to set system prompts to notify them when a particular level has been reached or exceeded. As the same level instrument typically drives these prompts and the LAH, they do not add significantly to the overall integrity of the system.

Determining action levels

89 Having defined generically the minimum set of action levels in the preceding section, it is necessary to consider the factors that determine the spacing between action levels in particular cases. In all cases, the spacing should be directly related to the response time required to detect, diagnose and act to stop an unintentional and potentially hazardous increase in level.

Response times

90 Care is needed when estimating the likely time for operators to respond to an incident. Consideration should be given to the detection, diagnosis, and action stages of response.

91 Detection covers how an operator will become aware that a problem exists. Assessment of alarm priorities and frequencies, the characteristics of the operator and console displays, as well as operators' past experience of similar problems on sites, are all useful aspects to review. Storage operation problems that appear over a period of time, and where the information available to the operators can be uncertain, are particularly difficult to detect. When control rooms are not continually staffed, the reliable detection of plant problems needs careful consideration.

92 Diagnosis refers to how an operator will determine what action, if any, is required to respond to the problem. Relevant factors to think about include training and competence assurance, the availability of clear operating procedures and other job aids, and level of supervision. The existence of more than one problem can make diagnosis more difficult.

93 Action covers how a timely response is carried out. Key aspects include: the availability of a reliable means of communicating with other plant operators; the time needed to locate and operate a control (close a valve, stop a pump); the need to put on personal protective equipment (PPE); the ease of operating the control while wearing PPE; and how feedback is given to operators that the control has operated correctly. Occasionally there may be circumstances where operators may hesitate if shutting down an operation might lead to later criticism.

94 A 'walk-through' of the physical aspects of the task with operators can provide useful information on the minimum time needed to detect and respond to an overfilling incident. However, due allowance needs to be made for additional delays due to uncertainty, hesitation or communications problems. This will need to be added to the minimum time to produce a realistic estimate of the time to respond.

95 Figure 2 summarises this guidance. The spacing between levels in the diagram is not to scale and it is possible that the greatest response time, and hence the largest separation in level, will be between the LAHH and the overfill level. This is because the response is likely to involve equipment that is more remote and for which the location and method of operation is less familiar. An exception to this would be if the high-high level device included a trip function, when a shorter response time might be anticipated.

Any increase in level beyond the overfill level will result in loss of containment and/or damage to the tank. (All other levels and alarm set points are determined relative to the overfill level.)

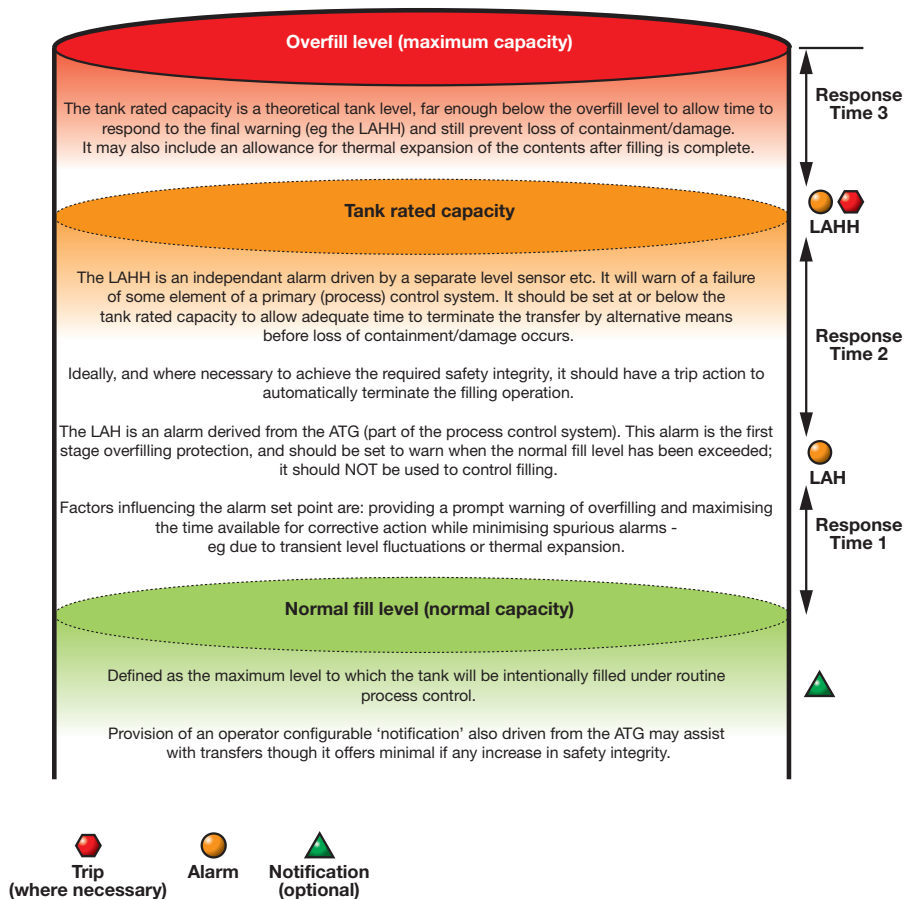


Figure 2 Overfilling protection: Tank levels (based on API 2350¹³)

Response time 3: LAHH to overfill/damage level (maximum capacity)

96 This is the response time between the LAHH and the overfill level (or maximum capacity – at which loss of containment or damage results). It should be assumed that the action taken to respond to the LAH has not been successful, eg the valve did not close or the wrong valve closed, and so corrective or alternative contingency action is now urgently required.

97 The response time to do this is identified as the worst combination* of filling rate and time taken to travel from the control room to the tank and positively stop the flow. This may be an alternative valve and may need additional time to identify and close it if not regularly used.

98 This could be done per tank or, more conservatively, standardised at the longest margin time for a group of or all tanks. In all cases, however, it should be recorded in writing.

Response time 2: LAH to LAHH

99 The response time between the LAH and the independent LAHH should again be defined based on the worst combination of filling rate and time taken to activate and close a remotely operated valve (ROV) if installed, or to get from the control room to the tank manual valve if not.†

* The tank with the highest fill rate might have a remotely operated valve operated conveniently from the control room, allowing for very rapid shutdown, whereas a slower filled (and/or smaller diameter) tank that required a long journey to get to a local manual valve may in fact result in a lengthy time before the fill is stopped.

† It is essential to take into account all of the organisational and human factors relevant to the site, eg failure of remote operation, loss of communications etc.

100 Again, this could be done per tank, or more conservatively, standardised at the longest margin time for a group of or all tanks. In all cases, however, it should be recorded in writing.

Response time 1: Normal fill level to LAH

101 The normal fill level should be close enough to the LAH to enable overfilling to be rapidly detected (and to maximise the usable capacity of the tank), but should be set an adequate margin below the LAH to prevent spurious operation of the alarm, eg due to liquid surge or thermal expansion at the end of an otherwise correctly conducted transfer.

102 Separation between the normal fill level and the LAH may also help to discourage inappropriate use of the LAH to control the filling operation.

103 Appendix 3 contains worked examples of the application of this guidance for setting tank capacities.

Fire-safe shut-off valves

104 Each pipe connected to a tank is a potential source of a major leak. In the event of an emergency it is important to be able to safely isolate the contents of the tank. Isolation valves should be fire-safe, ie capable of maintaining a leak-proof seal under anticipated fire exposure.

Fire-safe criteria

105 Fire-safe shut-off valves should be fitted close to the tank on both inlet and outlet pipes. Valves should either conform to an appropriate standard (BS 6755-2¹⁴ or BS EN ISO 10497¹⁵), equivalent international standards or be of an intrinsically fire-safe design, ie have metal-to-metal seats (secondary metal seats on soft-seated valves are acceptable), not be constructed of cast iron and not be wafer bolted.

Remotely operated shut-off valves (ROSOVs)

106 In an emergency, rapid isolation of vessels or process plant is one of the most effective means of preventing loss of containment, or limiting its size. A ROSOV is a valve designed, installed and maintained for the primary purpose of achieving rapid isolation of plant items containing hazardous substances in the event of a failure of the primary containment system (including, but not limited to, leaks from pipework, flanges and pump seals). Valve closure can be initiated from a point remote from the valve itself. The valve should be capable of closing and maintaining tight shut off under credible conditions following such a failure (which may include fire).

107 *Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice HSG244*¹⁶ provides guidance on how to assess the need to provide ROSOVs for emergency isolation. It has been written for a wide range of circumstances and as a result the section dealing with ROSOV failure modes requires additional interpretation.

108 A review of HSG244 ROSOV assessments showed that assessments did not always fully address the risks in the structured manner required by HSG244, but rather simply asserted that the provision of ROSOVs was not reasonably practicable. Others did not fully apply the primary and secondary selection criteria. Of those that did properly follow the steps in HSG244 it was concluded that:

- where the case-specific risk assessment indicated a ROSOV was required where currently only manual valves existed, then there was a worthwhile improvement to be gained by fitting a ROSOV;
- where the case-specific risk assessment indicated a ROSOV should be provided where currently a ROV (which would not fail safe) existed, it was not reasonably practicable to upgrade to a fail-safe device. But additional risk reduction could be achieved by ensuring that the cables are fire protected, and a rigorous regime is in place for inspection and testing the operation of the valves and control systems.

109 For tanks within scope, the expectation is that primary and secondary criteria in HSG244 would not normally eliminate the need for a ROSOV to the outlet pipe and as such a case-specific assessment as set out in Appendix 1 of HSG244 should be undertaken. For existing sites, the case-specific assessment should fully consider:

- whether fitting a ROSOV, where none is currently provided, is reasonably practicable;
- where a ROV is provided but it does not normally fail safe, whether upgrading to a fail-safe valve is reasonably practicable; and
- where an existing ROV does not fail safe, and it is not considered reasonably practicable to upgrade it, what additional measures should be provided to protect against failure, eg providing fire protection to the cabling and increasing the frequency of inspection and testing of the valve and associated cabling and energy supply.

Configuration

110 Bulk storage tanks can have their import and export lines arranged in a variety of configurations. These have a bearing on the necessary arrangements for isolating the tank inlets/outlets. Some tanks will have separate, dedicated import and export lines. Within this group, some will fill from the top and export from the base; some will both fill and export from either the top or the base. Others will have a single common import/export line, commonly connected at the base of the tank.

Dedicated import line

111 Tanks with dedicated import lines, whether these enter at the top or the base can be protected against backflow from the tank by the provision of non-return valves. Lines that enter at the top of the tank and deliver via a dip leg may in some cases be adequately protected by the provision of a siphon break to prevent the tank contents flowing back out via the feed line.

112 The provision of either or both of these features may affect the conclusion of any assessment of the need to provide a ROSOV for the purpose of emergency isolation of the tank against loss of the contents. These factors need to be considered when determining the appropriate failure mode for the valve or whether motorised 'fail in place'-type valves are acceptable.

Dedicated export line

113 Dedicated export lines on bulk tanks containing petrol should ideally be fitted with fire-safe, fail-closed ROSOVs; this would be the minimum expectation for a new tank installation. For existing installations, the need to provide ROSOVs retrospectively should be subject to an assessment according to the principles in HSG244. This assessment will need to include consideration of an individual having to enter a hazardous location to manually operate a valve for emergency isolation.

Common import/export lines

114 These lines cannot be provided with a non-return valve and it appears most appropriate to assess the ROSOV requirement, including the failure mode of the valve, based on the export function.

MIIB Recommendation 6

The sector should put in place arrangements to ensure the receiving site (as opposed to the transmitting location) has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) without depending on the actions of a remote third party, or on the availability of communications to a remote location. These arrangements will need to consider upstream implications for the pipeline network, other facilities on the system and refineries.

MIIB Recommendation 7

In conjunction with Recommendation 6, the sector and the Competent Authority should undertake a review of the adequacy of existing safety arrangements, including communications, employed by those responsible for pipeline transfers of fuel. This work should be aligned with implementing Recommendations 19 and 20 on high reliability organisations to ensure major hazard risk controls address the management of critical organisational interfaces.

115 Appendix 5 sets out detailed guidance on improving safety of fuel transfers. Dutyholders and all other parties involved in the transfer of fuel should:

- adopt the principles for safe management of fuel transfer;
- where more than one party is involved in the transfer operation, ensure that fuel is only transferred in accordance with consignment transfer agreements consistent with those principles;
- ensure that suitable 'job factors' are considered and incorporated into systems and procedures to facilitate safe fuel transfer;
- for inter-business transfers, agree on the nomenclature to be used for their product types;
- for ship transfers, carry out a site-specific review to ensure compliance with the *International Safety Guide for Oil Tankers and Terminals (ISGOTT)*; ¹⁷
- for receiving sites, develop procedures for transfer planning and review them with their senders and appropriate intermediates; and
- ensure that written procedures are in place and consistent with current good practice for safety-critical operating activities in the transfer and storage of fuel.

MIIB Recommendation 8

The sector, including its supply chain of equipment manufacturers and suppliers, should review and report without delay on the scope to develop improved components and systems, including but not limited to the following:

- (a) Alternative means of ultimate high level detection for overfill prevention that do not rely on components internal to the storage tank, with the emphasis on ease of inspection, testing, reliability and maintenance.
- (b) Increased dependability of tank level gauging systems through improved validation of measurements and trends, allowing warning of faults and through using modern sensors with increased diagnostic capability.
- (c) Systems to control and log override actions.

Improved level instrumentation components and systems

116 When selecting components and systems for level measurement or overfill protection systems designers should ensure adequate testability and maintainability to support the required reliability and take account of the safety benefits available in modern components and systems, such as diagnostics. Designers should also take account of the potential advantages of the use of non-invasive systems compared with systems using components inside the tank. Data retrieval and display systems with software features which assist operator monitoring during tank filling should be considered.

Overflow detection

117 Overflow detection is a mitigation layer and not a preventative layer and hence is of secondary priority to overflow prevention. Examples of detecting a loss of containment at a fuel storage installation are by operator detection directly or by monitoring CCTV display screens.

118 There are currently no standards for use of gas detectors for fuel storage installations and no fuel storage installations within the UK where gas detectors are installed. Gas detectors are available but the dispersion of gasoline vapour is complicated and hence effective detection by gas detectors is subject to many uncertainties. Open path detection devices are available and could provide boundary detection at bund walls or around tanks. Liquid hydrocarbon detectors, however, may offer effective detection because it is easier to predict where escaping liquid will collect and travel. There are a number of installations where liquid hydrocarbon detectors are installed. Typical locations would be in a bund drain, gutter or sump where sensors can detect oil on water using conductivity measurement. The detection system may be subject to failures or spurious trips

resulting from water collecting in the bund or sump. The installation of liquid hydrocarbon sensors at suitable locations connected to alarms in the control room should be considered.

119 The installation of the correct resolution CCTV with appropriate lighting of tanks and bunds may assist operators in detecting tank overflows, so this should also be considered. The action to take on detection of an overflow should be clearly documented, typically as part of an emergency plan.

120 Designers and dutyholders should review how they currently control and log override actions. In general they should consider:

- the need for any overrides – when they may be needed, who should have access to them and their duration;
- the possible impairment of effective delivery of a safety instrumented function created by an override against any safety risks that an inability to override could result in. Such reviews should consider both normal operation and the response to abnormal/emergency situations;
- if current logs would allow the effective identification and review of when overrides are in operation or have been operated.

121 More detailed guidance on the approach to overrides can be found in Appendix 4.

MIIB Recommendation 9

Operators of Buncefield-type sites should introduce arrangements for the systematic maintenance of records to allow a review of all product movements together with the operation of the overfill prevention systems and any associated facilities. The arrangements should be fit for their design purpose and include, but not be limited to, the following factors:

- (a) The records should be in a form that is readily accessible by third parties without the need for specialist assistance.
- (b) The records should be available both on site and at a different location.
- (c) The records should be available to allow periodic review of the effectiveness of control measures by the operator and the Competent Authority, as well as for root cause analysis should there be an incident.
- (d) A minimum period of retention of one year.

122 Dutyholders should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially have developed into a major incident. The records should be retained for a minimum period of one year. Refer to 'Availability of records for periodic review' in Appendix 5.

123 Further information relating to the retention and storage of records for SIS can be found in the guidance provided against Recommendation 2, 'Management of instrumented systems for fuel storage tank installations'.

MIIB Recommendation 10

The sector should agree with the Competent Authority on a system of leading and lagging performance indicators for process safety performance. This system should be in line with HSE's recently published guidance on *Developing process safety indicators* HSG254.

124 Dutyholders should measure their performance to assess how effectively risks are being controlled. Active monitoring provides feedback on performance and a basis for learning to improve before an accident or incident, whereas reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from failures.

125 Appendix 5 provides guidance on establishing process safety performance measures.

Part 3 Engineering against escalation of loss of primary containment

126 Failure of an overfill protection system places reliance on the tank to avoid the uncontrolled loss of primary containment of hazardous substances. The adoption of appropriate design standards should ensure tank integrity and suitable overflow and venting mechanisms. Throughout the life of the tank, integrity of primary containment should be maintained through a process of periodic inspection, maintenance and repair.

MIIB Recommendation 11

Operators of Buncefield-type sites should review the classification of places within COMAH sites where explosive atmospheres may occur and their selection of equipment and protective systems (as required by the Dangerous Substances and Explosive Atmospheres Regulations 2002). This review should take into account the likelihood of undetected loss of containment and the possible extent of an explosive atmosphere following such an undetected loss of containment. Operators in the wider fuel and chemicals industries should also consider such a review, to take account of events at Buncefield.

127 In addition to a dutyholder's responsibility to review their DSEAR (Dangerous Substances and Explosive Atmospheres Regulations) risk assessment on a regular basis (eg using the guidance in *Area classification for installations handling flammable fluids* (EI 15)¹⁸) there are also requirements to undertake reviews if there is reason to believe that the risk assessment is no longer valid or if there has been a significant change. Hazard and risk analysis may be required to ascertain appropriate risk reduction measures through additional layers of protection, as described in the guidance provided for Recommendation 1. DSEAR risk assessments should reflect the findings of the LOPA assessments (see Appendix 2). The need for a suitable and sufficient risk assessment is an ongoing duty and, as further understanding of the mechanisms of the incident becomes available and if additional specific guidance is produced, there may be a need for further reviews. DSEAR risk assessments and the measures to control identified risks should, in addition to any sector or industry-specific guidance, take account of the general guidance contained by the HSE Approved Code of Practice (ACOP) L138¹⁹ and where relevant the additional activity related DSEAR ACOPs:

- *Unloading petrol from road tankers* L133;²⁰
- *Design of plant equipment and workplaces* L134;²¹
- *Storage of dangerous substances* L135;²²
- *Control and mitigation measures* L136;²³ and
- *Safe maintenance, repair and cleaning procedures* L137.²⁴

Reference should also be made to Appendix 2, paragraph 136 when considering the selection of equipment and protective systems.

MIIB Recommendation 12

Following on from Recommendation 11, operators of Buncefield-type sites should evaluate the siting and/or suitable protection of emergency response facilities such as firefighting pumps, lagoons or manual emergency switches.

128 Appendix 6 provides guidance on siting emergency response facilities.

MIIB Recommendation 13

Operators of Buncefield-type sites should employ measures to detect hazardous conditions arising from loss of primary containment, including the presence of high levels of flammable vapours in secondary containment. Operators should without delay undertake an evaluation to identify suitable and appropriate measures. This evaluation should include, but not be limited to, consideration of the following:

- (a) Installing flammable gas detection in bunds containing vessels or tanks into which large quantities of highly flammable liquids or vapour may be released.
- (b) The relationship between the gas detection system and the overfill prevention system. Detecting high levels of vapour in secondary containment is an early indication of loss of containment and so should initiate action, for example through the overfill prevention system, to limit the extent of any further loss.
- (c) Installing CCTV equipment to assist operators with early detection of abnormal conditions. Operators cannot routinely monitor large numbers of passive screens, but equipment is available that detects and responds to changes in conditions and alerts operators to these changes.

129 Refer to the guidance given in response to Recommendation 8 for further details, paragraphs 116–121.

MIIB Recommendation 14

Operators of **new** Buncefield-type sites or those making major modifications to existing sites (such as installing a new storage tank) should introduce further measures including, but not limited to, preventing the formation of flammable vapour in the event of tank overflow. Consideration should be given to modifications of tank top design and to the safe re-routing of overflowing liquids.

130 It cannot be shown, without further research, whether significant modifications to tank top design would have the desired mitigating effect in practice. Where new research or revised design codes indicate that modification of tank tops may reduce the formation of vapour clouds, then these should be adopted.

131 New tanks should be designed to BS EN 14015 or API 650 (or equivalent) as these offer up-to-date standards providing in-depth guidance on design and construction elements for vertical cylindrical atmospheric storage tanks.

132 New tanks should be of single-bottom design, which can be supported by suitable inspection arrangements providing the optimum configuration for ensuring continuing integrity. This will facilitate full non-destructive examination of floor-plate welds.

133 BS EN 14015 offers an alternative double bottom configuration. Provided robust integrity management arrangements are in place, in line with guidance set out in EEMUA 159 and 183,²⁵ such a configuration, although not preferred, would also be acceptable. EEMUA 183 sets out the technical disadvantages of this option. Arrangements for inspection and maintenance should be carefully considered for such configurations to secure containment integrity.

134 Consideration should be given to the overflow route from vent to bund to ensure that, within the constraints of the design code, obstacles in the overflow route are minimised.

135 Tanks should either be of ‘frangible roof’ construction, or should be equipped with an emergency vent of adequate area to prevent over-pressure under accidental relief conditions, which exclude internal explosions. For further information reference should be made to EEMUA

180 *Frangible roof joints for fixed roof storage tanks: Guide for designers and users*.²⁶ Emergency vents should comply with an appropriate design standard (API 2000²⁷ or equivalent).

MIIB Recommendation 15

The sector should begin to develop guidance without delay to incorporate the latest knowledge on preventing loss of primary containment and on inhibiting escalation if loss occurs. This is likely to require the sector to collaborate with the professional institutions and trade associations.

136 EEMUA 159 and API 653²⁸ represent relevant good practice and should form the basis of minimum industry standards for tank integrity management and repair to prevent loss of primary containment.

137 Industry should also adopt EEMUA 183 *Guide for the Prevention of Bottom Leakage*, particularly with regard to the maintenance and repair aspects for tanks with a double bottom configuration.

138 HSE guidance *Integrity of atmospheric storage tanks* SPC/Tech/Gen/35²⁹ highlights the factors to consider when operating storage tanks containing hazardous substances and includes reference to EEMUA 159 and API 653.

Internal/out-of-service inspections

139 The scope of inspections, detailed in EEMUA 159 and API 653, acknowledges the typical tank failure modes including corrosion, settlement and structural integrity and provides good guidance for early detection and measurement of symptoms that could lead to failure.

140 A written scheme of examination is required for internal/out-of-service inspections. EEMUA 159, Appendix B2 provides an example of such a checklist.

141 EEMUA 159 and API 653 provide guidance on inspection intervals by either fixed periodicity or by a risk-based methodology. The tables of fixed inspection intervals within this guidance can be used where there is little or uncertain tank history available. A risk-based inspection (RBI) approach allows the use of actual corrosion rates and performance data to influence the most appropriate inspection interval. An example of such a risk assessment is also shown in CIRIA 598.³⁰

142 Many companies have their own technical guidance on tank inspection, maintenance, and engineering best practices, in addition to established RBI programmes. In such cases they are best placed to determine inspection frequencies informed by inspection history. HSE research report RR729 (*Establishing the requirements for internal examination of high hazard process plant*)³¹ establishes relevant good practice covering RBI assessment of hazardous equipment.

143 The frequency of internal/out-of-service inspections should be routinely reviewed and in the light of new information. Inspections may become more frequent if active degradation mechanisms are found.

144 Particular attention should be given to insulated storage tanks, as corrosion under insulation and external coating prior to insulation can have significant effects on tank integrity. For corrosive products protective coatings may be applied internally. This may lengthen the inspection interval. To ensure quality control, particular attention should be paid during the application of coatings.

145 Thorough internal inspections can only be carried out by removing the tank from service and cleaning. As a minimum, a full-floor scan along with internal examination of the shell to annular/floor weld, annular plate and shell nozzles using non-destructive testing and visual inspection in line with good practice.

146 Operators of floating roof tanks should have a system in place to manage water drains appropriately to ensure precautions have been taken to prevent loss of containment incidents. HSE document *Drainage of floating roof tanks* SPC/Enforcement/163³² provides additional guidance on this topic.

External/in-service inspections

147 A written scheme of examination is required for external/in-service inspections. EEMUA 159 provides an example of such a checklist.

148 Thorough internal inspections must be supplemented by external/in-service inspections. These inspections must be completed periodically, as this forms a part of obtaining the overall tank history and assessing fitness for future service. In-service inspection frequency may be determined through RBI assessment or may be based on fixed intervals (see EEMUA 159) based on the type of product stored. Frequency of in-service inspections should be subject to review and may become more frequent if active degradation mechanisms are found.

149 Full guidance for routine operational checks is provided in EEMUA 159 and API 653. These documents also provide guidance on internal and external mechanical inspections to be undertaken by a trained and competent tank inspector. All inspections and routine checks should be documented. Evaluation should include fixed roof venting, floating roof drainage and general operation.

Deferring internal examinations

150 Deferral of the required inspection date must be risk assessed by a competent person. Where necessary, deferral decisions should be supported by targeted non-destructive testing. This additional testing can be carried out to the shell, roof and in many cases annular plate. Deferral decisions must also consider previous inspection history and other relevant information including changes in operating conditions, etc.

151 Particular attention should be given to tanks that have had no previous internal examination as the probability of floor failure will increase with every year that the recommended interval is exceeded. In such cases it is unlikely that a deferral could be justified. It is the dutyholder's responsibility to ensure that the risk of loss of containment is properly managed.

Competency

152 When assessing storage tanks, users should use competent personnel who are aware of and able to apply relevant tank design codes where necessary. Competent personnel may be directly employed or accessed on a contractual basis by the user. Tank assessors should be qualified to EEMUA 159 Tank Integrity Assessor level 1 (minimum) or equivalent. The API 653 Tank Inspector qualification is also acceptable.

153 EEMUA 159 takes into account the requirements of both BS 2654 (now succeeded by BS EN 14015) and API 653.

154 Regular online operational checks can be undertaken by suitably trained personnel with the competencies required to carry out such checks properly.

Remedial work

155 Tank repair is a specialised activity, and should be performed only by those competent in tank design, reconstruction and repair works. Non-destructive testing should be carried out by personnel qualified to TWI's Certification Scheme for Welding and Inspection Personnel or Personnel Certificate of Non-Destructive Testing, or equivalent.

156 Repair options are detailed in API 653. For floor plate repairs, if local overplating or plate replacement is not deemed appropriate, the original floor plates should be removed and a new floor installed.

157 The disadvantages of double bottom designs (including, settlement, product entrapment and modification to nozzle compensating plates) are detailed in EEMUA 183.

158 BS EN 14015 requires that a loss of vacuum in a double bottom tank should alarm to alert the operator that either the upper or lower floor has failed (effectively reverting to a single layer of protection). Remedial action should be carried out within one year. Continued operation in the interim period pending repair should be supported by a technical justification confirming ongoing fitness for service.

159 Having completed a tank inspection, repair and any additional testing, a new risk- or time-based inspection frequency should be determined, taking into account all relevant factors including the condition of the tank, future service requirements, potential degradation mechanisms and failure consequences.

MIIB Recommendation 16

Operators of **existing** sites, if their risk assessments show it is not practicable to introduce measures to the same extent as for new ones, should introduce measures as close to those recommended by Recommendation 14 as is reasonably practicable. The outcomes of the assessment should be incorporated into the safety report submitted to the Competent Authority.

160 Ensuring risks are ALARP is a continuous improvement process. Good practice therefore requires a periodic assessment of existing tanks against current standards. As a minimum, existing tanks should comply with a relevant recognised design code at their date of manufacture. Where this is not the case, tanks should be assessed against an appropriate current standard, BS EN 14015 or API 650. Remedial action should then be taken, as necessary, informed by the resulting gap analysis, to reduce risks ALARP.

161 Where major modifications or repairs are undertaken on existing tanks these should comply with a suitable recognised standard, BS EN 14015 or EEMUA 159.

162 A single floor arrangement is preferred as this best supports thorough inspection and ongoing integrity management to prevent loss of containment. Tanks with a replacement floor fitted above a failed single floor are still deemed single bottom tanks, reliant on the integrity of a single floor.

163 A tank with a double bottom arrangement which does not comply with a recognised standard should be assessed against a recognised standard and any appropriate remedial action taken.

164 Tank top modification should be considered where appropriate to eliminate any obstructions present in the overflow route from vent to bund.

165 Emergency vents that do not comply with a suitable, recognised design standard at date of manufacture should be subject to a design gap analysis, and remedial action taken.

Part 4 Engineering against loss of secondary and tertiary containment

166 While priority should be given to preventing a loss of primary containment, adequate secondary and tertiary containment remains necessary for environmental protection and safety of people in the event of a loss of primary containment of hazardous substances. The failure of secondary and tertiary containment at Buncefield contributed significantly to the failure to prevent a major accident to the environment (MATTE).

167 The final report of the MIIB on the Buncefield Incident of 11 December 2005 provides two recommendations covering engineering against loss of secondary and tertiary containment. These are detailed below.

MIIB Recommendation 17

The Competent Authority and the sector should jointly review existing standards for secondary and tertiary containment with a view to the Competent Authority producing revised guidance by the end of 2007. The review should include, but not be limited to the following:

- (a) Developing a minimum level of performance specification of secondary containment (typically this will be bunding).
- (b) Developing suitable means for assessing risk so as to prioritise the programme of engineering work in response to the new specification.
- (c) Formally specifying standards to be achieved so that they may be insisted upon in the event of lack of progress with improvements.
- (d) Improving firewater management and the installed capability to transfer contaminated liquids to a place where they present no environmental risk in the event of loss of secondary containment and fires.
- (e) Providing greater assurance of tertiary containment measures to prevent escape of liquids from site and threatening a major accident to the environment.

MIIB Recommendation 18

The Competent Authority and the sector should jointly review existing standards for secondary containment. Revised standards should be applied in full to new build sites and to new partial installations. On existing sites, it may not be practicable to fully upgrade bunding and site drainage. Where this is so operators should develop and agree with the Competent Authority risk based plans for phased upgrading as close to new plant standards as is reasonably practicable.

168 The COMAH CA Containment Policy was issued in February 2008 and Containment Policy Supporting Guidance was issued in April 2008. These can be accessed at the following website <http://www.environment-agency.gov.uk> or the direct web page link: Environment Agency – COMAH containment policy. The sector has been reviewing its measures in relation to secondary and tertiary containment and implementing improvement programmes to ensure that the minimum standards of control are in place and that the risk to the environment and associated risks to people (for example, preventing uncontrolled flows of flammable liquids) are as low as reasonably practicable (ALARP).

169 The phase of implementing good practice has raised a number of practical issues from the field. This section of the PSLG Final Report provides further information on these aspects.

Bund lining systems

170 The COMAH Containment policy states that ‘Bunds shall be impermeable’ and that ‘bunds shall have fire resistant structural integrity, joints and pipework penetrations’. This covers the preparation of the tank base and foundation plus the selection of lining systems; concrete, earth or polymeric or polymeric and mineral composites.

171 It is important that protection from fire is included in risk assessment for selecting different types of lining systems.

172 The series of testing standards BS 476: *Fire tests on building materials and structures: Guide to the principles and application of fire testing*³³ provides a good guide.

173 There is no consolidated set of standards and guidance covering the options for lining systems for existing tanks addressing both the issue of what to do under the tank and the application of the selected system.

174 The selection of any system is based on a combination of risk (to the environment and people), cost and practicality. Any consideration of improvements to lining systems for existing establishments where the risk is tolerable should be subject to an ALARP assessment.

175 Table 2 provides examples of some commonly used lining systems. Advantages and disadvantages may vary subject to site conditions. The list is indicative only and not exhaustive. Fire resistance is covered in the table to reflect the current knowledge of performance based on product information, performance in fire incidents and some testing that has been carried out by Operators. Further testing is recommended on the relative performance of these lining systems where information is lacking. This testing may also be used to optimise system designs.

Table 2 Lining system options

Option	Advantages	Disadvantages	Fire resistance	Cost**
Concrete	<ul style="list-style-type: none"> – Proven durability – Able to cast around penetrations – Well suited to small congested areas – Hydrocarbon resistance 	<ul style="list-style-type: none"> – Requires joints for construction and movement – Requires regular maintenance of joint and penetration sealants and cracks – Can buckle under heat – Net excavation waste can be high – Potential for settlement and cracking 	<ul style="list-style-type: none"> – Very Good – Joints and penetrations are the weakness 	High
Bentonite (geosynthetic clay liner) (pre-hydrated or dry bentonite requiring in situ hydration)	<ul style="list-style-type: none"> – Hydrocarbon resistance – Lower maintenance – Self-sealing properties if punctured. – Pre-hydrated can be laid at performance specification required 	<ul style="list-style-type: none"> – Requires a protection layer. – Potential hidden problems at penetrations. – Potential for drying out on slopes – In situ hydration of dry systems to achieve performance specification required – Can be uncertain 	<ul style="list-style-type: none"> – Good as geotextile mat protected by layer of soil/stone 	Medium

Option	Advantages	Disadvantages	Fire resistance	Cost**
Fibreglass	<ul style="list-style-type: none"> – Easy application – Suited to small areas – Hydrocarbon resistance 	<ul style="list-style-type: none"> – Inflexibility needs to be catered for in design to allow for thermal movements and avoid overstress and de-bonding 	<ul style="list-style-type: none"> – Low – May require additional fire protection measures 	Low
Clay	<ul style="list-style-type: none"> – Inert material that has retained plasticity once in place – Hydrocarbon resistance 	<ul style="list-style-type: none"> – Labour intensive, weather dependent and time consuming activity in spreading and compacting the clay requiring significant vehicle movements – May not be safe to carry out installation whilst tanks are in service due to machinery requirements 	<ul style="list-style-type: none"> – High (non-combustible thick malleable layer) – Normally covered with top soil layer which provides further resistance 	Medium
Sand bitumen	<ul style="list-style-type: none"> – Remains flexible after installation – Resistant to puncture – Cracks can be repaired easily using hot bitumen – Hydrocarbon resistance 	<ul style="list-style-type: none"> – Specialist small plant required to work on bund wall slopes – Limitations on application for steep slopes – May require renewal before 25 years – Not suitable for floors 	<ul style="list-style-type: none"> – Performance not proven. – Expected to be 'Medium' based on bitumen road surfacing performance in vehicle fires – Material is combustible 	Low
Shotcrete (spray applied concrete)	<ul style="list-style-type: none"> – Ease and speed of installation as concrete is sprayed on – Plant can be operated from outside the bund if necessary – Proven durability – Able to cast around penetrations – Hydrocarbon resistance 	<ul style="list-style-type: none"> – Specialist contractors required – Requires joints for construction and movement – Requires regular maintenance of joint and penetration sealants and cracks – Can buckle under heat 	<ul style="list-style-type: none"> – Very Good – Joints and penetrations are weakness 	Low
Poly-vinylchloride (PVC)	<ul style="list-style-type: none"> – Resistant to oils and water 	<ul style="list-style-type: none"> – Not resistant to fuels – Requires protective layer – Potential hidden problems around seals and penetrations – Base ground to be prepared well, ie remove stones, requires a layer of gravel and sand/ geotextile before the liner – Requires specialist installer to weld joints 	<ul style="list-style-type: none"> – Very Low – Burns readily if unprotected 	Medium
Poly-urethane (PU)	<ul style="list-style-type: none"> – Water resistant 	<ul style="list-style-type: none"> – Not resistant to oils and fuels – Requires protective layer 	<ul style="list-style-type: none"> – Very Low – Burns readily if unprotected 	Medium

Option	Advantages	Disadvantages	Fire resistance	Cost**
Poly-ethylene (HDPE)	<ul style="list-style-type: none"> Resistant to water, hydrocarbons and most chemicals 	<ul style="list-style-type: none"> Requires protective layer Potential hidden problems around seals and penetrations Base ground to be prepared well, ie remove stones, requires a layer of gravel and sand/ geotextile before the liner Requires specialist installer to weld joints 	<ul style="list-style-type: none"> Very Low Burns readily if unprotected 	Medium
Poly-propylene (PP)	<ul style="list-style-type: none"> Resistant to water and oils Easier to lay than HDPE 	<ul style="list-style-type: none"> Limited resistant to fuels Requires protective layer Potential hidden problems around seals and penetrations Base ground to be prepared well, ie remove stones, requires a layer of gravel and sand/ geotextile before the liner Requires specialist installer to weld joints 	<ul style="list-style-type: none"> Very Low Burns readily if unprotected 	Medium
Synthetic rubber and EPDM	<ul style="list-style-type: none"> Resistant to water 	<ul style="list-style-type: none"> Not resistant to oils and fuels Requires protective layer 	<ul style="list-style-type: none"> Very Low Burns readily if unprotected 	Medium

** Costs are indicative and may vary based on installation issues and scale.

Fire resistance and integrity of pipe penetrations and expansion joints

176 The COMAH Containment policy states that: ‘Bunds shall have fire resistant structural integrity, joints and pipework penetrations.’

177 Improvements should be made to the fire resistance of bund joints and penetrations where the existing arrangement has inadequate fire resistance. Options for enhancing fire resistance of new designs and existing situations where reasonably practical if the risk is tolerable are covered in the following sections.

178 The objective is to retain the integrity of a bunded area as long as possible in the event of a fire. Concrete and clay have inherent fire resistance, but the risk of a loss of integrity is provided by joints and penetrations to the bund walls and floors and the way these features are sealed.

179 Sealants are now available which have enhanced fire resistance. The fire-resistance standards commonly referenced are BS 476-20:1987³⁴ and BS 476-22:1987.³⁵ The maximum fire resistance quoted in BS 476 is four hours.

180 Tests of fire rated and non fire rated joint sealants in combination with steel plates indicate that fire rated sealants provide improved fire resistance.

181 In considering the use of fire-resistant sealants, due regard should also be given to the suitability and compatibility of candidate products (for example hydrocarbon and water resistance) in the specific application.

182 Waterstops are integral design and construction features of concrete structures whose duty is to retain liquids. Good practice for the minimisation of leakage from concrete bunds includes the use of waterstops within movement joints, in accordance with BS 8007. In order to

meet both fire and corrosion resistance performance requirements metal waterstops should be used on new build and where reasonably practical if the risk is tolerable for existing bunds – as described in paragraphs 209–216.

183 Waterstops are defined in BS 8007 Appendix C3: ‘Waterstops are preformed strips of durable impermeable material that are wholly or partially embedded in the concrete during construction. They are located across joints in the structure to provide a permanent liquid-tight seal during the whole range of joint movements.’

184 Following the Buncefield incident it was recognised that the addition of steel plates to cover the inside faces of movement joints provided enhanced fire resistance to existing joints. It was recommended that improvements to existing bunds containing gasoline tanks should be made by replacing existing sealants with fire-resistant versions and, in addition, fitting steel cover plates where physically possible to fit. This proposal of the combination of cover plate and fire-resistance sealant is recommended as good practice retrofit solution for existing installations, where routine inspection of the sealant is carried out. See paragraphs 205–212 for further information.

185 From the information available regarding waterstops and steel plates, the following statements are reasonable:

Fire resistance:

- Metal waterstops are effective at resisting fire.
- Steel plates are a practical method of greatly enhancing fire resistance and minimising loss of integrity to joint materials due to fire.

Leakage:

- Waterstops provide the most effective way of minimising leakage from bund joints.
- Steel plates have been seen to significantly reduce leakage rates due to their role in providing protection to sealants and vulnerable plastic waterstops.
- They have not been seen to be as effective at minimising leakage in the same way as waterstops which are integral to the joint design.

Design of steel plate fire protection

Determined by the specific circumstances of their application. However, the following general guidance is useful:

- material of construction: stainless steel;
- width: minimum 20 cm;
- thickness: minimum 6 mm;
- fixings to bund walls: stainless steel bolts through oversized slotted holes.

(Note: Oversize holes cater for vertical expansion of the plate in a fire, whilst horizontally slotted holes allow for movement of the walls where the plate is bolted to both sides of the joint plates can be fabricated in short sections to limit the weight when fixing, with a lap detail to cover plate junctions – see Figure 3.)

Figure 3 An example of a design with fixing to one side of the joint only



Pipe penetrations: general

186 HSG 176 *The storage of flammable liquids in tanks*³⁶ states that:

- where reasonably practicable electrical equipment should be installed in non-hazardous areas ... and ... where this cannot be done, equipment should be selected, installed and maintained in accordance with BS 5345 *Code of practice for the selection, installation and maintenance of electrical apparatus for use in potentially explosive atmospheres** (or other equivalent standard), paragraph 38;
- pumps are potential ignition sources and should be located outside the bund – this will also avoid damage from fires or spillages in the bund and facilitate access for maintenance (and in practice the bund should not be considered to be a normal operational area), paragraph 104;
- the bund should be liquid tight ... andthe integrity of the bund wall may be put at risk if pipework and other equipment are allowed to penetrate it. If it is necessary to pass pipes through the bund wall, for example to the pump, then the effect on the structural strength should be assessed. Additional measures may be needed to ensure that the bund wall remains liquid tight.

187 It is common practice within some parts of the chemical industry to situate ATEX rated pumps in bunds, for operational or space reasons.

188 Recommendation 11 of the Buncefield MIIB report addresses the connected issue of “the classification of places within COMAH sites where explosive atmospheres may occur and their selection of equipment and protective systems (as required by the Dangerous Substances and Explosive Atmospheres Regulations 2002).

189 The COMAH Containment policy states that: “Bunds shall have no pipework that penetrates through the bund floor; no pipework that penetrates through the bund walls as far as reasonably practicable, otherwise it shall be with adequate sealing and support.”

190 Designing and modifying pipe systems to avoid pipe penetrations may be operationally difficult due to pumps, located outside the bund, requiring flooded suction lines at all tank inventory levels. Under these circumstances pipeline penetrations will be required.

191 If pipes do not have a continuous fall from the tank to the pump then:

- pumps cannot be primed (particularly when stop/starting pumping at low tank levels);
- retention of a pressure differential between tank and serving pump to ensure suction throughout the working volume of the tank may be compromised;
- lines would have to be drained and cleaned from inside the bund area when changing between products.

192 When these activities are carried out on a regular basis then pipes will need to pass through the bund wall. Where they do, structural effects should be assessed and penetrations should be designed to be liquid tight and fire resistant.

193 Smaller tanks can be installed at an elevated position and achieve line falls whilst avoiding pipe penetrations but this is generally not a practical solution for larger tanks (for example with a volume greater than 100 m³).

* Many of the sections of this code have been superseded/withdrawn. The application of the BS EN 60079³⁷ suite of standards is more appropriate and this is also referred to in HSG176. It covers selection of equipment, area classification, maintenance and inspection etc.

194 Top entry pipes can be considered for filling tanks to avoid wall penetrations. For tanks that are emptied on a regular basis however this should be avoided as splash filling cannot be avoided at the start of the filling operation. This is particularly important where flammable static-generating products are being handled.

Pipe penetrations: new builds/major upgrade work

195 The BSTG puddle flange design (as shown in the following figures) inherently provides fire resistance and offers industry a sound design.

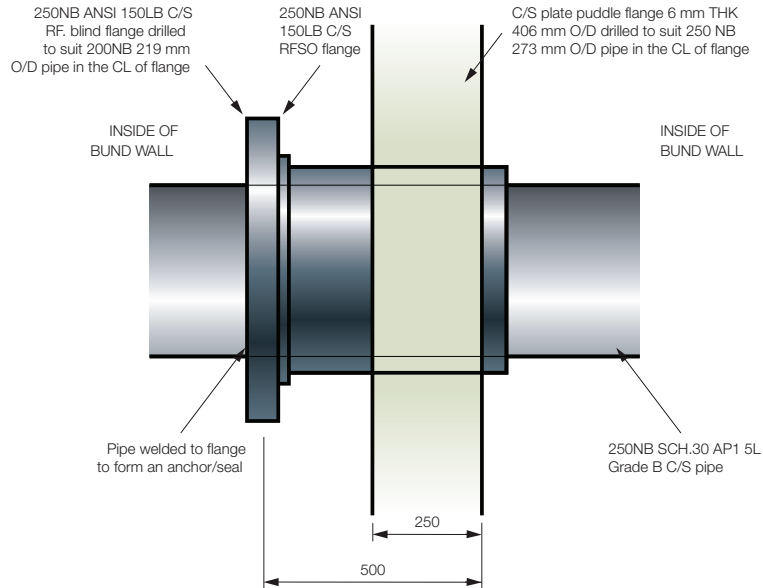


Figure 4 Example puddle flange cast into a bund wall

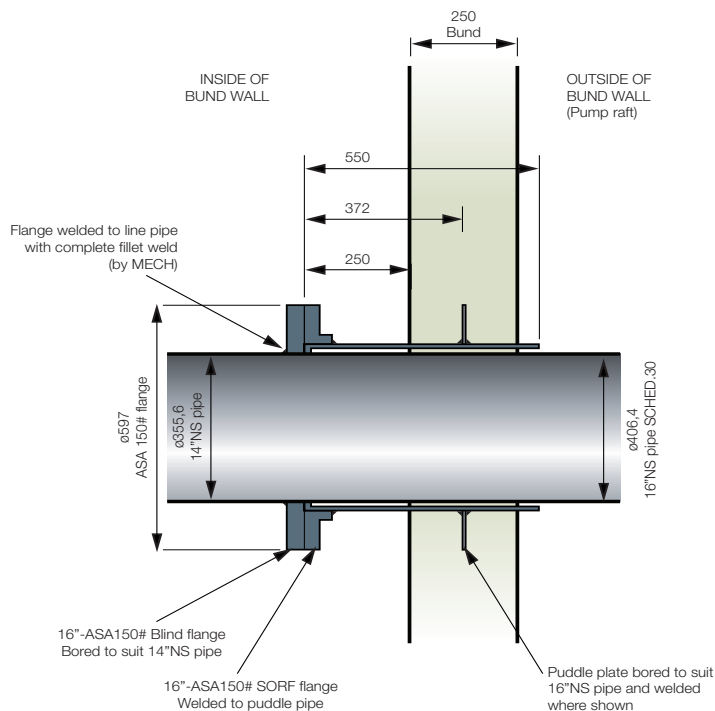


Figure 5 Example puddle flange for 14" BS pipe

196 It is important to note that this arrangement acts as an anchor for the pipe. When it is used the pipe arrangement between this anchor and the tank nozzle should allow sufficient flexibility to ensure forces on both the bund wall and tank shell are minimised and within design limits.

197 This is relatively easy to achieve for smaller pipe sizes (<16") and for new terminals where flexible pipe routing can be designed. For larger line sizes with greater temperature variations this design may not be workable, particularly for existing terminals with short distances between the tank and bund wall, where expansion loops cannot easily be added to the pipe layout. Under these circumstances alternative arrangements which allow for some movement of the pipe may need to be considered as seen in Figures 6, 7 and 8.

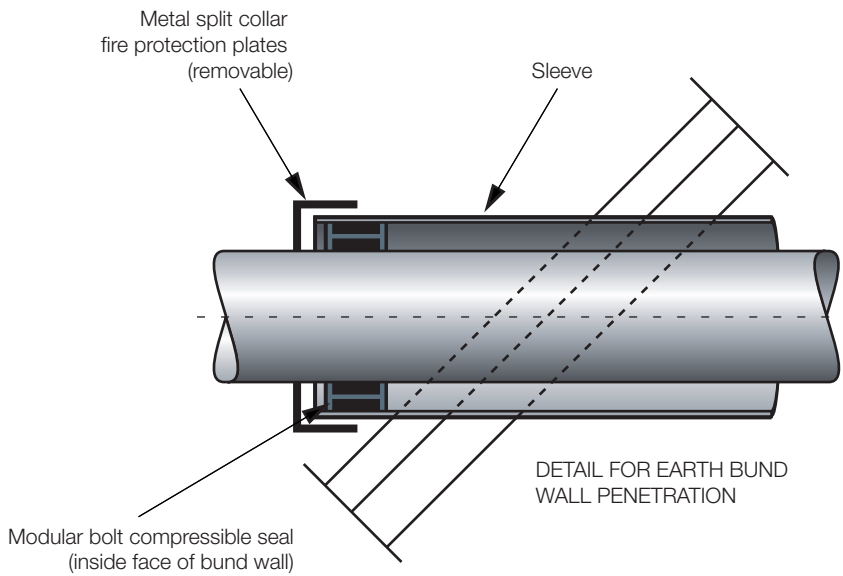


Figure 6 Detail for earth bund wall penetration

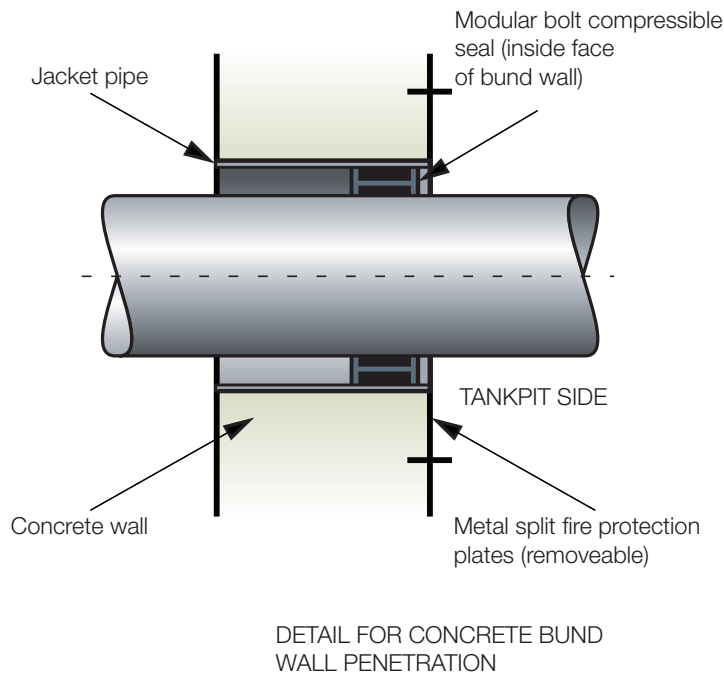


Figure 7 Detail for concrete bund wall penetration

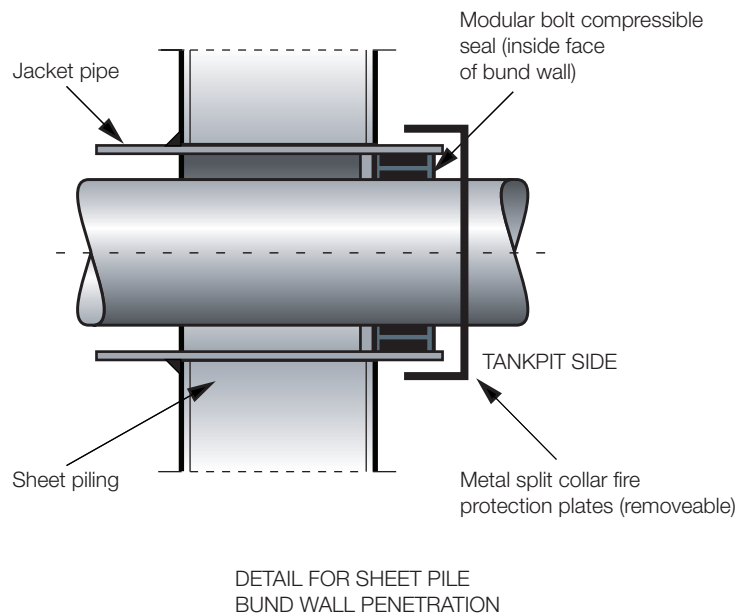


Figure 8 Detail for sheet pile bund wall penetration

198 The BSTG puddle flange arrangement has been used by operators for a number of years. As long as the space between the pipe and external sleeve remains free from debris, allows visual examination of the space and the pipe does not come into contact with the sleeve, it will provide a crevice-free arrangement that is relatively easy to maintain.

199 For the alternative arrangement there is a higher possibility of crevice corrosion between the pipe and the sleeve packing. For this reason pipe protective coatings and materials should be carefully selected for this detail and regular inspections should be carried out to ensure that protective coatings and seal arrangements remain in good condition and corrosion of the pipe is not taking place.

200 It is recommended that the fire rating of the link seal is carefully considered and future fire testing should be carried out to confirm the observed suitability of these pipe penetration arrangements.

Pipe penetrations: existing pipe penetrations

201 The upgrading of existing pipe penetrations to provide a liquid tight, fire proof corrosion free joint is more difficult to achieve. Any upgrade should be carefully reviewed to ensure that the upgraded penetration does not affect pipe flexibility and integrity. A summary table is provided below paragraph 206 outlining the main existing pipe penetrations details and methods of upgrade.

202 Terminals have utilised several designs for existing pipe penetrations through bund walls. Some of the methods are shown in Figure 9: straight-through; puddle flange; and sleeved arrangement. These can be assessed and/or applied based on ALARP principles if the risk is tolerable.

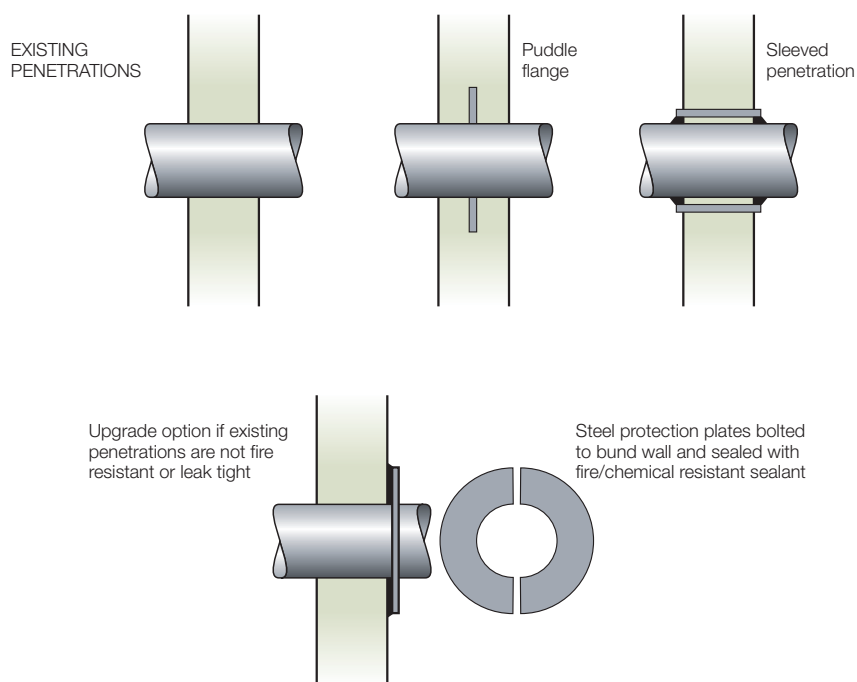


Figure 9 Designs for pipe penetrations through bund walls

203 Where the operator does not consider the existing joints to be fire resistant or leak tight, one upgrade option would be to bolt on a steel protection ring (split for installation) sealed with fire/chemical resistant sealant. This is similar in principle to the steel plates for expansion joints covered in the next section. Slit plates can be installed by cold methods without the need for removing the pipeline from service for modification and welding.

204 For existing pipes running through bund walls there are genuine concerns regarding possible corrosion crevices between the pipe and the wall. An upgrade option which has been used is to reduce the pipe size (only local to the penetration) and use the existing pipe as a sleeve with the BSTG puddle flange arrangement. This then allows various options to seal between the sleeve and bund wall without concerns for thinning of the product pipe (primary containment). Regular inspection is still required to ensure that long-term corrosion of the sleeve (secondary containment) does not provide a leak path from the bund.

205 Figure 10 provides a detail for a sealed sleeve upgrade option.

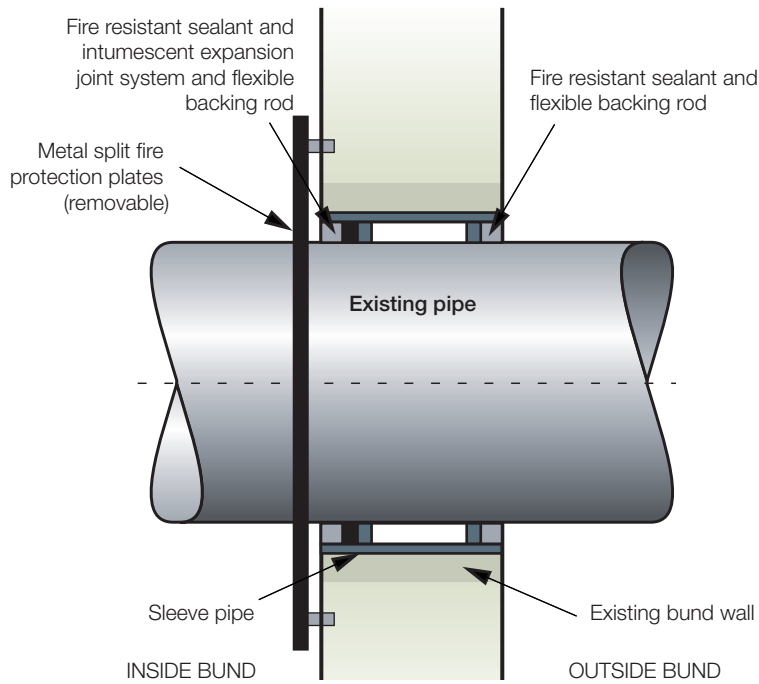
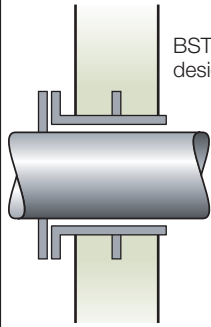
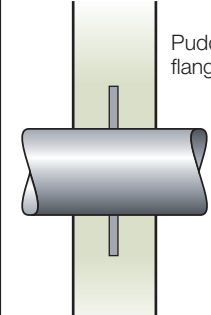
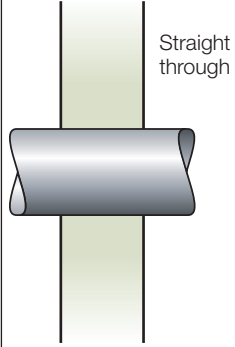
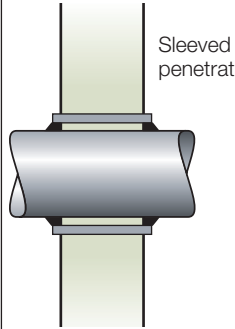


Figure 10 Detail for a sealed sleeve upgrade option

206 For sleeved penetrations, it may also be possible to seal between the sleeve and pipe using a proprietary (product and fire resistant) compression seal ring.

Table 3 Pipe penetrations

Existing Pipe Penetrations				
Design	Arrangement sketch	Fire and product resistant sealants	Acceptable standards	Required upgrade
BSTG Design	 <p>BSTG design</p>	Not applicable – design inherently fire and product resistant	Acceptable and good practice for existing plant; best practice for new build	No upgrade required Ensure product pipe is externally protected against corrosion – coated or wrapped
Puddle Flange Arrangement	 <p>Puddle flange</p>	Not applicable – design inherently fire and product resistant	Acceptable for existing plant but with inspection and maintenance regime	No upgrade required

Existing Pipe Penetrations				
Design	Arrangement sketch	Fire and product resistant sealants	Acceptable standards	Required upgrade
Straight-through Type Arrangement		No existing sealant	Acceptable for existing plant but operator to assess requirement for fire and product resistant sealant	Consider installing fire and product resistant sealants For pipelines which indicate substantial horizontal movement, upgrade option to install cover plates with sealants to retain joint integrity
Sleeved Arrangement		Existing sealant not fire or product resistant	Upgrade required with inspection and maintenance regime	Install fire and product resistant sealants and install fire protection steel cover plates (see paragraph 206)

Pipe penetrations: anchoring

207 Puddle flange arrangements act as anchor points and are inherently fire and product resistant. The sleeved arrangement does not act as an anchor and the sealant accommodates minor vertical and horizontal movements.

208 The straight-through type arrangement, although offering pipeline restraint in the vertical direction, allows horizontal movement and is therefore difficult to seal. If the extent of movement is such that sealants do not retain the joints' integrity, then an upgrade solution to install cover plates should be considered.

Bund wall expansion and construction joints

209 Bund wall expansion joints are important to ensure ongoing bund structural integrity. In addition they need to provide a liquid tight, fireproof joint.

210 New joints should be installed with metal waterstops and fireproof joints. Waterstops fabricated from stainless steel or copper are in use at terminals and the choice of metal is informed by performance requirements.

211 Where practicable, existing joints should be upgraded to provide waterstops and/or fireproof joints. There are realistic methods available – however it is recognised that retrofitting waterstops to existing bund wall joints is not a simple task and it may degrade the joint integrity.

212 The following lists a range of possible existing bund wall joint arrangements and reviews product resistance, fire resistance and upgrade options for each arrangement.

- a A joint with a stainless steel waterstop and fire- and product-resistant sealants – This meets current good practice and no upgrade would be required. It is unlikely to have a significant rate of liquid egress from the joint during an incident, with or without fire.

- b A joint with a plastic waterstop and stainless steel cover plate designed to ensure product and fire resistance to BS 476 – This meets current good practice and no upgrade would be required. It is unlikely to have a significant rate of liquid egress from joint although loss of integrity of the plastic waterstop may eventually occur after protracted heat exposure.
- c A joint with no waterstop but with a stainless steel cover plate, with product and fire-resistant sealants designed to ensure fire resistance to BS 476 – This joint may be considered to be fire resistant and would be considered impermeable (liquid tight) whilst the product-resistant sealant remains in good condition. Leakage rate through movement of the joint would also be expected to increase with sealant ageing and hence frequent sealant inspection and replacement routines shall be in place to ensure sealants remain in a good condition.
- d A joint with no waterstop, no cover plate but with product- and fire-resistant sealant – This joint only provides limited fire resistance and is impermeable only when the product-resistant sealant remains in good condition. Leakage rate through movement of the joint would be expected to increase with sealant ageing. As a minimum, this should be upgraded with a stainless steel cover plate and inspection and replacement routines shall be in place to ensure sealants remain in good condition.
- e A joint with product-resistant sealant but no waterstop, no stainless steel cover plate and no fire-resistant sealants – This joint will be impermeable whilst the sealant remains in good condition but is not fire-resistant, and would be expected to leak rapidly following a fire. Leakage rates through movement of the joint would be expected to increase with sealant ageing. As a minimum, this joint should be upgraded with a stainless steel cover plate and fire-resistant sealants. In addition, inspection and replacement routines shall be in place to ensure sealants remain in good condition.

Table 4 The potential for bund failure

Bund Wall Expansion and Construction Joints					
Text para	Waterstops	S/S cover plates	Fire-/product-resistant sealants	Acceptable standard	Required upgrade
a	Stainless steel	None	Yes	Acceptable and good practice for existing plant Best practice for new build	None required
b	Plastic	Yes	Yes	Acceptable and good practice	None required
c	None	Yes	Yes	Acceptable and good practice for fire resistance and for existing bunds only acceptable for minimising leakage provided an adequate inspection and maintenance regime was in place (see paragraph 213)	None required for fire resistance Upgrade for bund integrity dependent on extent of tertiary containment
d	None	None	Yes	Upgrade required and inspection and maintenance regime	Install S/S cover plates to achieve c
e	None	None	None	Upgrade required and inspection and maintenance regime	Install S/S cover plates and fire resistance to achieve c

213 The process of risk assessment assesses the level of risk posed by the establishment as a whole and to inform planning of measures such as tertiary containment and emergency arrangements. The potential for bund failure from the effects of fire/explosion and failure to retain liquid due to design and construction aspects needs to be recognised to assess the extent to which tertiary containment may be required. The greater the deviation from good practice, the more likely it is bunds will fail and the greater the rate of liquid release from the bund. The paragraph c arrangement in Table 4 does not require upgrade for fire resistance.

214 Where it is difficult to install product-resistant sealants to ensure a liquid tight seal, for example due to the condition of the concrete faces of the joint, it may be practicable to create a new joint with fireproof waterstop on the outside of existing bund wall. This would require two new concrete pillars joined to the outside of the bund wall either side of the existing bund wall joint. A fireproof waterstop joint could be installed between the two new pillars which would then form the new bund wall joint. Care would need to be taken to ensure pillars are supported with suitable foundations and that any new stresses would not lead to cracking of the existing bund wall.

215 It is recommended that a suitable fire test method be agreed and a test programme of trial joints be carried out to confirm the observed suitability of these expansion joint arrangements.

216 Figure 11 shows a design for the BSTG wall joint with stainless steel protective plate.

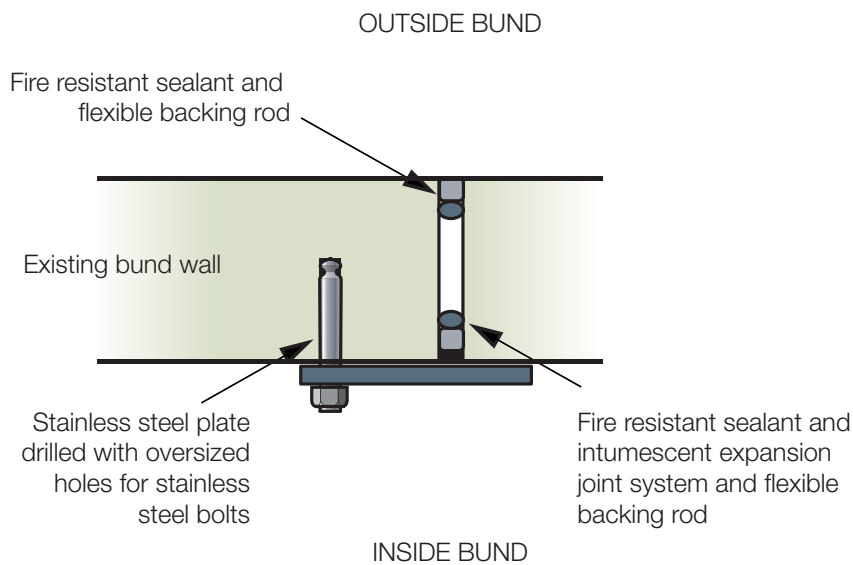
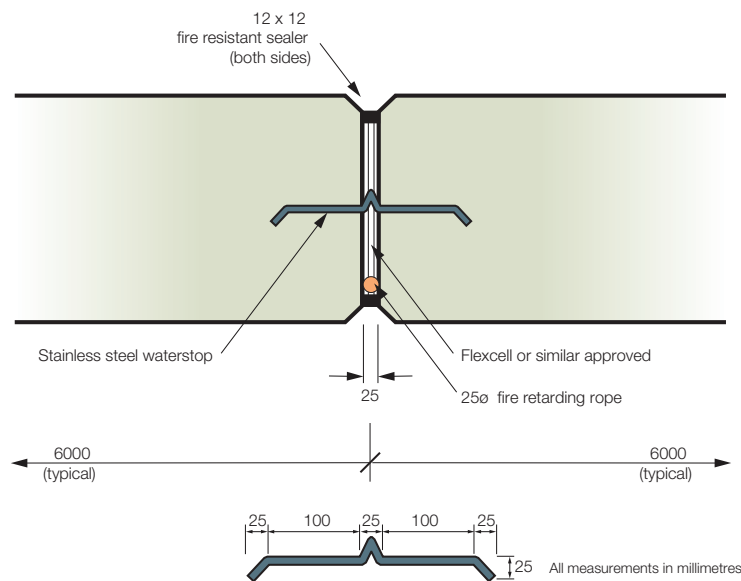


Figure 11 BSTG wall joint with stainless steel

217 Figure 11 shows a bund wall joint with a stainless steel waterstop.



- Notes:**
- 1: Fire retarding rope to be placed on both sides of an internal bund wall
 - 2: Waterstop, rope and fire resistant sealer to be omitted in bundwalls footings
 - 3: Stainless steel for waterbar to be grade 316 and 1.0 mm thick

Figure 12 Example puddle flange cast into a bund wall

Secondary containment systems under tanks

218 In addition to overfill events which are within PSLG scope, there have been a number of significant leaks of gasoline, kerosene and diesel from the base of storage tanks.

219 It is important that secondary and tertiary containment systems are designed to deal with both types of event.

220 The following provide additional guidance:

- API 650 *Welded tanks for oil storage* – Appendix I is the fundamental classic guide to prevent bottom leakage from storage tanks.
- API 340 *Liquid release prevention and detection measures for aboveground storage tanks*.³⁸
- API 341 *A survey of diked-area liner use at aboveground storage tank facilities*.³⁹
- EEMUA 183 *Guide for the prevention of bottom leakage from vertical cylindrical steel storage tanks* – Chapter 3 also provides similar data, but again quotes the API 650 and the repair guide API 653.
- BS EN 14015 *Specification for the design and manufacture of site built vertical cylindrical flat-bottomed above ground storage tanks*.

Basis for bund capacity based on tank capacity

221 Within the PSLG Final Report, particular emphasis is given to overfill prevention as this is the primary means by which this major accident hazard can be prevented. In assessing what overfill prevention measures are required to reduce the risk to the environment to ALARP, the existing capacity of the bund and the tank level it was based on must be taken into account to determine the potential environmental consequences, eg whether the spillage is likely to be retained by the secondary containment system. If the overfill prevention system and the primary containment measures as a whole are in accordance with good practice, the risk to the environment is reduced.

222 The COMAH Containment policy states that: ‘Bunds shall have sufficient capacity to allow for tank failure and firewater management. This will normally be a minimum capacity of either 110% of the capacity of the largest tank or 25% of the total capacity of all the tanks within the bund whichever is the greater.’ It is unclear what is meant by ‘capacity’.

223 Figure 2 in Part 2 of this report 'Overfilling protection: Tank levels' (based on API 2350) gives three levels:

- Normal fill level;
- Tank rated capacity;
- Overfill level.

224 When determining the bund size required, three modes of loss of containment have to be addressed:

- Overfills;
- Leak;
- Catastrophic failure.

225 The bund should be sized for 110% of the 'tank rated capacity' (TRC) as a minimum. This assumes that the minimum standards for overfill protection systems *of control* are in place relating to:

- tank levels and capacities are determined in accordance with Appendix 3;
- position and type of level gauges and high level detectors;
- how are these monitored and the required response;
- response times to shutdown inflow.

226 If – for example, the TRC level is alarmed and the overfill protection system setting is at TRC – it is reasonable to take this as tank capacity.

227 If – for example the TRC level is alarmed and interlocked at – it is reasonable to take this as tank capacity (subject to failure rate of alarm and interlock).

228 Operators should also record overfill volumes to establish the difference in risk between TRC and overfill levels – which may involve significant volumes for larger tanks. This is to be reported for information only.

229 Unless multiple tanks sharing the same bund are hydraulically linked, simultaneous overfill of independent tanks can be discounted as a realistic hazard. Therefore, the 25% criteria would not apply to the Overfill level. For the bund capacity calculation based on 25% of the total capacity of all the tanks, the normal fill levels of all the tanks within the bund should be used.

230 The 25% criterion applies to the risk of loss of containment of more than one tank and provision for firewater management. This provides a buffer to deal with the incident and informs risk assessment as to the degree of tertiary containment that may be required to deal with subsequent failure of secondary containment in a severe and prolonged event. The actual sizing for multi-tank bunds will be determined by the hazard and the risk – including the modifying factors stated above. Where increased bund area leads to larger dispersion distances to a safe vapour concentration, operators may consider providing remote secondary storage.

Bund strength

231 A bund should be capable of withstanding the full hydrostatic head of liquid that may arise from the loss of primary containment.

232 Following catastrophic failure of a tank⁴⁰ – overtopping of a bund to some extent is usually inevitable. In the absence of practical guidance on assessment of bunds for likely levels of overtopping or hydrodynamic loads – emphasis should be placed on mitigation and control of the effects of overtopping through tertiary containment.

Firewater management and control measures

233 Well-planned and organised emergency response measures are likely to significantly reduce the potential duration and extent of fire scenarios, and so reduce firewater volumes requiring containment and management. Site-specific planning of firewater management and control measures should be undertaken with active participation of the local Fire and Rescue Service, and should include consideration of:

- bund design factors such as firewater removal pipework, aqueous layer controlled overflow to remote secondary or tertiary containment (for immiscible flammable hydrocarbons);
- recommended firewater/foam additive application rates and firewater flows and volumes at worst-case credible scenarios (including severe pool fire or multiple tank / multiple bund fire); and
- controlled-burn options appraisal, and pre-planning/media implications.

Tertiary containment

234 This guidance applies only to the loss of secondary containment from bunds containing tanks within the scope (the COMAH CA Containment Policy has a wider scope). At installations where bunds contain tanks within scope, operators should assess the requirement for tertiary containment, on the basis of environmental risk, and to make site action plans for improvement. Provision of tertiary containment should also take into account safety aspects – for example the flows and accumulations of hazardous liquids on and around a site.

235 Tertiary containment minimises the consequences of a failure in the primary and secondary containment systems by providing an additional barrier preventing the uncontrolled spread of hazardous liquid. Tertiary containment is achieved by means external to and independent of the primary and secondary containment systems, such as site drainage and sumps, diversion tanks, impervious liners and/or flexible booms. Tertiary containment will be utilised when there is an event that causes the loss of containment (for example bund joint failure or firewater overflowing from a bund during a prolonged tank fire), and is intended to ensure that loss of control of hazardous materials does not result from such an event.

Risk assessment

236 A risk assessment should be undertaken to determine the extent of the requirement for tertiary containment, taking into account:

- foreseeable worst-case scenario – severe pool fire or multiple tank/multiple bund fire (following an explosion or due to escalation);
- foreseeable bund failure modes, including:
 - the amount of spilled substances, including hydrodynamic effects of catastrophic tank failure and emergency response actions such as fire fighting;
 - the potential impact of fire on bund integrity including joints in walls and floors;
 - worst-case foreseeable delivered firewater volumes including fire fighting agents (see IP19⁴¹); and
 - passive and active firewater management measures.
- environmental setting, including:
 - all relevant categories of receptors as specified in *Guidance on the interpretation of Major Accident to the Environment*; ⁴²
 - proximity of receptor, for example groundwaters under the site;
 - site and surrounding topography;
 - geological factors affecting the permeability of surrounding land and environmental pollution pathways; and
 - hydrogeological factors affecting liquid pollutant flows and receptor vulnerabilities;
- known pathways and potential pathways to environmental receptors in the event of failure of secondary containment;
- likely environmental impact consequences, in terms of extent and severity, of the pollutant and/or firewater quantities and flows resulting from foreseeable bund failure scenarios.

Design standards

237 Based on the scope and capacity determined by the site-specific risk assessment, tertiary containment should be designed to:

- be independent of secondary containment and associated risks of catastrophic failure in a worst-case major accident scenario;
- be capable of fully containing foreseeable firewater and liquid pollutant volumes resulting from the failure of secondary containment;
- be impermeable to water and foreseeably entrained or dissolved pollutants;
- use cellular configuration, to allow segregation of 'sub-areas' so as to limit the extent of the spread of fire and/or polluted liquids;
- operate robustly under emergency conditions, for example in the event of loss of the normal electrical power supply;
- avoid adverse impacts on fire fighting and other emergency action requirements;
- allow the controlled movement of contained liquids within the site under normal and emergency conditions;
- facilitate the use of measures for the physical separation of water from entrained pollutants;
- incorporate practical measures for the management of rainwater and surface waters as required by the configuration; and
- facilitate clean-up and restoration activities.

Transfer systems and routes for tertiary containment should facilitate timely transfer and do not necessarily need to be impermeable – dependent on the environmental risk.

238 For larger establishments on-site effluent facilities, sized to allow collection and treatment of polluted firewater, are an option where justifiable.

Design options

239 Selection of tertiary containment options will be highly dependent on site-specific factors such as layout, topography and available space. The term 'transfer systems' (CIRIA 164⁴³ chapter 13) is used to describe the means for collecting and conveying spillage/firewater to remote and combined secondary and tertiary containment.

240 Design options for tertiary containment include:

- local cellular tertiary containment surrounding secondary containment – gravity fed;
- local gravity collection systems at identified failure points, connected with:
 - gravity transfer to remote containment;
 - pumped transfer to remote containment;
 - tankage dedicated to tertiary containment; and
 - sacrificial land;
- local dedicated gravity drainage and collection sump(s), capable of handling total emergency liquid flows into secondary containment, and connected with pumped transfer to remote containment.

241 Remote tertiary containment may serve more than one secondary containment system, as long as it is designed to be capable of accommodating total foreseeable flows and quantities.

242 Existing secondary containment systems may be used to provide tertiary containment for other secondary containment, as long as foreseeable secondary containment failure scenarios are mutually exclusive and equipment (for example pumps) is independent and reliability of emergency operation is assured.

243 Some tertiary containment assessments have considered the environmental receptors surrounding the installation and potential pathways for pollution flows. However, many concentrated solely on assessing the maximum practical use of installed containment capacity, and determining the consequent fire-fighting attack duration. Buncefield showed that consequences might be much more extensive than expected.

244 Assessment of tertiary containment should start with an initial worst-case assumption that available secondary containment will fail or capacity will be exceeded, and the consequent firewater flows and directions should be identified and estimated. Based on this, implementation of basic good practice measures should be considered, for example site kerbing/banking, sleeping policemen/ramps, permanent or temporary measures to close off potential environmental pathways and/or direct flows, and temporary emergency containment provision. This could include the provision of pollution containment equipment, for example pipe-blockers, drain sealing mats and land booms.

245 Further assessment should consider firewater volumes from worst-case credible scenarios. Implementation of additional measures should be considered by means of a cost-benefit analysis comparison versus the expected value of the consequences. Consideration of tertiary containment measures beyond basic good practice should be informed by an integrated risk assessment of the primary/secondary/tertiary controls as a whole.

Published guidance

246 General guidance on the design of remote containment systems (including lagoons, tanks and temporary systems such as sewerage storm tanks and sacrificial areas such as car parks, sports field and other landscape areas) is available in numerous documents including CIRIA 164, and PPG18.⁴⁴

247 Catchment areas used for tertiary containment often serve a dual purpose, for example roadways, hard standing, car parks. Such areas are normally routinely drained to surface water drainage systems. Therefore, to be considered for emergency tertiary containment, such areas must be capable of reliable emergency sealing of drains and interception of pollutants. Furthermore, arrangements must not compromise emergency access or unduly compromise day-to-day operations.

248 Major accident case studies provide valuable approaches to tertiary containment design, for example:

- Allied Colloids, Bradford (July 1992).
- Monsanto, Wrexham (1985).
- Sandoz, Switzerland (1986).

The first two of these are described in CIRIA 164, chapter 6.

Risk assessment guidance

249 Suitable and precautionary methodologies should be used for the above risk assessment. In view of the high uncertainties in modelling the transport of entrained or dissolved pollutants in liquids escaping secondary containment, it is recommended that assessments concentrate on quantifiable physical parameters such as those indicated in Table 5.

250 Two important references for an overall approach to environmental risk assessment are the Energy Institute *Environmental Risk Assessment of Bulk Liquid Storage Facilities: A Screening Tool*⁴⁵ and *Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports*⁴⁶ – http://www.environment-agency.gov.uk/static/documents/Research/comah_environmental_risk_assessment.pdf

Table 5 Environmental risk assessment checklist

Action/parameter	Guidance
<i>For the worst-case foreseeable severe pool fire scenario</i> severe pool fire or multiple tank / multiple bund fire (following an explosion or due to escalation)	
Identify firewater volumes	Energy Institute IP19
Assess firewater management effects	
Identify bund potential failure points	MIIIB second progress report ⁴⁷
For each failure point, assess: <ul style="list-style-type: none"> – likely liquid/firewater flow and volume – direction of escaped liquid flows 	
<i>For the worst-case catastrophic tank failure</i>	
Identify expected liquid volumes, flow directions and receiving locations outside bund walls	
<i>For the surrounding environment, construct a conceptual site model</i>	
Construct conceptual site model	El <i>Environmental guidelines for petroleum distribution installations</i> ⁴⁸
Identify surrounding environmental receptors, for example sites of special scientific interest, rivers, agricultural land. Classify in terms of receptor type and sensitivity/importance	Environment Agency: www.environment-agency.gov.uk/ ; Natural England: www.naturalengland.org.uk/ ; Scottish Environment Protection Agency: http://www.sepa.org.uk/ ; Scottish National Heritage: http://www.snh.org.uk/ ; Defra Tables 1–12: http://www.defra.gov.uk/environment/quality/chemicals/accident/documents/comah.pdf
Identify geological characteristics	
Identify hydrogeology	British Geological Survey www.bgs.ac.uk/
Identify flow gradients and likely flow outcomes	
Identify direct pathways, for example drains, boreholes	
Identify indirect pathways to sensitive receptors, for example permeable ground	
Assess permeability of ground and thus permeation flow-rates and quantities of pollutant into ground	CIRIA 164
<i>Consider appropriate defensive tertiary containment measures</i>	
Kerbing to roadways, car parks etc, toe walls, area grading	
Eliminate direct pathways, for example cap boreholes	
Emergency drain seals (for example auto-actuated bellows)	
Overflows to remote containment lagoons	
Channel spillages to remote containment	
Additional hardstanding	
Dedicated tankage	
Transfer to other secondary containment	

Part 5 Operating with high reliability organisations

251 The need for high reliability organisations follows from the recommendations relating to technological improvements in hardware. Such improvements are vital in improving process safety and environmental protection, but achieving their full benefit depends on human and organisational factors such as the roles of operators, supervisors and managers.

MIIB Recommendation 19

The sector should work with the Competent Authority to prepare guidance and/or standards on how to achieve a high reliability industry through placing emphasis on the assurance of human and organisational factors in design, operation, maintenance, and testing. Of particular importance are:

- (a) understanding and defining the role and responsibilities of the control room operators (including in automated systems) in ensuring safe transfer processes;
- (b) providing suitable information and system interfaces for front line staff to enable them to reliably detect, diagnose and respond to potential incidents;
- (c) training, experience and competence assurance of staff for safety critical and environmental protection activities;
- (d) defining appropriate workload, staffing levels and working conditions for front line personnel;
- (e) ensuring robust communications management within and between sites and contractors and with operators of distribution systems and transmitting sites (such as refineries);
- (f) prequalification auditing and operational monitoring of contractors' capabilities to supply, support and maintain high integrity equipment;
- (g) providing effective standardised procedures for key activities in maintenance, testing, and operations;
- (h) clarifying arrangements for monitoring and supervision of control room staff; and
- (i) effectively managing changes that impact on people, processes and equipment.

252 A high reliability organisation has been defined as one that produces product relatively error-free over a long period of time. Two key attributes of high reliability organisations are that they:

- have a chronic sense of unease, ie they lack any sense of complacency. For example, they do not assume that because they have not had an incident for ten years, one won't happen imminently;
- make strong responses to weak signals, ie they set their threshold for intervening very low. If something doesn't seem right, they are very likely to stop operations and investigate. This means they accept a much higher level of 'false alarms' than is common in the process industries.

253 The following factors should be addressed to achieve a high reliability organisation:

- Clear understanding and definition of roles and responsibilities, and assurance of competence in those roles.
- Effective control room design and ergonomics, as well as alarm systems, to allow front-line staff, particularly control room operators, to reliably detect, diagnose, and respond to potential incidents.

- Appropriate staffing, shift work arrangements and working conditions to prevent, control and mitigate major accident hazards.
- Setting and implementing a standard for effective and safe communication at shift and crew change handover.
- Effective management of change, including organisational change as well as changes to plant and processes.

254 Refer to Appendix 5 for detailed guidance

MIIB Recommendation 20

The sector should ensure that the resulting guidance and/or standards is/are implemented fully throughout the sector, including where necessary with the refining and distribution sectors. The Competent Authority should check that this is done.

255 The 'Scope and application' section of this report sets out how the sector intends to implement the improvements identified in the management of risk. PSLG's Principles of Process Safety Leadership provide the foundation to ensure high reliability organisations. These coupled with the guidance on the management of operations and human factors in Appendix 5 should ensure high reliability for human and organisational factors in design, operation, maintenance and testing.

256 The CA, within its regulatory programme, should check that dutyholders are complying with this guidance.

MIIB Recommendation 21

The sector should put in place arrangements to ensure that good practice in these areas, incorporating experience from other high hazard sectors, is shared openly between organisations.

257 A new Process Safety Forum has been established to collectively review incidents and share the lessons and good practice. See Appendix 8 for the Forum's terms of reference.

MIIB Recommendation 22

The Competent Authority should ensure that safety reports submitted under the COMAH Regulations contain information to demonstrate that good practice in human and organisational design, operation, maintenance and testing is implemented as rigorously as for control and environmental protection engineering systems.

258 The CA should check that safety reports submitted for COMAH sites demonstrate compliance with this and other guidance.

Part 6 Delivering high performance through culture and leadership

259 Industry leaders have a critical role to play in delivering high performance in process safety management. Recent incidents at Buncefield and Texas City have shown that a culture of process safety should be actively developed, grown and championed from the top of an organisation. Industry should demonstrate a commitment to process safety leadership, and a willingness to promote the process safety agenda at all levels within an organisation, and externally with other stakeholders.

MIIB Recommendation 23

The sector should set up arrangements to collate incident data on high potential incidents including overfilling, equipment failure, spills and alarm system defects, evaluate trends, and communicate information on risks, their related solutions and control measures to the industry.

MIIB Recommendation 24

The arrangements set up to meet Recommendation 23 should include, but not be limited to, the following:

- (a) Thorough investigation of root causes of failures and malfunctions of safety and environmental protection critical elements during testing or maintenance, or in service.
- (b) Developing incident databases that can be shared across the entire sector, subject to data protection and other legal requirements. Examples exist of effective voluntary systems that could provide suitable models.
- (c) Collaboration between the workforce and its representatives, dutyholders and regulators to ensure lessons are learned from incidents, and best practices are shared.

MIIB Recommendation 25

In particular, the sector should draw together current knowledge of major hazard events, failure histories of safety and environmental protection critical elements, and developments in new knowledge and innovation to continuously improve the control of risks. This should take advantage of the experience of other high hazard sectors such as chemical processing, offshore oil and gas operations, nuclear processing and railways.

260 PSLG has addressed the issues of leadership and sharing and learning lessons from incidents from both a sector- and dutyholder-specific perspective.

261 To demonstrate the importance of culture and leadership in the delivery of a high reliability organisation, PSLG has published Principles of Process Safety Leadership. The principles can be found in Appendix 7 of this report. They should be adopted by individual dutyholders. Further guidance is provided in Appendix 5.

262 A new Process Safety Forum has been established to collectively review incidents and share the lessons and good practice. Refer to Appendix 8 for the terms of reference for the Process Safety Forum.

263 Several initiatives have been launched by trade associations to address the issues of delivering high performance in process safety management, aligning with the PSLG Principles of Process Safety Leadership.

264 UKPIA launched their Process Safety Leadership Commitment in April 2008, which aims to facilitate the downstream oil sector in becoming a leader in process safety excellence. Through the Process Safety Leadership Commitment, UKPIA:

- has appointed a process safety programme manager, who under the guidance of UKPIA's Process Safety Leadership Network, manages the implementation of the process safety leadership commitment, and works closely with the PSLG;
- has established a framework for self assessment in key areas of process safety, and is developing self assessment modules for these key areas;
- is agreeing common leading and lagging process safety performance indicators, aligning with API RP 754;⁴⁹
- has developed an effective process for the sharing of, and learning lessons from, relevant high potential safety incidents, both internally with UKPIA members through Process Safety Information Notes, and externally through the Process Safety Forum with Process Safety Alerts;
- is a founding member of the Process Safety Forum, reviewing relevant incident and near-miss data, and sharing lessons learned and good practice. UKPIA's self-assessment module on Management of Change has already been shared with other industry sectors through the forum. UKPIA have also taken the lead in developing the protocol by which incident/near miss data can be shared amongst industry sectors;
- is enhancing dialogue with key stakeholders, ensuring proper account is taken of their concerns.

265 TSA fully supports the PSLG's Principles of Process Safety Leadership. TSA's members are reporting quarterly their process safety incidents based on the lagging metrics set out in the CCPS publication 'Process Safety Leading and Lagging Metrics'.⁵⁰ Process safety incidents and near misses are posted on TSA's website and discussed at the quarterly meetings of TSA's Safety, Health and Environmental Committee. TSA is also a founding member of the Process Safety Forum. In addition to these activities some TSA member companies have additional specific initiatives in the field of process safety; these include:

- formal documentation describing how the company delivers process safety;
- monitoring of company performance against a suite of leading and lagging process safety measures;
- reviewing process safety performance at every board meeting;
- effective communication on process safety issues to all stakeholders;
- top-down leadership on the topic of process safety;
- effective training and development in the area of process safety; and
- investment in infrastructure to ensure good process safety.

Conclusion

266 The guidance provided in parts 1 to 6 of this report represents the full and final response to the 25 recommendations of the MIIB *Design and operations* report. Appendices 1 through 8 provide additional detailed technical guidance in achieving these recommendations.

267 PSLG recognises that industry has already made significant progress in addressing these recommendations in part, particularly those covered by the original BSTG report, and in the areas of high reliability organisations and delivering high performance through culture and leadership.

268 Following the publication of this report a period of gap analysis will be undertaken to identify where additional work is required, prioritising this work on a risk basis and agreeing timescales for implementation with the CA.

269 The method of working adopted for the development of this, and the BSTG guidance, has proved extremely effective, and it is the intention of the PSLG that this philosophy in tackling improvements in the management and control of process safety risks will be continued following publication of this report.

270 Finally, PSLG once again wishes to thank all those from industry, trade unions and the CA for their efforts in developing this guidance. A full list of contributors can be found in Appendix 10.

Appendix 1 Mechanisms and potential substances involved in vapour cloud formation

Part 1 Research paper – Liquid dispersal and vapour production during overfilling incidents

SYMPOSIUM SERIES NO. 154

Graham Atkinson,* Simon Gant,* David Painter,* Les Shirvill† and Aziz Ungut†

* HSE, † Shell Global Solutions

This article is published with the permission of the Controller of HMSO and the Queen's Printer for Scotland.

There have been a number of major incidents involving the formation and ignition of extensive flammable clouds during the overfilling of atmospheric pressure tanks containing gasoline, crude oil and other volatile liquids.⁵¹⁻⁵³ These incidents are characterised by widespread fire and overpressure damage.

The purposes of this paper are threefold:

- 1 to discuss physical processes of liquid dispersal, vaporisation and air entrainment that lead to the formation of a flammable cloud;
- 2 to describe an approximate method of calculation that can be used to determine whether the formation of a flammable cloud is possible for a given filling operation – a scoping method;
- 3 to describe the implications for safety and environmental standards for fuel storage sites in the UK.

Physical processes

Liquid flow

1 The nature of the liquid release from an overfilled tank depends primarily on the flow rate and on the tank design. Three categories of tank have been identified that differ significantly in the character of the liquid release in the event of overfilling.

Type A: Fixed roof tanks with open vents (typically with an internal floating deck).

Type B: Floating deck tanks with no fixed roof.

Type C: Fixed roof tanks with pressure/vacuum valves and possibly other larger bore relief hatches.

Liquid release from Type A tanks

2 This is the type of tank that was involved in the Buncefield incident. This tank was typical of Type A tanks with a number of open breather vents close to the edge of the tank at a spacing of around 10 m around the perimeter.

3 Tanks of this sort may be provided with a fixed water deluge system, which delivers water to the apex of the conical top of the tank. In the event of a fire, injected water flows down over the tank roof. Typically there is a 'deflector plate' at the edge of the tank, which redirects water draining from the top of the tank on to the vertical tank wall.

4 In the event of tank overfilling, liquid will flow out of the open vents, spreading a little before it reaches the tank edge. The flow rates during overfilling are typically much higher than cooling water flow for which the deflector is designed. A proportion of the liquid release is directed back on to the wall of the tank and a proportion simply flows over the edge of the plate. This is illustrated in Figure 13.

5 Some tanks, including the tank involved in the Buncefield incident, have wind girders part way down the tank wall to stiffen the structure. Any liquid falling close to the tank wall will hit this girder and be deflected outwards, away from the tank wall. This outward spray may intersect the cascade of liquid from the top of the tank. This is illustrated in Figure 14.

6 The lateral spread around the tank perimeter of the free cascade of liquid formed from each breather vent is slightly greater if a deflector plate or wind girder is present. With these features present, the spray typically extends approximately 3 m around the tank perimeter. If the vents are spaced at 10 m intervals and the elevation of the vents is similar, the final result is a series of liquid cascades that cover approximately 30% of the total tank perimeter.

Liquid release from Type B tanks

7 Floating deck tanks with no fixed roof typically have a large wind girder close to the top of the tank wall. This is fully welded to the side of the tank (to avoid stress concentration) and may be used as an access way (Figure 15). Small bore holes drain the top girder shelf but in the event of an overfill almost all of liquid overtopping the wall of the tank will flow out over the edge of the top girder forming a cascade. Typically the top girder is wide enough that liquid will not subsequently contact the tank wall and will therefore form a free cascade.

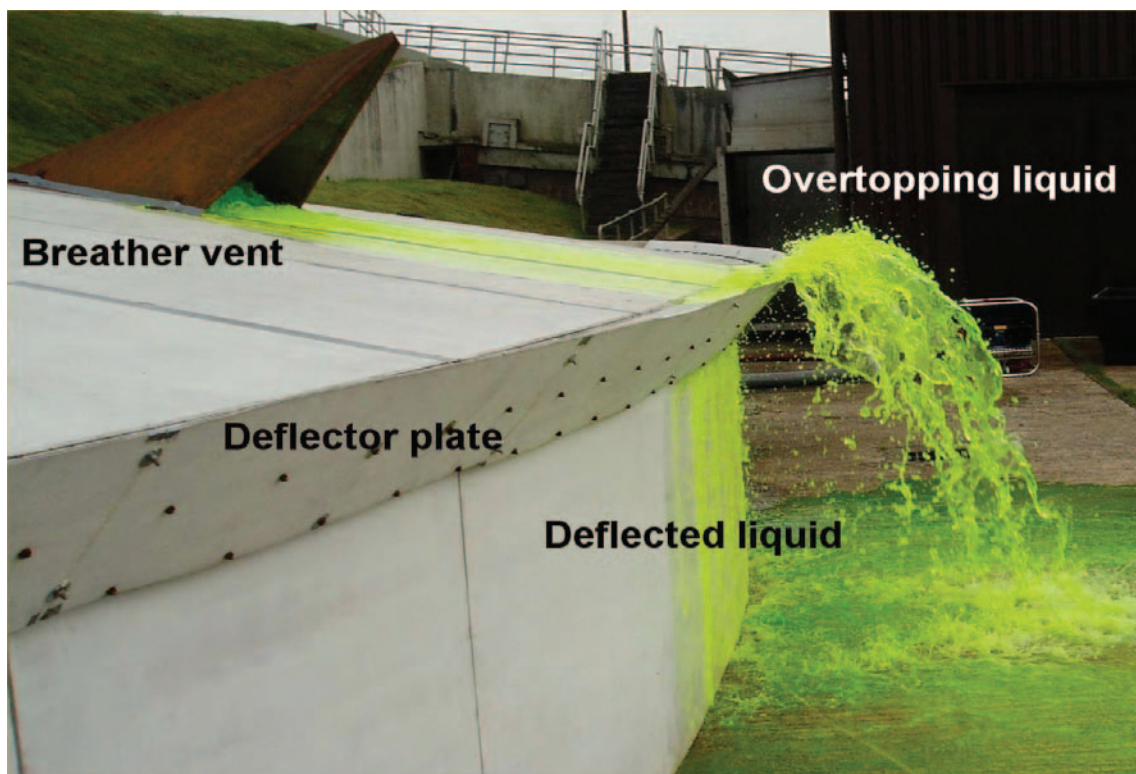


Figure 13 Liquid release from a vented fixed roof tank with a deflector plate



Figure 14 Intersection of free cascades from a Type A tank with a deflector plate



Figure 15 Top girder (walkway) on floating roof tank

8 The proportion of the tank perimeter over which this cascade extends is likely to depend on the construction of the tank. Any variations in the elevation of the tank wall will tend to concentrate the release on one side of the tank. Similarly any damage to the tank wall by the floating deck or access to this deck prior to the overflow may concentrate the release in an even smaller fraction of the tank perimeter. It is unlikely to extend round the full tank perimeter.

Liquid release from Type C tanks

9 Pressure/vacuum valves provided for pressure balancing during filling and emptying operations will generally not be adequate to relieve the liquid flow during overfilling. Liquid will come out of larger bore pressure relief hatches if these are fitted or from a split in the tank if they are not. Normally the tank construction should ensure that any split is at the junction between the tank top and wall.

10 In any case, it is likely that the release will be concentrated in a cascade covering a relatively small proportion of the total tank perimeter.

Liquid dispersal

11 There do not appear to have been any previous studies of high volume, low momentum liquid releases that accelerate and disperse under the action of gravity. Some large-scale tests on water and petrol undertaken in the aftermath of the Buncefield incident have provided some useful indicators but there is a pressing need for more data.

12 In the first few metres of fall the large-scale liquid strings and lamellae formed in the release separate and accelerate, dividing into large droplets with a diameter of order 10 mm. The fate of these large fragments depends on the mass flux density of liquid in the cascade (ie the amount of liquid falling through each square metre per second). If the flux density is relatively low most of the initial liquid fragments shatter rapidly to form a range of secondary droplets a few millimetres in diameter. The characteristic size is clearly a function of the liquid surface tension. Comparisons between 15 m high water and petrol cascades at similar mass densities showed that, at ground level, the droplets of water are variable in size in the range 2-5 mm whereas the characteristic size of petrol droplets are around 2 mm.

13 If the liquid flux density is very high, the aerodynamic drag forces on individual droplets in the core of the cascade will be lowered and some of the large fragments initially formed may persist for the full height of the drop.

14 All of the droplets then hit the ground. In cascades with high liquid mass flux densities the droplet impact speed may considerably exceed the terminal velocity for a single drop. Again the number and size of smaller secondary droplets formed on impact depends on the surface tension, impact speed and the nature of the impact surface ie wetted solid or deep liquid.

15 An initial estimate of the size range of secondary droplets produced by a petrol cascade impinging onto a bund floor can be made using the droplet splashing model of Bai et al.⁵⁴ This predicts secondary droplets of diameter 130-200 microns for impingement on a dry floor and 100-180 microns diameter for a wetted floor. The total mass of splash products is very dependent on the depth of liquid on the impact surface and may even exceed the incident droplet mass in some circumstances.

16 In this paper, the phrase 'vapour flow' is used to describe the air drawn into a liquid cascade and any gas produced from the liquid evaporating and mixing with the air. The fineness of droplets in the splash zone is very significant because the vapour flow driven by the cascade (described in Section 1.3) passes through the splash zone. There is an opportunity for very rapid exchange of mass, heat and momentum. Exchanges of heat and mass in the splash zone drive the liquid and vapour flows closer to thermodynamic equilibrium. Fine (100-200 micron diameter) droplets rapidly picked up by the vapour flow in the splash zone absorb momentum from the vapour flow and this may have a significant effect on its subsequent dispersion.

17 It is worth pointing out that the settling velocity for droplets in the size range 100-200 microns is 0.2 to 0.8 m/s. This means that droplets this size may remain airborne for a time of order 1-5 seconds during which they may be convected a distance of order 10 metres from the base of the tank. This means that some liquid droplets may remain suspended in the vapour flow as it impacts on the bund wall or other tanks within the bund.

Air entrainment

18 Jets of air or buoyant plumes entrain air through the action of shear driven vortices. A dense liquid cascade entrains air in a different, somewhat less complex way. Individual falling drops drag the air within the cascade downwards and air is drawn in through the sides to compensate. There are shear forces and induced vortices at the edge of the cascade but if the cross section is large these processes make little difference to the total volume flux of air – which is the quantity of primary interest.

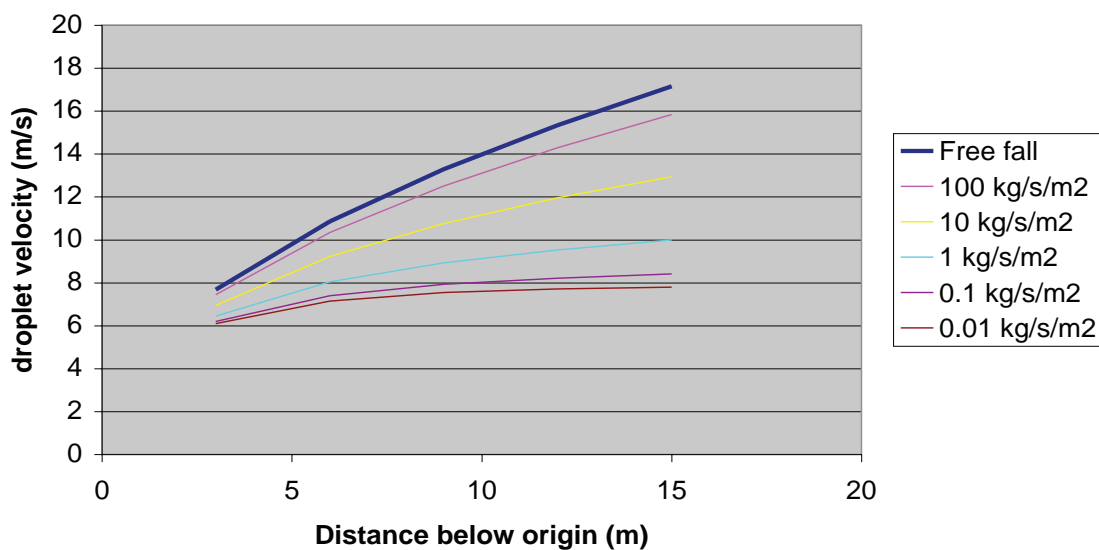
19 A comparison has been made of detailed CFD predictions, which have included all the aerodynamic processes involved in falling sprays, and a simple momentum conservation model which ignores the induced shear flow on the spray periphery. This has shown that for the scenarios considered here it is adequate to use the latter, simpler treatment, which is described in Annex 1. Typical results obtained using the simple momentum conservation model are shown in Figure 16. In overfilling incidents the mass flux density is likely to be in the range 1 to 10 kg/m²/s. This corresponds to maximum droplet velocities of 10-13 m/s and vapour velocities of 4-6 m/s.

20 CFD methods of the sort reported in Section 3 are capable of calculating droplet and vapour velocities both in the liquid cascade and in the vapour flow spreading out from the foot of the tank. These calculations fully encompass exchange of mass, heat and momentum between liquid and vapour phases.

Vaporisation of liquid

21 The fineness of liquid dispersal controls the extent to which liquid and vapour approach thermodynamic equilibrium. Example results from a CFD study of heat and mass transfer in the cascade are shown in Figure 17.

Droplet dynamics in spray of varying mass density



Vapour flow driven by sprays of varying mass density

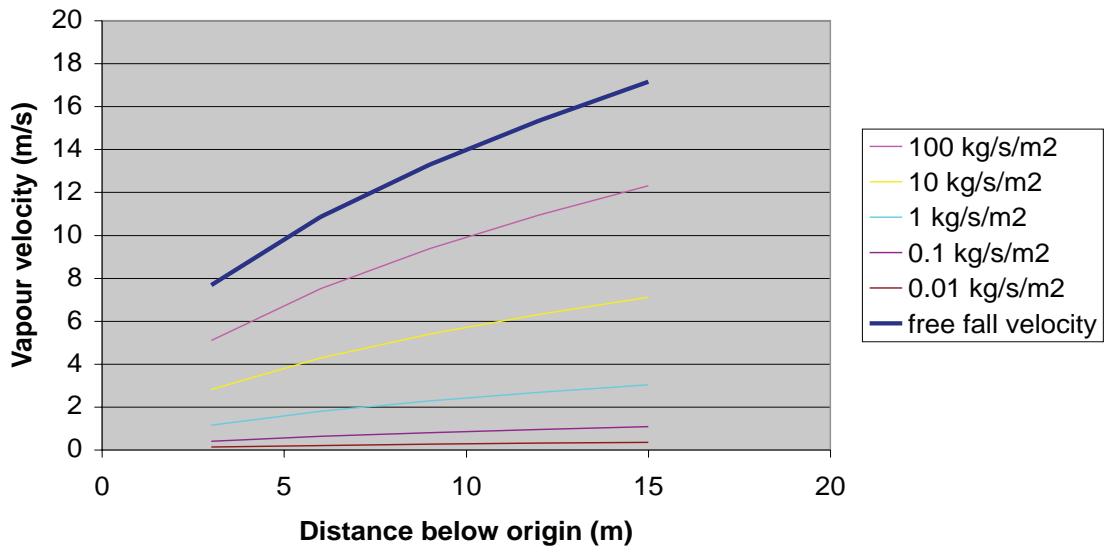


Figure 16 Vapour and droplet velocities induced by liquid cascades of different densities. The highest velocities shown in both plots (for comparison) correspond to free-fall with no air resistance. The lower velocities correspond respectively to liquid flux densities of 100, 10, 1, 0.1 and 0.01 kg/m²/s.

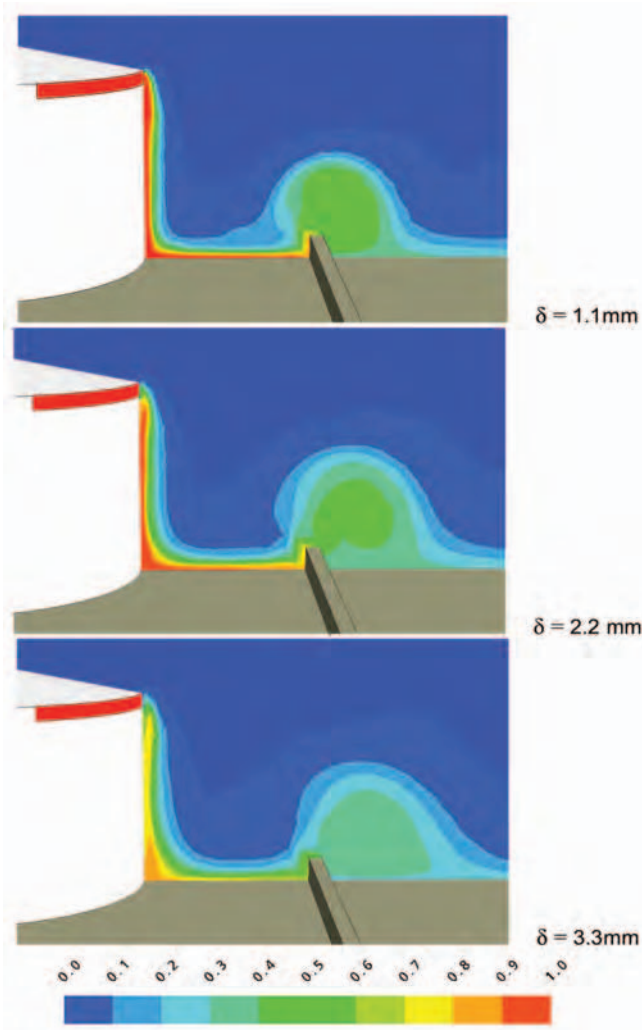


Figure 17 Contours of the ratio of predicted vapour volume fraction to the saturation volume fraction. A value of 1.0 indicates that the vapour is saturated. The three predictions are for different initial droplet size distributions using the Rosin-Rammler diameters shown.

22 For droplets of a diameter of 2 mm or less, droplets and vapour in the core of the cascade (where the mass flux is concentrated) are very close to equilibrium. Areas on the fringes of the cascade where there is a greater proportion of fresh air are clearly further from equilibrium.

23 The CFD modelling shown in Figure 17 does not include droplet splashing – droplets in the model disappear on impact with the ground. The presence of the pool of liquid in the bund around the base of the tank is also ignored. It is likely that in most circumstances the splash zone at the base of the tank is an additional area where vapour and very finely divided liquid are vigorously mixed for a significant period of time, which pushes the whole of the flow closer to equilibrium.

24 In the scoping method described in Section 2 it is assumed that the liquid released and the gas flow that it entrains in the cascade and splash zone are in thermodynamic equilibrium. This is a conservative assumption in the assessment of vapour cloud production but available information on liquid dispersal and heat and mass transfer calculations suggest it is also reasonably close to the truth in most cases.

25 One important exception to this may be tanks where high volume releases are concentrated in very small sections of the tank perimeter. Releases from many Type C tanks could be of this sort. Very high liquid mass flux densities $O(100 \text{ kg/m}^2/\text{s})$ could result. In this case liquid dispersal would be limited and the spray would be composed of very large droplets or streams of liquid. For the very large liquid fragments, the rate of vaporisation could be limited by the ability of lighter, more volatile fractions to diffuse to the surface of the liquid in contact with the air. This is significant in the analysis of the potential for Type C tanks to produce flammable clouds when overfilled with liquids composed of only a small volume fraction of volatile material eg light crude oils.

Near field dispersion

26 Generally, dispersion of a release of flammable vapour cloud is treated separately from the source term (unless a full CFD treatment of the whole release is possible). To take this approach it is necessary to identify where the source term ends and the dispersion calculation should begin. The choice taken here for this point of separation is at the base of the tank or at the edge of the zone where the vapour flow is deflected into the horizontal.

27 Care has to be taken in joining source term and dispersion calculations in this way. High vapour velocities $O(5 \text{ m/s})$ are typically induced by the cascade at the foot of the tank. Even though the flow is denser than air, such a flow will entrain air as it flows out across the floor of the bund. This entrainment process occurs whether the flow impacts on a bund wall (as in Figure 17) or not. Any entrainment of fresh air after the bulk of the liquid has rained out will result in a reduction in vapour concentration. Contact between the vapour and liquid pool on the floor of the bund may on the other hand increase the concentrations, although this may be limited since the vapour close to the floor of the bund may be close to being saturated already.

28 There is a tendency for the entrained air to move through the cascade towards the tank wall (the Coanda effect). This means that the bulk of the vapour flow passes through the droplet splash zone at the base of the tank – see Figure 18. Droplet splash products are capable of absorbing part of the vapour jet momentum and consequently suppressing the tendency for entrainment – even in the near-field. This effect is still under investigation. Large-scale experimental releases of hydrocarbons are needed to obtain reliable data on the flow behaviour for this case.

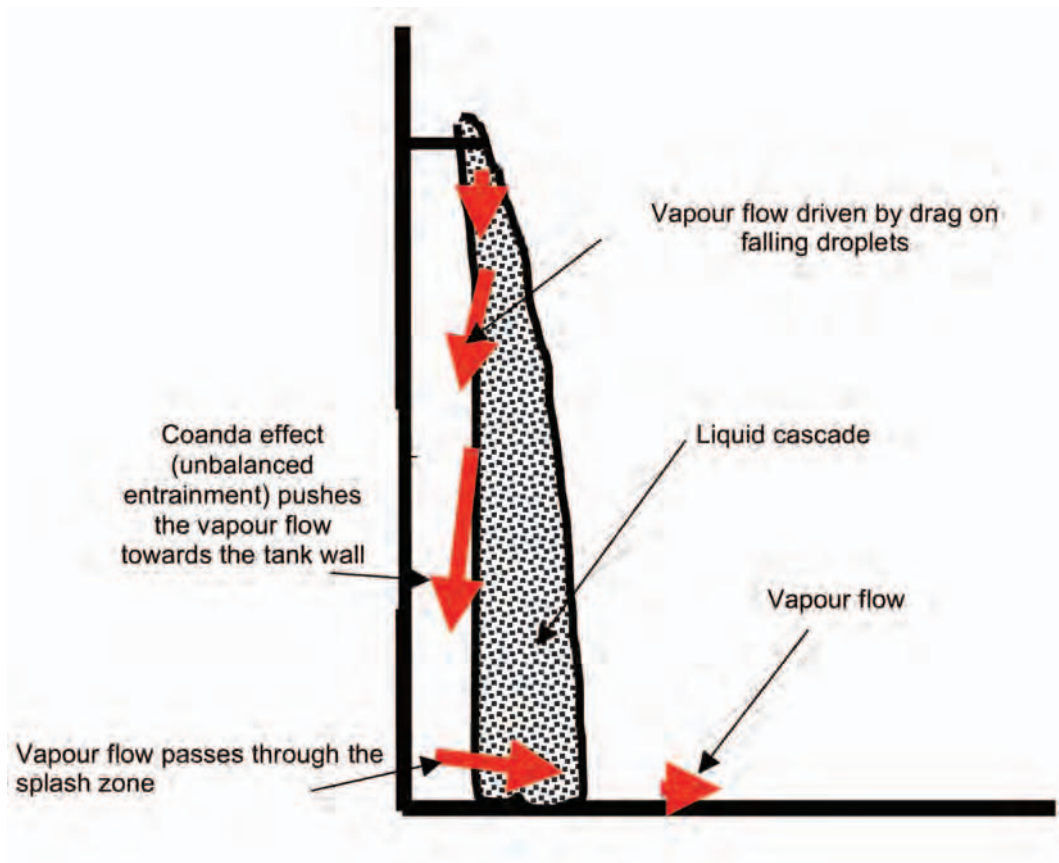


Figure 18 Schematic showing vapour flow driven by a free liquid cascade

Scoping method

Approach and assumptions

29 The scoping method described here is based on principle that production of vapour concentrations within the flammable range at the base of the tank will bring liquids 'in scope'. This is a somewhat conservative, but reasonable, assumption that might be refined if more was known about the splashing process and its effects on the near-field dispersion.

30 The method provides a means of determining whether a given filling operation in a given tank can lead to the generation of a flammable cloud. Such a scoping method is clearly of interest in determining the appropriate level of protection against overfilling. The volume and concentration of flammable vapour close to the source are outputs but to predict the potential extent of the cloud would require a dispersion model.

31 Although it may appear initially counter-intuitive, the likelihood of producing flammable vapour for many substances increase as the amount of fresh air entrainment is reduced. Enhanced air entrainment leads overall to greater evaporation but the vapour produced is often below the lower flammability limit.

32 The scoping method is divided into a number of stages which are described below:

A *Proportion of tank perimeter covered by liquid release*

It is assumed that in all cases the liquid released is distributed over 30% of the tank perimeter. In the case of Type C tanks this may be an overestimate. In principle this might lead to non-conservative overestimation of the induced vapour flow, however this is unlikely to lead to serious underestimates of risk because of the relatively low sensitivity of the induced flow to the liquid mass flux and the tendency for vapour concentrations to fall short of equilibrium at very high liquid mass fluxes.

B *Liquid mass flux in the cascade*

The distance the spray extends away from the tank wall is assumed to be 1.5 m over the full height of the cascade. This is a reasonable minimum figure based on observations on water cascades. Wind girders part way down the tank can increase the width to in excess of 3 m but any broadening of the liquid cascade increases the total induced air flow and tends to reduce the maximum vapour concentration. Given the cross section of the cascade and the total liquid release rate the liquid mass density can be calculated.

C *Entrained airflow*

Given the liquid mass density the volume flow of entrained air can be taken from a plot such as that shown in Figure 16. The height over which air is entrained is not the full height of the tank because it typically takes several metres for primary aerodynamic break up to be complete and there is likely to be re-entrainment of contaminated air from the splash zone in the last few metres of fall. It has therefore been assumed that air is entrained over a minimum height of 6 m. For very high tanks (>15 m) this may be an underestimate leading to minor underestimates of airflow and overestimation of risk.

Observations of petrol releases suggest that 2 mm is an appropriate droplet diameter for this calculation. The airflow is insensitive to this choice of diameter within a reasonable range.

D *Equilibrium calculations*

The concentration of vapour at the foot of the tank is estimated by assuming thermodynamic equilibrium. Given total liquid flow rates and air entrainment rates (and the temperatures of both) the final temperature and vapour concentration can be calculated straight forwardly. Examples of results of such a calculation for a winter grade petrol are given in Annex 2. Water vapour condensation should be included in the enthalpy balance but only makes a substantial difference if the humidity and ambient temperatures are high.

E *Comparison with flammability limits*

If the vapour concentration calculated in D exceeds the Lower Flammable Limit it is possible that overfilling of the tank will produce a flammable cloud.

33 The method described above accounts for the fact that the temperature drop due to evaporation of spray droplets may reduce the saturation vapour pressure sufficiently to avoid the production of flammable vapour. This means that in some cases a substance that is flammable at room temperature, such as toluene, may not produce flammable vapour in the cascade from a tank overfilling release. In reality, in such cases, the liquid from the tank overfill will accumulate within the bund and may eventually rise to ambient temperatures and start to produce flammable vapour. This hazard could be modelled using standard pool-evaporation models.

34 Results of such scoping analyses on typical high volume refinery liquids and crude oils are shown in Figures 19 and 20. Composition data for the mixtures analysed are shown in Annex 3. In all cases the temperature of the released fluid was 15 °C and the ambient temperature 15 °C. The independent variable is the total liquid release rate divided by the total tank diameter.

Implications for safety and environmental standards at fuel storage sites

35 The technical work described in this paper was carried out in support of the Buncefield Standards Task Group (BSTG). The BSTG was formed soon after the Buncefield incident and consisted of representatives from industry and the joint Competent Authority for the Control of Major Accident Hazards (COMAH). The aim of the task group was to translate the lessons from the incident into effective and practical guidance.

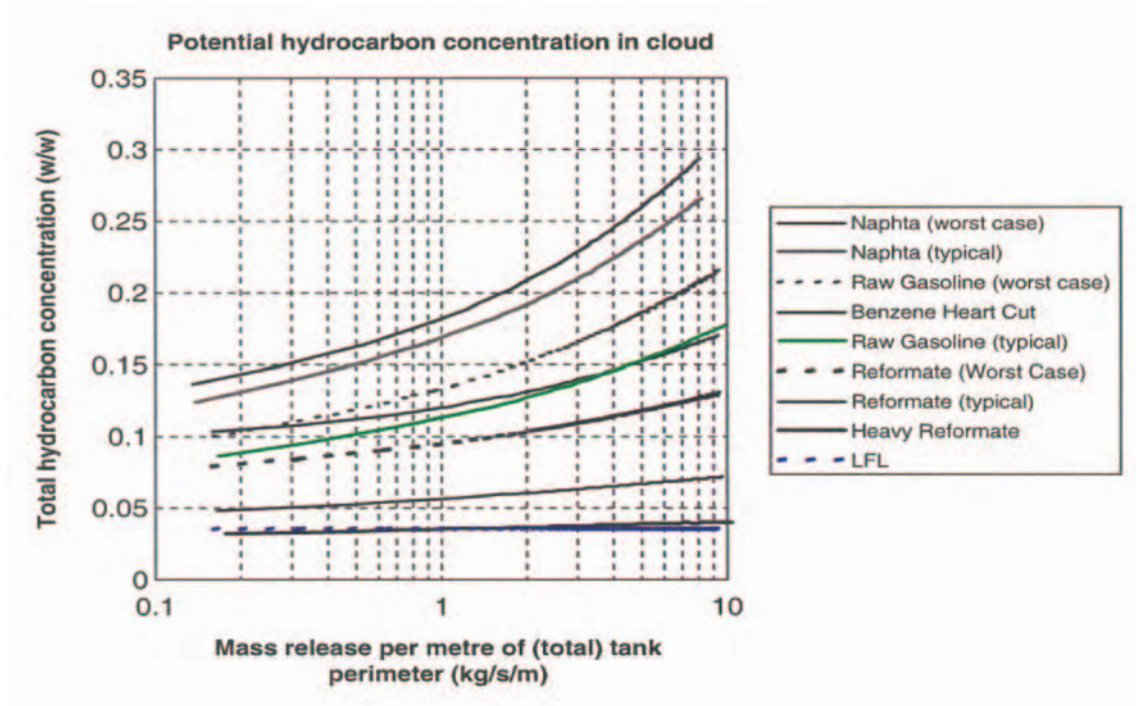


Figure 19 Vapour concentrations in air driven by cascades of various refinery liquids

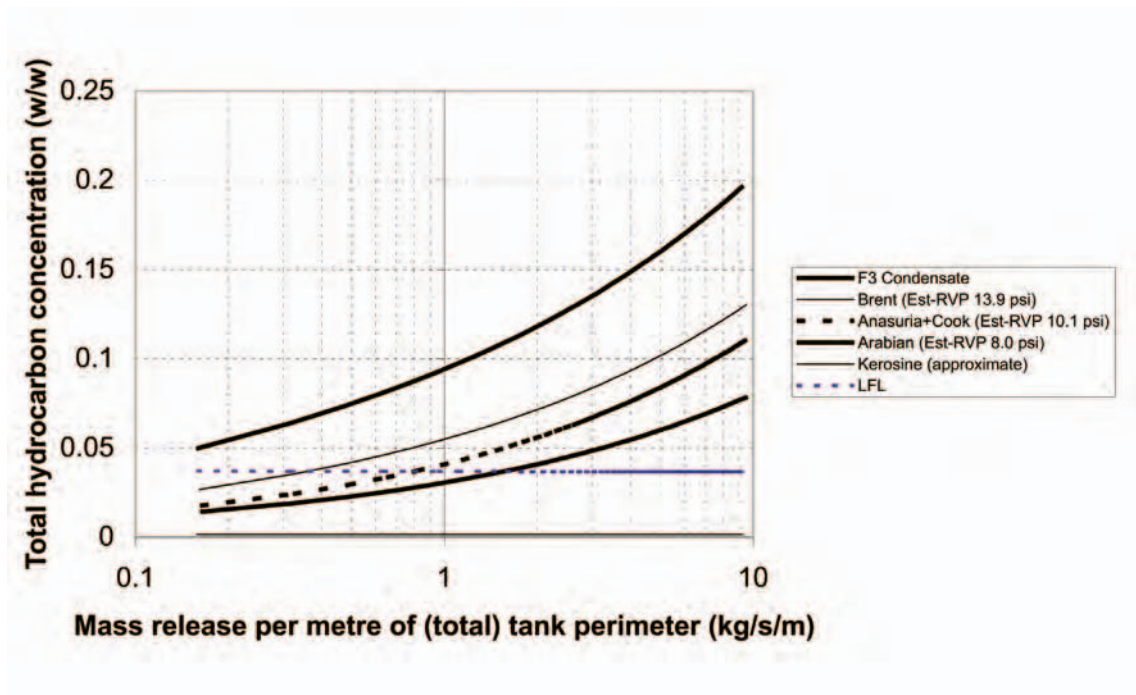


Figure 20 Vapour concentrations in air driven by cascades of various crude oils

36 To ensure focused and timely responses to the issues arising from Buncefield the scope of application for the work of the task group was defined in the initial report by BSTG.⁵⁵ This was confirmed in the final report of July 2007⁵⁶ and is repeated here:

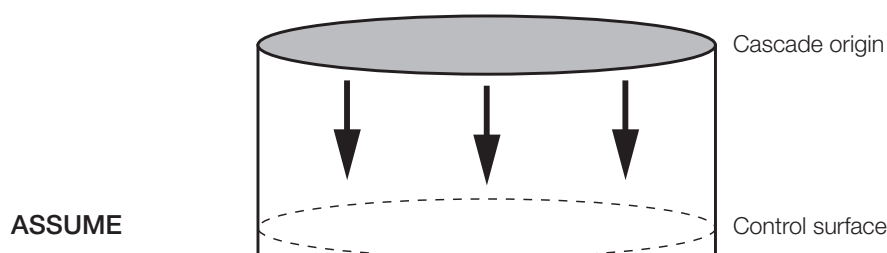
- COMAH top- and lower-tier sites, storing:
- Gasoline (petrol) as defined in Directive 94/63/EC [European Parliament and Council Directive 94/63/EC of 20 December 1994 on the control of volatile organic compound (VOC) emissions resulting from the storage of petrol and its distribution from terminals to service stations], in:
- vertical, cylindrical, non-refrigerated, above-ground storage tanks typically designed to standards BS 2654, BS EN 1401:2004, API 620, API 6508 (or equivalent codes at the time of construction); with
- side walls greater than 5 metres in height; and at
- filling rates greater than 100 m³/hour (this is approximately 75 tonnes/hour of gasoline).

37 The results of the work reported in this paper confirm the scope of application for the initial response to Buncefield. That is to say that all types of storage tank described in paragraph 1 are believed to be capable of generating a cascade of liquid droplets in the event of overfilling with hydrocarbon liquid. If that liquid hydrocarbon is gasoline then there is the potential for the formation of a large flammable vapour cloud.

38 This work also indicates that there is the potential for other substances with similar physical properties to behave in a similar way in the event of a loss of primary containment following overfilling. Work continues in order to establish an agreed definition for the extension of scope to a limited number of other substances. This might also lead to a better understanding of the release conditions that might lead to this scenario. The further work continues under the Petroleum Process Standards Leadership Group which has been formed to take forward the work started by the BSTG.

39 In the meantime the results of the work of BSTG have been taken forward as a series of actions required of operators. The final report details these actions and includes the supporting guidance.

Annex 1 Gas flow driven by liquid cascade



- 1 The spray has little initial non-axial velocity and the cross section remains constant.
- 2 The spray is uniform over a given area with a mass flux density of M (kg/m²/s).
- 3 The induced gas phase velocity is constant across the section. The additional gas mass flow required is presumed to be entrained through the vertical boundary of the spray and rapidly mixed across the section.
- 4 The spray is monodisperse (ie all droplets are the same size).

Droplet dynamics

$$m_{\text{droplet}} \frac{du_{\text{droplet}}}{dt} = m_{\text{droplet}} \cdot g - \frac{1}{2} C_d P_{\text{vap}} A_{\text{drop}} (u_{\text{droplet}} - u_{\text{vapour}})^2$$

Vapour dynamics

Vapour velocity at a horizontal control surface below the origin of the spray

$$P_{\text{vap}} u_{\text{vapour}}^2 = \sum_{\text{droplets}} \frac{1}{2} C_d P_{\text{vap}} A_{\text{drop}} (u_{\text{droplet}} - u_{\text{vapour}})^2$$

The summation is carried out over droplets above the control surface
Additional relations used

$$N(x) = \frac{M}{m_{\text{droplet}} u_{\text{droplet}}(x)}$$

This relates the number density of droplets to M the mass flux density (kg/s/m²) in the spray

$$\frac{A_{\text{drop}}}{m_{\text{droplet}}} = \frac{3}{4r_{\text{drop}} p_{\text{drop}}}$$

These equations can easily be integrated (numerically) from the origin of the cascade to yield droplet and vapour velocities.

Annex 2 Characteristics of vapour produced by a cascade of winter petrol

(Ambient temperature of 0 °C). Liquid flow rate 550 m³/hr

The conditions given below are calculated based on equilibrium between the liquid and vapour phases. A given flow rate of liquid is mixed with a given flow rate of fresh air and allowed to reach equilibrium in terms of both temperature and concentration.

Initial liquid composition (Liquid temperature 15 °C)

n-butane (as a surrogate for all C4 hydrocarbons)	9.6%	wt/wt
n-pentane (as a surrogate for all C5)	17.2%	wt/wt
n-hexane (as a surrogate for all C6)	16%	wt/wt
n-decane (as a surrogate for all low volatility materials)	57.2%	wt/wt
Rate at which air entrained into cascade	96 m ³ /s	
Final vapour and liquid temperature	-8.5 C	

Vapour composition

n-butane (as a surrogate for all C4 hydrocarbons)	6.0%	wt/wt
n-pentane (as a surrogate for all C5)	6.1%	wt/wt
n-hexane (as a surrogate for all C6)	2.06%	wt/wt
Total hydrocarbons (in air)	14.17%	wt/wt

Residual liquid composition

n-butane (as a surrogate for all C4 hydrocarbons)	2.4%	wt/wt
n-pentane (as a surrogate for all C5)	11.5%	wt/wt
n-hexane (as a surrogate for all C6)	16.3%	wt/wt
n-decane (as a surrogate for all low volatility materials)	69.6%	wt/wt

Annex 3

Composition % (w/w)	Paraffins					Aromatics				Naphthenes			
	C4	C5	C6	C7	C8	C9	C6	C7	C8	C9	C5	C6	C7
Naphtha (worst case)	9	58	20				4				7	2	
Naphtha (typical)	2	56	21	6	1		3	1			2	5	3
Raw gasoline (worst)	2	20	20				35	15	8				
Raw gasoline (typical)	1	9	21				35	13	7	14			
Benzene heartcut			50				50						
Reformate (worst)			22	27	3		21	25	2				
Reformate (typical)			4	18	17	4	5	24	23	5			
Heavy reformate			4	5	3		1	31	34	22			

Composition (w/w)	Paraffins					Aromatics		Nap	
	C2	C3	C4	C5	C6	C7	C6	C7	C5
F3 condensate		0.3	4.4	6.5	4.1	6.5	4.7	1.4	2.8
Anusa	0.02	0.4	1.78	2.72	2.3		1.42		0.28
Brent	0.07	0.74	1.75	2.65	2.27	2.84	2.53	1.25	1.5
Arabian		0.57	0.76	1.75	1.53	1.68	1.22	0.37	0.08

The balance of the crude oil mixture is modelled as a range of low volatility alkanes (not shown).

Part 2 Consideration of substances other than gasoline that may give rise to a large vapour cloud in the event of a tank overflow

1 Application of the methodology outlined in Part 1 of this appendix indicates that there are a number of other liquids stored in bulk at COMAH establishments that have a similar potential to gasoline to generate a flammable vapour cloud in the event of an overflow.

2 There is no simple definition based on a single liquid physical property that could be used to determine the extent to which other liquids give rise to similar risks to those associated with gasoline. There are some highly flammable liquids that on the basis of the application of the methodology clearly would not give rise to a large vapour cloud. These include: methanol, ethanol and higher chain alcohols, solvent SBP3 and middle distillate oil products such as kerosines and diesels.

3 However, there are a number of substances where the application of the methodology indicates that the result of a tank overflow would produce a flammable air mixture near to the lower flammable limit, or only just above the lower flammable limit under certain release conditions.

4 It is recognised that there is still uncertainty over the behaviour of hydrocarbon releases from the top of overfilled tanks. This uncertainty cannot be resolved without considerable additional experimental work. Under the circumstances it is difficult to apply judgement to decide whether a multiple of lower flammable limit should be used as a criterion for including liquids in scope. One view is that if the methodology indicates that a vapour mixture above the lower flammable limit could be produced, then there was not a rational basis for treating these substances differently to gasoline. However, it is recognised that a judgement on the risk indicated that there was a low likelihood of the specific release circumstances required to produce a vapour cloud significantly worse than that arising from a large spill into a bund.

5 An initial review of commonly stored liquids using the methodology indicates that the following substances have the potential to give rise to a large vapour cloud in the event of an overfill:

- acetone;
- benzene;
- natural gas liquids (condensates);
- iso pentane;
- methyl ethyl ketone;
- methyl tert-butyl ether;
- naphthas;
- raw gasoline;
- reformat (light);
- special boiling point 2;
- toluene.

6 Further work has shown that the methodology can be further refined for substances that appear to be borderline by consideration of the Reid vapour pressure (RVP), composition and heat of vaporisation. This system is summarised below:

- Use Reid vapour pressure for single component liquids not listed in paragraph 5. Single component liquids with RVP ≥ 2.5 should be considered as capable of giving rise to a large vapour cloud.
- For multi-component mixtures the tank filling rate and tank size should be considered. For these liquids including crude oils, mixtures with RVP ≥ 2.5 and meeting the following condition should also be considered as giving rise to a large vapour cloud:
 - Filling rate (m^3/hr) x liquid density (kg/m^3)/tank perimeter (m) > 3600 . Note: a default density of $750 \text{ kg}/\text{m}^3$ could be used.
 - This indicates that crude oils (meeting the criteria outlined in paragraph 6) and toluene also have the potential to form a large vapour cloud in the event of an overfill. For toluene, the cloud concentration at the base of a tank has been shown by research to be just above its lower flammable limit. However, there is a degree of uncertainty over whether its subsequent movement and dilution would lead to the formation of a large flammable vapour cloud. Taking a precautionary approach it would seem sensible to consider that it would.

7 In conclusion Table 6 shows the outcome of the application of the methodology in Part 1 and the refinement using Reid vapour pressure, as set out in paragraph 6, to commonly stored liquids. Note that the conditions which apply to these other substances in order to be considered likely to form a large vapour cloud, are as defined for gasoline in paragraph 24 of the main report.

Table 6 Substance propensity to form large flammable vapour clouds

Substances considered likely to form a large vapour cloud	Substances not considered likely to form a large vapour cloud
Acetone	Diesel
Benzene	Ethanol and other alcohols
Crude oils (subject to paragraph 6)	Kerosene
Raw gasoline	Methanol
Methyl ethyl ketone	Reformate (full range)
Naphthas	Reformate (heavy)
Reformate (worst case – light)	Special boiling point solvent 3
Natural gas liquids (condensates)	
Methyl tert-butyl ether	
Iso Pentane	
Special boiling point solvent 2	
Toluene	

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.

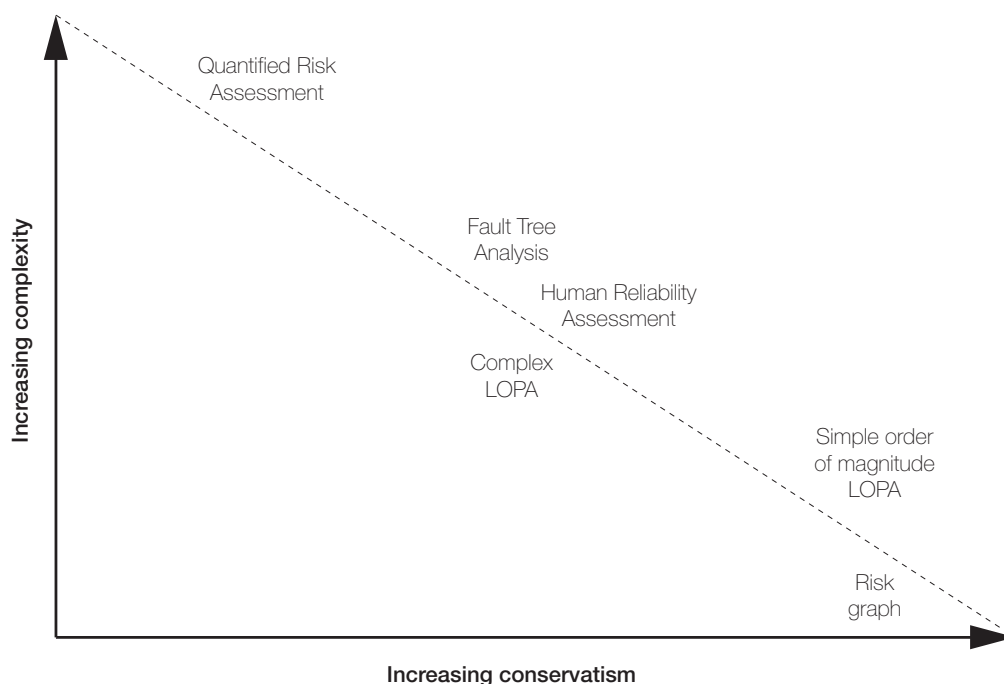


Figure 21 Relationship of LOPA technique to other risk assessment methodologies

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 f^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).

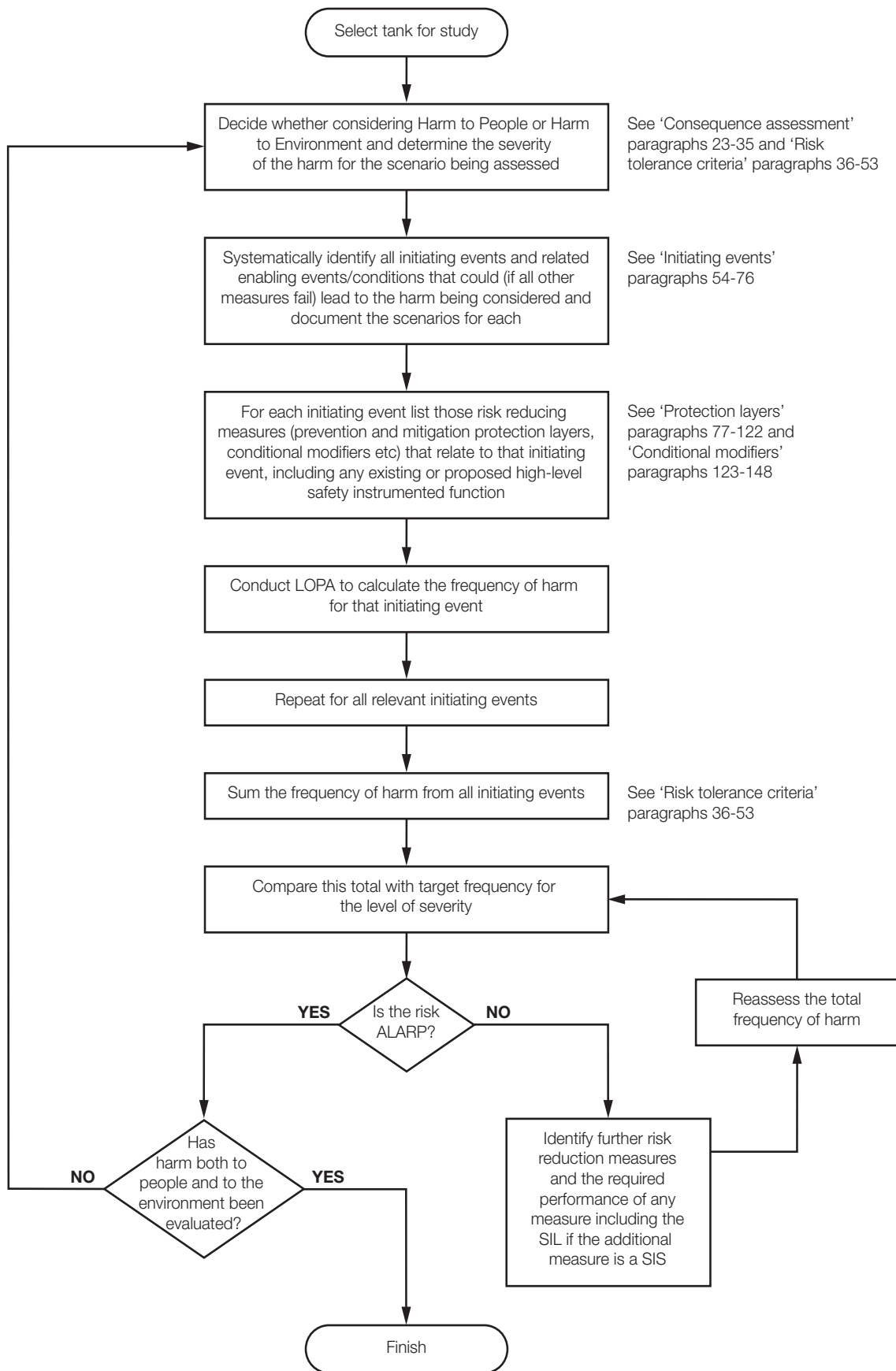


Figure 22 Flowchart for application of LOPA process

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 (RR718⁵⁹). 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	$250\text{m} < r < 400$ 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.

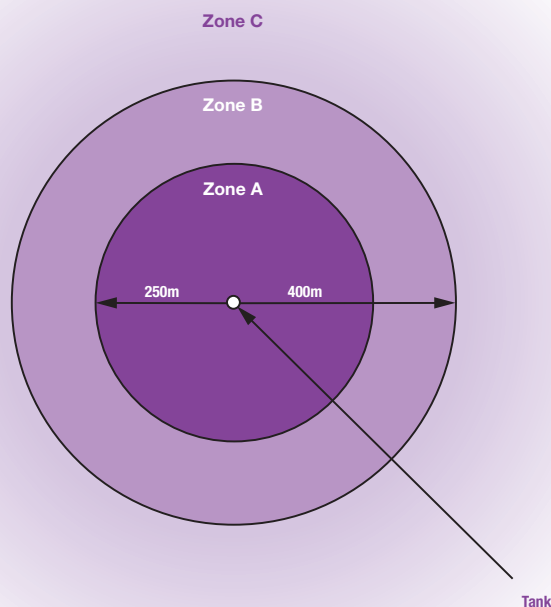


Figure 23 Hazardous zones for a Buncefield-type explosion

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 <ul style="list-style-type: none"> – Major airborne release with serious off-site effects – Site shutdown – Serious contamination of groundwater or watercourse with extensive loss of aquatic life
5	Major <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – Hospital treatment required – Public warning and off-site emergency plan invoked – Hazardous substance releases into water course with ½ mile effect
3	Significant <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 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

111 Secondary 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 CRR133⁶⁵). 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 Industries⁶⁶ 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 *Ignition 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 CRR203⁶⁹ 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:

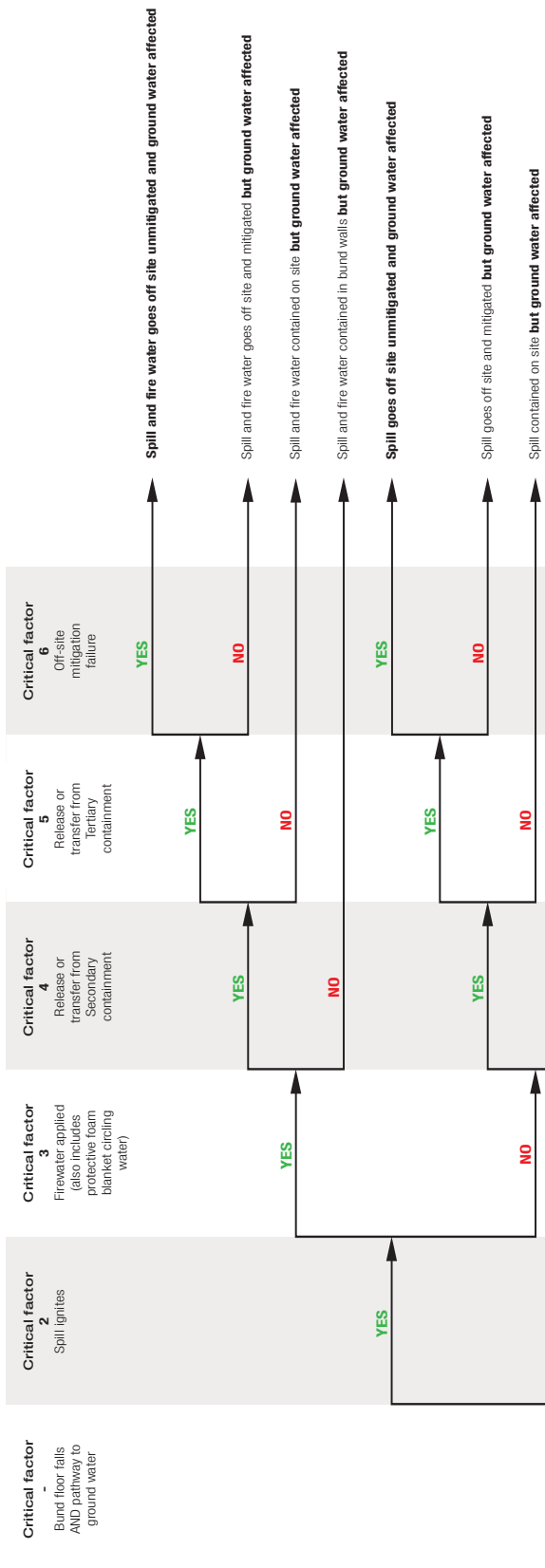
- clear definition of the SIL required for the safety instrumented system in terms of reliability level, eg PFD;
- it should also provide the basis of the functional specification of the SIS.

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

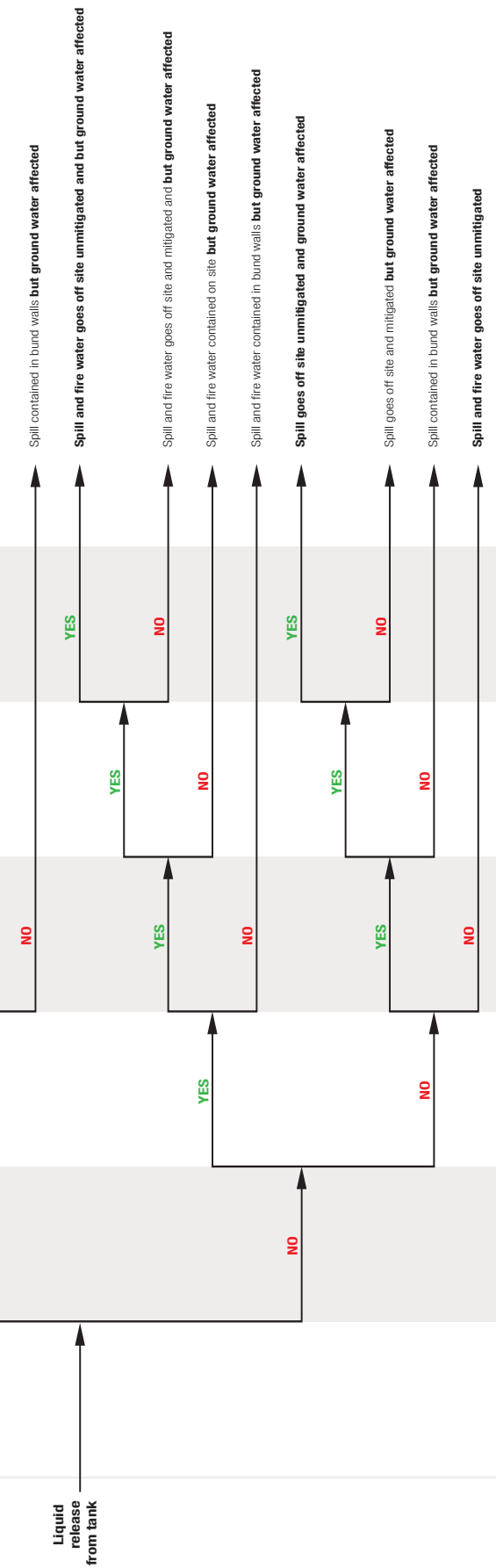
153 HSE reviewed a number of early LOPA studies of overfill protection completed following the Buncefield incident (see RR716⁷⁰). A number of errors and problems, listed below, were identified:

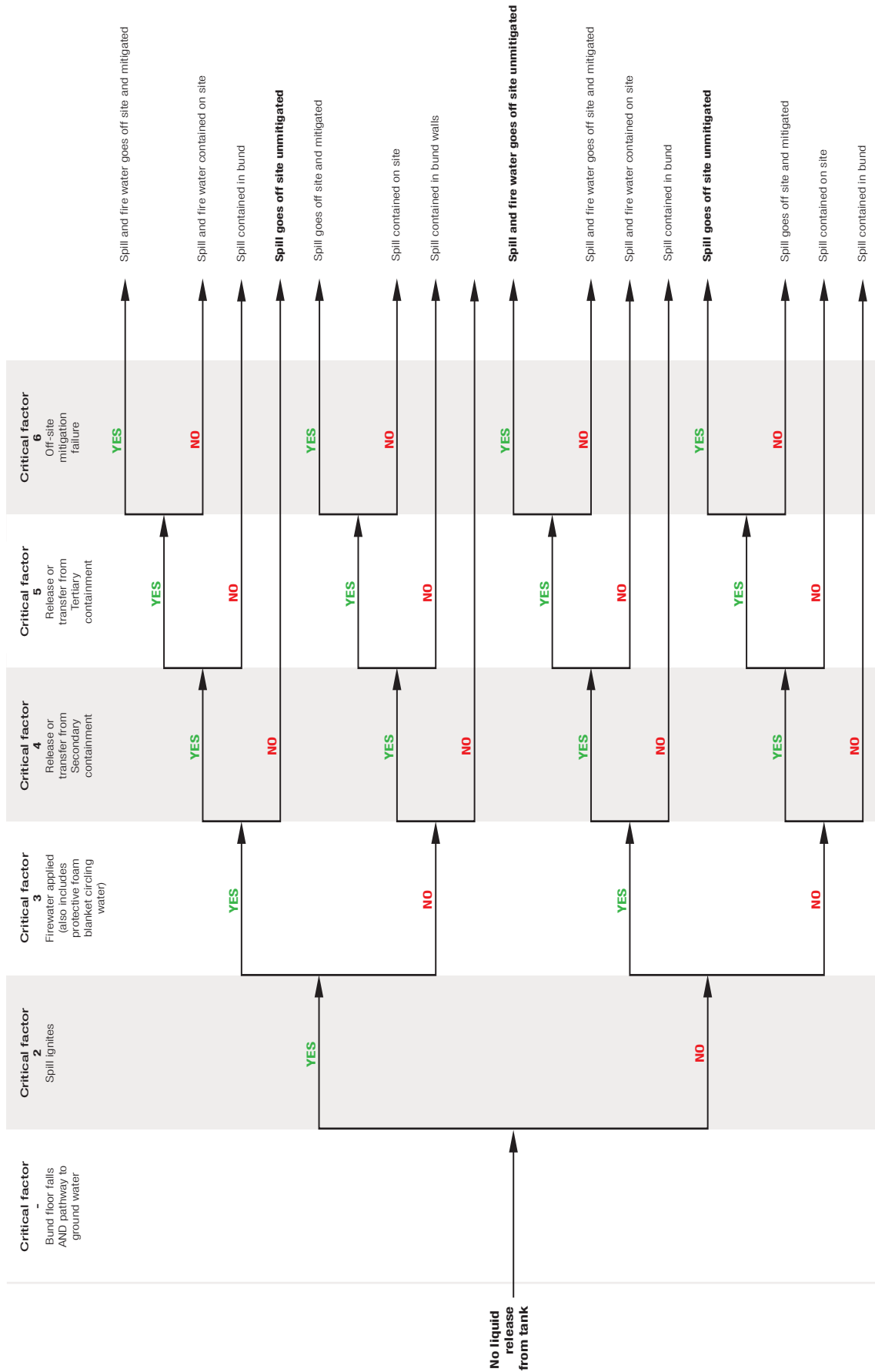
- human error probability too optimistic;
- independence of human operators (double counting of benefit from human tasks);
- risk factors due to the number of tanks on any particular site;
- little available data on ATG errors and failures;
- incorrect logic used to combine various factors;
- incorrect 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



Environmental damage from a tank overflow





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.

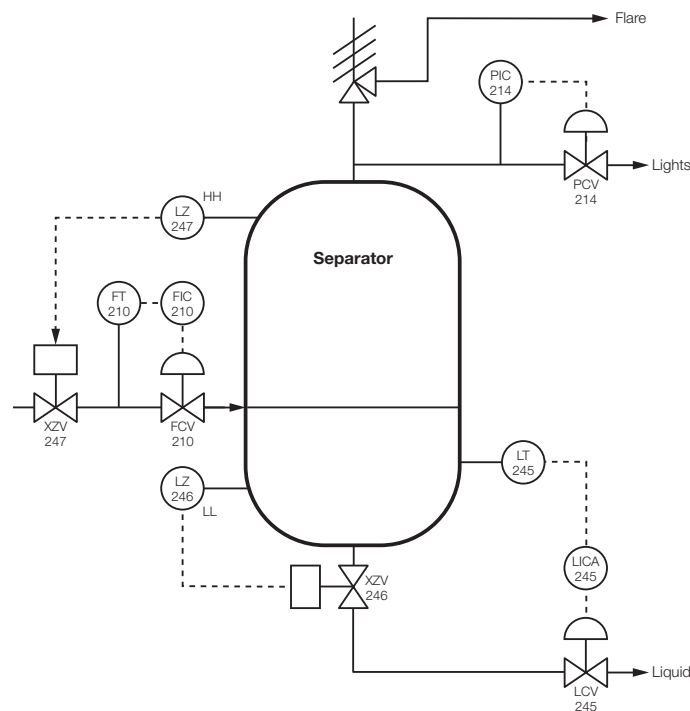


Figure 24 Simplified process schematic

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.

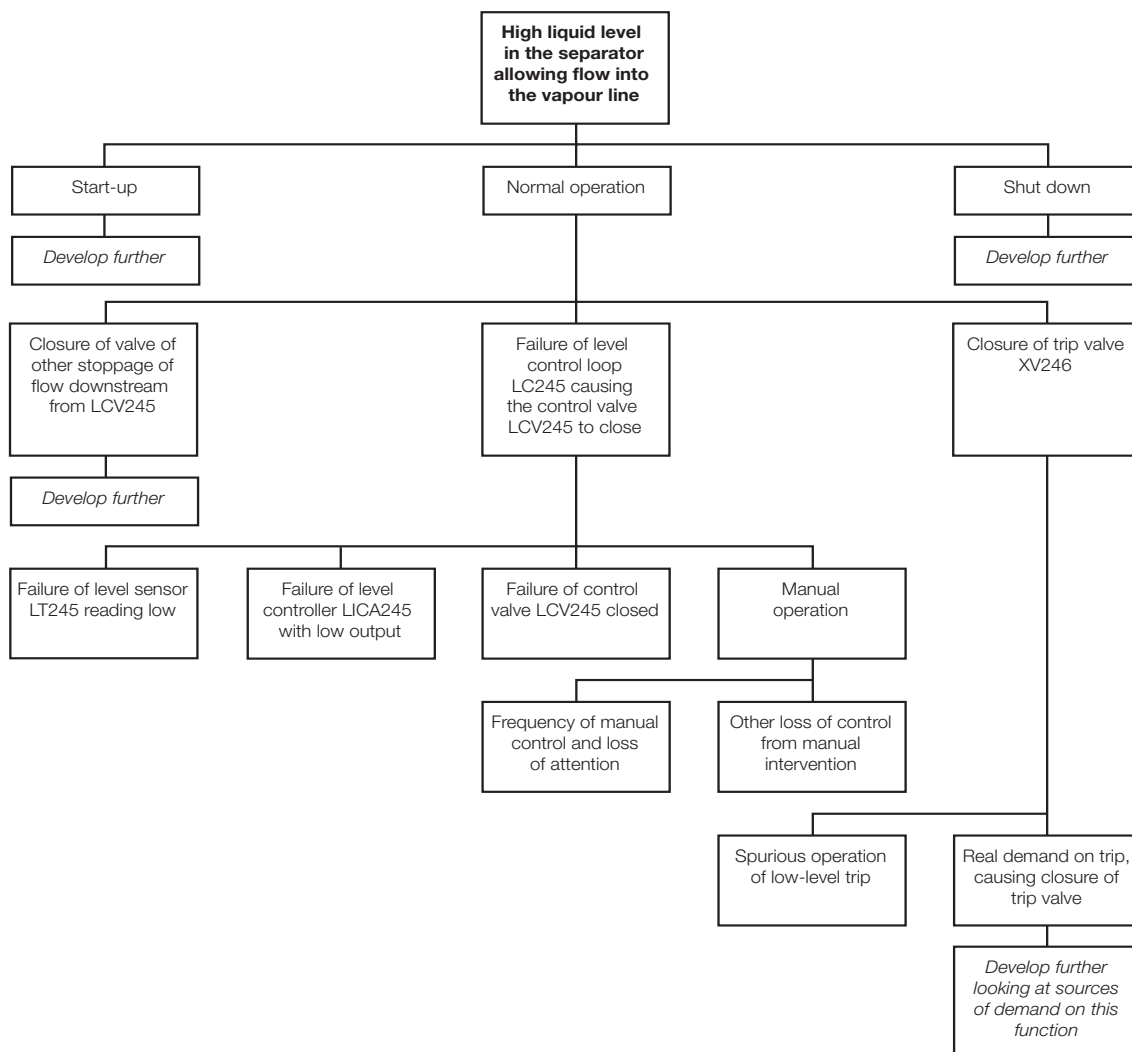


Figure 25 Demand tree illustration

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.

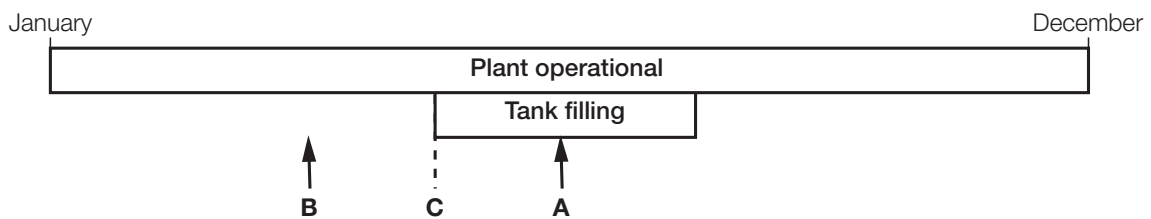


Figure 26 Equipment item failure

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 $\lambda \times t/8760$ 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.

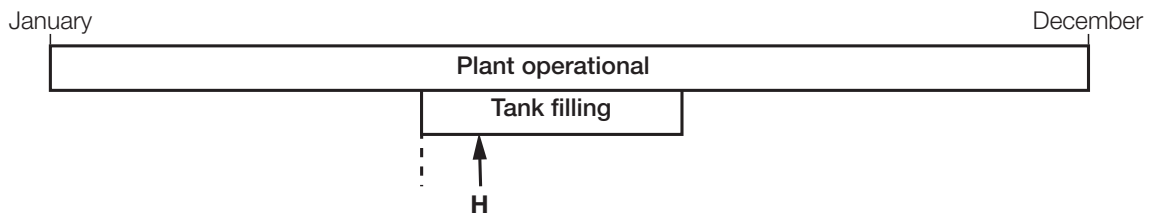


Figure 27 Human action

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.

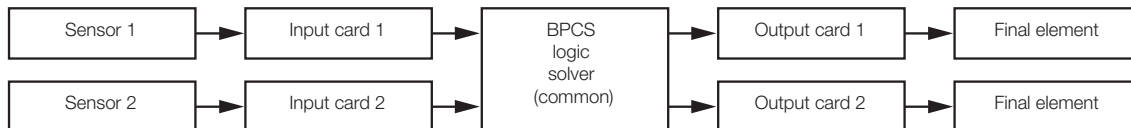


Figure 28 Possible structure of sufficient independent control functions within the BPCS

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	<ul style="list-style-type: none"> – 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.

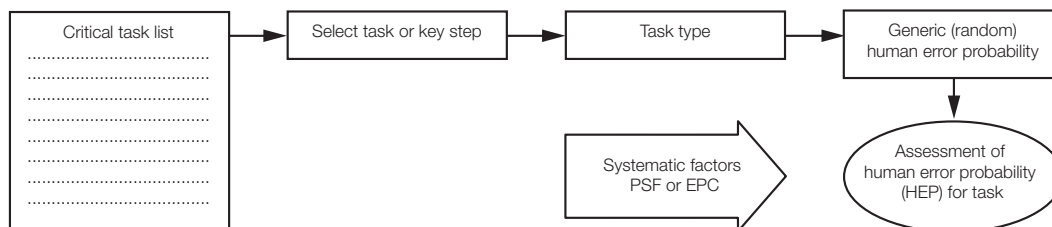


Figure 29 Process for assessing human error probability

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:

$$\text{Initiating event frequency (/yr)} = \text{Task frequency (/yr)} \times \text{HEP}$$

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:

$$\begin{aligned} \text{Initiating event frequency (/yr)} &= \text{Task frequency (/yr)} \times \text{HEP} \\ &= 52 \times 0.01 \\ &= 0.52 \text{ per year} \end{aligned}$$

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.

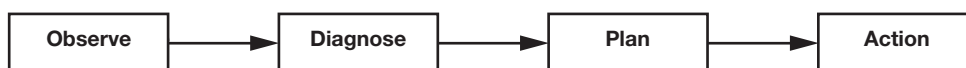


Figure 31 Sequence of operator sub-tasks

- **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.

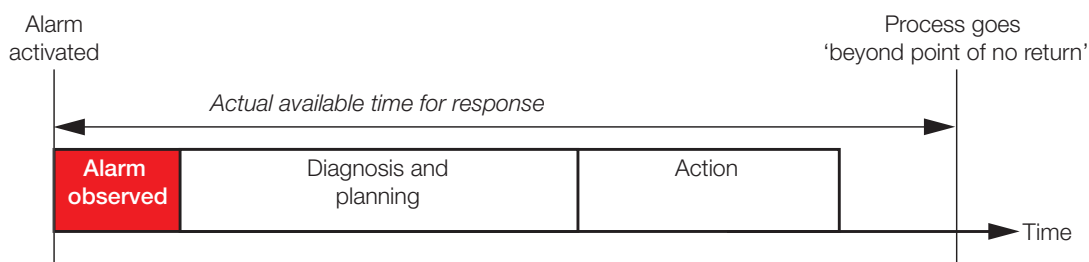


Figure 32 Time for response to alarm

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:

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

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 191⁷² 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.

Appendix 3 Guidance on defining tank capacity

This appendix was previously published as 'Appendix 2: Defining tank capacity' of the BSTG report.

Worked example 1

1 The following is an example of the application of this guidance to an actual tank.

Tank parameters

2 The tank in this example is a fixed roof type (no internal floating roof) with a shell height of 20 m measured from the base, which is flat and level. The tank has a nominal maximum capacity of 10 000 m³ if filled to the overfill level. It receives a product with an SG of less than 1.0, at rates up to a maximum of 1200 m³/hr.

Maximum capacity (overfill level)

3 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank. For fixed roof tanks without an internal roof, loss of containment is expected to occur from a fitting in the roof, typically a PV valve or a dip hatch (if open). For the purposes of setting alarms the overfill level for tanks of this type is considered to be the top of the shell. This gives additional safety margins and greatly simplifies the overfill calculation. Thus for this example the overfill level is defined as the top of the shell. This is 20 m above the base of the tank.

LAHH

4 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

5 On this tank, the LAHH includes a trip function to terminate the transfer. For a well-designed and maintained safety instrumented protective system, a response time of two minutes between activation and complete cessation of flow into the tank is claimed. This includes the time needed to take urgent action in case the trip action is not successful – in this case to immediately close another remotely operated valve, readily accessible in the control room (the system having been designed for this emergency closure).

6 This equates to a maximum volume of $2 \times 1200/60 = 40 \text{ m}^3$. Based on the tank dimensions, this is equivalent to a height of 0.08 m. Thus, the LAHH is set 0.08 m below the overfill level at 19.92 m.

7 There might need to be an additional allowance added to this bare-minimum figure, for 'level surges' during filling, and also possible thermal expansion of the contents after the transfer has been stopped.

LAH

8 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail.

9 In this case, a response time of five minutes is claimed between activation of the LAH and complete cessation of flow into the tank.

10 This equates to a maximum volume of $5 \times 1200/60 = 100 \text{ m}^3$. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the LAH is set 0.2 m below the LAHH, or 0.28 m below the overfill level, at 19.72 m.

Normal fill level

11 The process control system should ensure that all filling operations are terminated at the pre-determined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

Worked example 2

12 The following is a second example of the application of this guidance to an actual tank.

Tank parameters

13 The tank in this example is an internal floating roof type with a shell height of 20 m measured from the base, which is flat and level. The tank has a nominal maximum capacity of 10 000 m³ if filled to the overfill level. It receives a product with an SG of less than 1.0, at rates up to a maximum of 1200 m³/hr.

Maximum capacity (overfill level)

14 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank.

15 For internal floating roof tanks a level must be established at the point where the floating roof will be damaged by any internal roof structure. Hence for these tanks this level will always be below the top of shell.

16 For this example the overfill level is determined as the point at which the internal floating roof strikes an internal stiffening spar located 0.25 m below the top of the shell. The floating roof is 0.25 m deep. Thus the overfill level is 0.5 m below the top of the shell, or 19.5 m above the base of the tank.

LAHH

17 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

18 On this tank, the LAHH includes a trip function to terminate the transfer. For a well-designed and maintained safety instrumented protective system, a response time of two minutes between activation and complete cessation of flow into the tank is claimed. This includes the time needed to take urgent action in case the trip action is not successful – in this case to immediately close another remotely operated valve, readily accessible in the control room (the system having been designed for this emergency closure).

19 This equates to a maximum volume of $2 \times 1200/60 = 40 \text{ m}^3$. Based on the tank dimensions, this is equivalent to a height of 0.08 m. Thus, the LAHH is set 0.08 m below the overfill level at 19.42 m.

20 There might need to be an additional allowance added to this bare-minimum figure, for 'level surges' during filling, and also possible thermal expansion of the contents after the transfer has been stopped.

LAH

21 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail.

22 In this case, a response time of five minutes is claimed between activation of the LAH and complete cessation of flow into the tank.

23 This equates to a maximum volume of $5 \times 1200/60 = 100 \text{ m}^3$. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the LAH is set 0.2 m below the LAHH, or 0.28 m below the overfill level, at 19.22 m.

Normal fill level

24 The process control system should ensure that all filling operations are terminated at the pre-determined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

25 The normal fill level and the LAH should not coincide. The normal fill level and LAH should be close to maximise the usable capacity of the tank, but sufficiently separated so as to avoid spurious alarms, eg due to level surge or thermal expansion when the tank is filled to the normal fill level.

26 Any process alarm/notification used to indicate that the normal fill level has been reached must be clearly distinguishable from the LAH, and reflect the higher priority response applicable to the LAH.

27 In this example, an allowance of five minutes is given for the process control system (including the operator) to terminate the transfer when the level reaches the normal fill level. This equates to a maximum volume of $5 \times 1200/60 = 100 \text{ m}^3$. Based on the tank dimensions, this is equivalent to a height of 0.2 m. Thus, the normal fill level is set 0.2 m below the LAH, or 0.48 m below the overfill level, at 19.02 m.

Worked example 3

28 The following is a third example of the application of this guidance to an actual tank.

Tank parameters

29 The tank in this example is an external floating roof type with a shell height of 22 m measured from the base (which is flat and level) and a diameter of 24 m giving $450 \text{ m}^3/\text{m}$. It receives a product with an SG of less than 1.0, at rates up to a maximum of $1100 \text{ m}^3/\text{hr}$, resulting in a rising level rate of 2.43 m/hr .

Maximum capacity (overfill level)

30 The tank overfill level is defined as the point at which either the tank will suffer mechanical damage or product will be lost from the tank. The company standard for its external floating roof tanks requires:

- 800 mm for the depth of the floating pontoon;
- 750 mm for the depth of the primary and secondary seal;
- 50 mm additional free clearance between moving parts of the roof and seal, and any parts fixed to the shell.

The total allowance is therefore 1600 mm, and so the overfill level is this distance below the top of the shell, or 20.4 m above the base of the tank.

LAHH

31 The fundamental aim of the tank alarm and trip system is to ensure that the overfill level is never reached. In reality, there will remain a small, but finite probability of failure of the device.

32 This tank does not have a trip function to terminate the transfer. The company has determined the actual response time for all its tanks, based upon actual timed emergency response exercises, has documented that as part of its tank level documentation, would review it when any relevant change was made, and tank level documentation is included on its audit schedule. Rather than use specific values per tank, a conservative value of 10 minutes is used for all tanks, in order to achieve standardisation and clarity.

33 This 10 minutes equates to a height margin of 0.4 m ($2.43 \times 10/60$). Thus, the LAHH of the independent device is set 0.4 m below the overfill level at 20.0 m.

LAH

34 A primary purpose of the LAH is to reduce demand on the LAHH by ensuring that the level of the LAHH is never reached. In reality, there will be a finite probability that the LAH (or other components of the process control system linked with the LAH) will fail. In this case, the company uses the same 10 minutes response time, having confirmed that the same actions would be taken between activation of the LAH and complete cessation of flow into the tank. Again, the 10 minutes margin results in another 0.4 m drop to this LAH setting for the ATG at 19.6 m.

Normal fill level

35 The process control system should ensure that all filling operations are terminated at the predetermined level and hence should never exceed the specified normal fill level. In reality, there is a finite probability that the process control system will fail and filling will continue.

36 The normal fill level and the LAH should not coincide. The normal fill level and LAH should be close to maximise the usable capacity of the tank, but sufficiently separated so as to avoid spurious alarms, eg due to level surge or thermal expansion when the tank is filled to the normal fill level. This is the point at which operations stop the transfer, and valves are closed. The company has decided that its 10 minute gap is again applicable, and so the normal fill level is set at 19.2 m.

37 Any process alarm/notification used to indicate that the normal fill level has been reached must be clearly distinguishable from the LAH, and reflect the higher priority response applicable to the LAH. This alarm is on the company's tank information system computer. This particular company also sets an additional 'warning' level, again in the TIS, which is intended to alert operations to prepare to stop the transfer. The 10 minutes is again used, to give 18.8 m.

Appendix 4 Guidance on automatic overfill protection systems for bulk gasoline storage tanks

Introduction

1 This appendix provides guidance on good practice on overfill protection for new and existing in-scope tanks. It covers the design, implementation, lifecycle management, maintenance and proof testing for an automatic system on tank overfill protection to achieve the required SIL in compliance with BS EN 61511 so far as is reasonably practicable. It includes annexes on PFD calculations, hardware reliability, configuration requirements for fault tolerance and redundancy.

2 The following items are not covered:

- mechanical integrity of pipelines and delivery systems;
- the effects of automatic shutdown on continuous processes;
- the integrity of manual response to alarms where automatic shutdown is not provided.

3 This guidance is not intended to replace BS EN 61511 but supplement it specifically in relation to tank overfill protection SIS (safety instrumented system). It does not cover all the requirements of BS EN 61511. Where guidance is not given on any requirement such as protection against systematic failures then reference should be made to the standard.

Standards of overfill protection

4 Paragraphs 70–77 in the main report set out the overall requirement for overfill protection. Tanks meeting the criteria in paragraph 24 of the main report should be provided with a high integrity overfill prevention system that, as a minimum, provides a level of SIL 1 as defined in BS EN 61511-1. To reduce risk as low as reasonably practicable the overfill prevention system should preferably be automatic and should be physically and electrically separate from the tank gauging system.

Detailed design requirements

5 The following specific requirements from BS EN 61511 should all be complied with:

- the design must meet the safety requirement specification;
- the system architecture must meet the hardware fault tolerance requirements for the specified SIL (see Annexes 1 and 2);
- the overall PFD of the safety instrumented function design must meet the PFD as determined by the risk assessment (see Annex 3);
- subsystems should meet the general requirements of BS EN 61511 section 11.5.2 and section 12 for programmable subsystems.

6 General good practice: The following should be considered during the design, development and maintenance of an automatic overfill protection system:

- Dominant failure modes of any device should be to the safe state or dangerous failure detected, unless architecture allows for fault tolerance.
- Diagnostics for all subsystems are recommended where necessary to detect dangerous unrevealed failures. Procedures should be in place to respond to diagnostic alarms. Diagnostics should be tested during proof testing
- The SIS should be capable of carrying out its designed function on loss of power (pneumatic, electric, hydraulic) (BS EN 61511 section 11.2.11).
- Operation of the SIF should generate an alert to the operator.
- Sufficient independence and separation should be demonstrated between the SIS and the BPCS (BS EN 61511 section 9.5).
- User's own valid failure rate data should be used within PFD calculations. Where this is not available use of appropriate recognised external data sources is acceptable.
- The SIS design should provide facilities for ease of proof testing.
- All equipment should be suitably designed for the process and operating conditions, the environment and the hazardous area requirements.
- Input overrides should only be provided where justified (as described in paragraph 24). Output overrides should not be used.

7 Level sensors:

- Analogue level sensors are preferred to digital (switched) sensors.
- A discrepancy alarm between the tank level indication system and an analogue trip system can be used to alert that there is a problem with the level measurement.

8 Logic solver fault tolerance:

- Non-programmable logic solvers should comply with Table 6 of BS EN 61511.
- Programmable logic solvers should comply with Table 5 of BS EN 61511.

9 Final elements:

- Electrically operated valves that do not fail safe on loss of power should have a backup power supply. The loss of power supply should be alerted to the operator.
- Auto reset of the final element should not be possible.
- An adequate margin of safety factor should be provided for actuator torque on shut-off valves. The break off (from open position) force/torque recommended as minimum 1.5 times.
- Manual operating facilities which inhibit the SIF operation on valves (eg hand wheels) are not recommended.
- Performance of the shut-off valve should meet the requirements of the safety requirement specification (eg shut-off classification)
- Closure of shut-off valves should be designed to prevent pressure surges on the system pipework and couplings (particularly to flexible pipes on ship to shore).

Note To prevent damage to pipelines and flexible hoses due to pressure surges or over-pressure in the event of a shutdown for any reason including inadvertent export valve closure, the supplying source (eg ships) should already be fitted with the necessary protection against over-pressure or no flow in the event of dead head or other effect of shutdown. This is the responsibility of the shipping company and ship owner but the terminal owner has the responsibility of informing the shipping company that an automatic shutdown system is in operation and may operate at any time.

Architectures of overfill protection systems

New tank automatic overfill protection system

10 Automatic overfill protection systems for a new tank should meet the requirements of BS EN 61511 and paragraphs 5 to 9.

11 The following architecture shows an independent automatic system, which will operate to shut off product delivery to the tank without any human action.

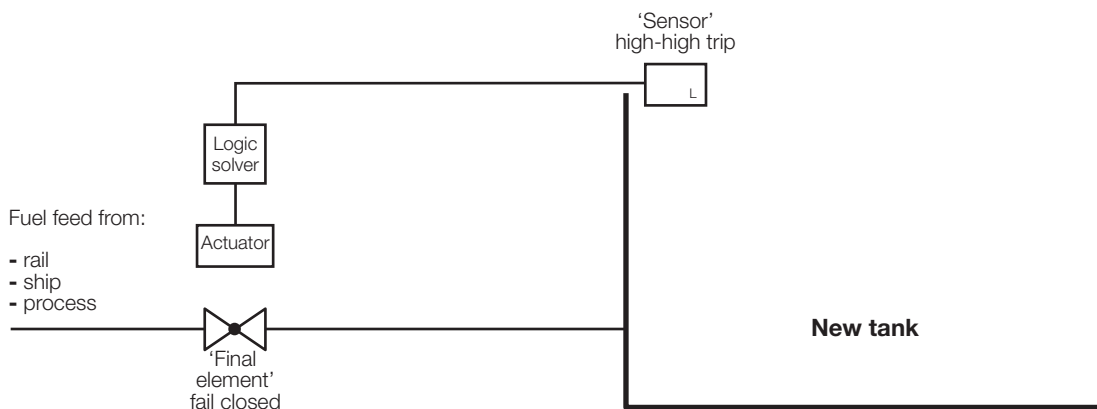


Figure 33 High-high level trip

12 Figure 33 shows a new tank fitted with a high-high trip sensor (independent from any other tank instrumentation) connected to a logic solver and a fail closed valve. This arrangement should meet the requirements for SIL 1 and may meet the requirements for SIL 2. PFD calculations and conformity to hardware fault tolerance require checking. (See Annexes 1–3.)

Existing tank installations

13 Where there is an existing overfill protection system to a standard other than BS EN 61511, a gap analysis should be conducted to determine the extent of compliance with BS EN 61511.

14 For SIL 2 or higher safety requirements the installation should fully comply with BS EN 61511.

15 For SIL 1 safety requirements, improvements to existing systems may still be necessary to meet ALARP even in cases where it is not reasonably practicable to upgrade or replace existing systems to fully meet the requirements of BS EN 61511. The following issues should be addressed when considering what improvements are required:

- The degree of independence of sensors used for the high-high alarm/shut-off.
- The suitability of the logic solver.
- Degree of independence from BPCS.
- Demonstration and evidence of prior use.
- Suitability of final elements.

16 It should be noted that a prescriptive description of the steps needed to meet BS EN 61511 so far as is reasonably practicable cannot be provided in this guidance. The degree of compliance should be discussed and agreed between the dutyholder and the CA on a case-by-case basis. However some further more detailed points for consideration are given below, and in Annex 4.

17 Figure 34 illustrates the use of a motor operated valve/electrically operated valve (MOV/EOV) as the final element within an overfill protection system.

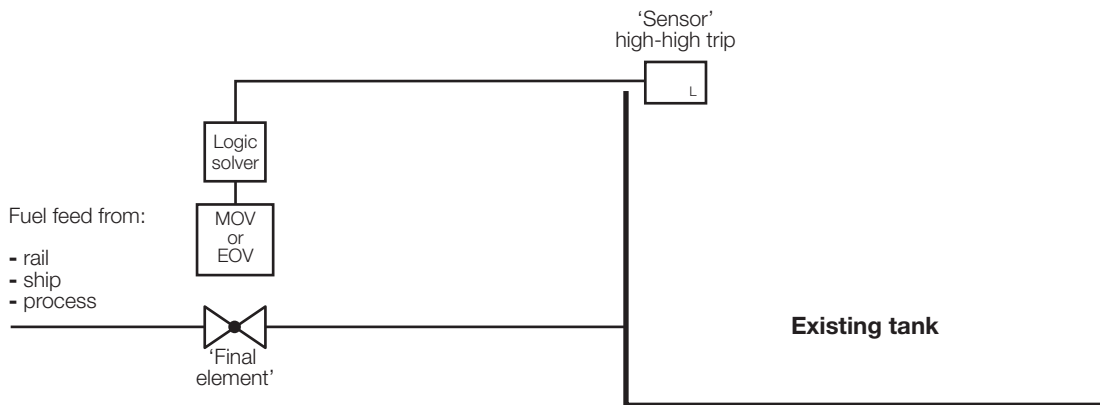


Figure 34 Motor/Electrically operated valve final element

18 Use of supply pump: Figure 35 shows a supply pump that can be used as the final element of an automatic trip system where it can be demonstrated that the gravitation feed through the stopped pump does not continue with an unacceptable overfill rate. This system should be followed with manual closure of an isolation valve.

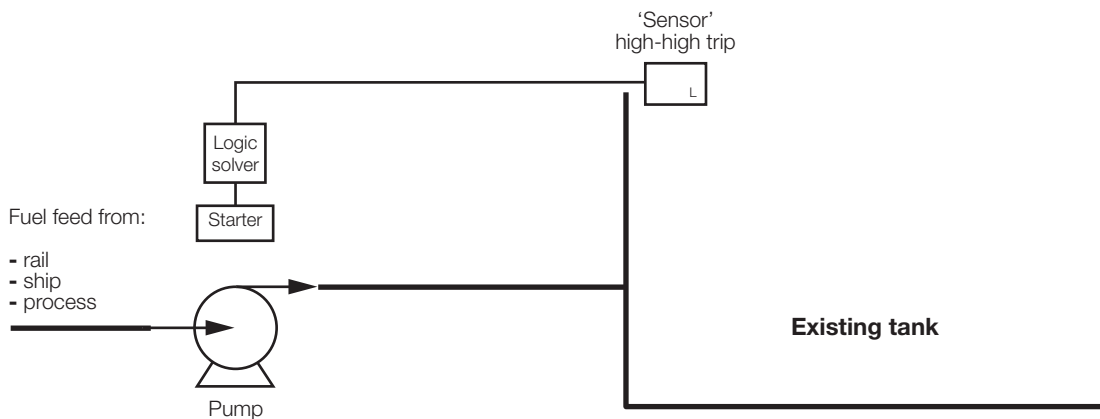


Figure 35 Supply pump as final element

19 Multiple tanks:

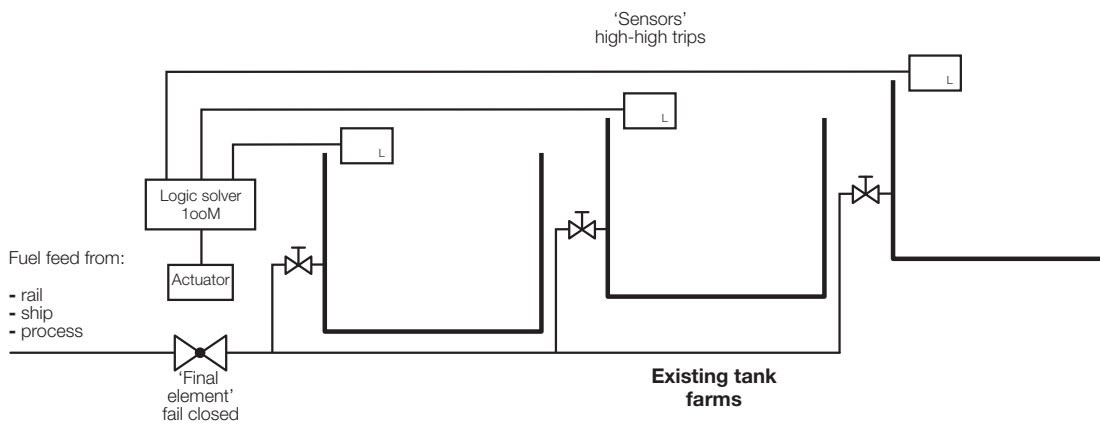


Figure 36 Use of a single final element (valve or pump) to isolate multiple tanks. Any sensor trips the final element

Lifecycle maintenance

20 To assure the continued effective operation of an overfill protection system appropriate maintenance will be required over its lifetime. Key elements in planning such lifecycle maintenance are:

- The principal activity of maintenance is proof testing to identify any dangerous un-revealed failures. See 'Proof testing' in this appendix.
- System hardware should be inspected to check the mechanical integrity of system components; this may be performed at the same time as the testing.
- Manufacturers' recommended installation and maintenance activities should be carried out to ensure that all system components are correctly installed, in good working order, lubricated, adjusted and protected.
- Calibration, where necessary, should be checked when systems are tested or more frequently if required.
- Modifications should be subject to a management of change procedure to check that the safety function is not affected by the modification (see section on management).

Further guidance on the management of instrumented systems for fuel storage tank installations is given in response to Recommendation 2.

Overrides

21 Overrides should not be used during tank filling. However, if an override is deemed to be necessary then management control is required. As a minimum the override management controls should include:

- override management process;
- a method for risk assessing and identifying appropriate measures before applying override;
- time limit for the override;
- authorised signatory;
- override information handed across shift changes;
- time limit for review of an override;
- no output overrides allowed;
- the status when an override has been applied (eg alarmed);
- an audit process.

Manual shutdown push-buttons

22 A manual means should be provided to terminate the transfer of product into the tank. This does not form part of the automatic tank overfill instrumented function. Periodic testing of this function is recommended.

Proof testing

Testing overfill protection systems

23 Overfill protection alarms or shutdown systems using high level switches or other two-state detectors may be inactive for long periods and may develop unrevealed faults. Such faults cause the system to fail to danger when required to operate.

Proof testing

24 All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures frequently enough to ensure the specified safety integrity level is maintained in practice.

25 Proof testing should be end to end so far as is reasonably practicable including the detector at the liquid interface and the final element. The test period should be determined by calculation according to the historical failure rate for each component or the system and the probability of failure on demand required to achieve the specified SIL. Records of test results, including faults found and any repairs carried out, should be kept. Part 1 of BS EN 61511 provides appropriate guidance on this issue.

26 Safety systems which operate only infrequently may remain dormant for long periods and may suffer failures which are unrevealed. Proof testing is required to reveal such failures, exercise the system and demonstrate that the system functions as intended.

Test coverage

27 A proof test or a number of tests should cover, where practicable, all dangerous failure modes. The test interval will be that determined in the PFD calculations.

Part tests

28 A full function test should be carried out, where practicable. Where not practicable, and more than one test is used to demonstrate the function operation, then there should be sufficient overlap such that no parts of the function are not tested.

29 Proof tests (part or full) should be carried out before and after any calibration, corrective, remedial or intrusive action carried out. For example, proof tests should be carried out before and after maintenance.

Proof test method

30 This should be carried out, where practicable, using wetted process conditions to operate the sensor. Where this is not practicable then a simulated test of the sensor (eg radar, vibronics or radio frequency admittance) may be acceptable where it can be demonstrated that the wetted contact cannot be prevented from operating the sensor on genuine high-level condition.

31 Final element (Isolation valves, pump) should be tripped for a full proof test.

32 Testing should cover the testing of any diagnostic features.

33 Further guidance is in the HSE research report CRR428 Principles for proof testing of safety instrumented systems in the chemical industry.⁷³

Documentation

34 The requirements of BS EN 61511 concerning documentation should be met in full for new systems. For existing systems, the documentation requirements should be complied with as far as is reasonably practicable.

Recommended data sources for SIL calculations

35 Where a company does not have their own failure data, paragraph 38 lists typical data sources that could be used to establish the recommended parameter values for the SIL calculation of SIFs and the architectures of the SISs.

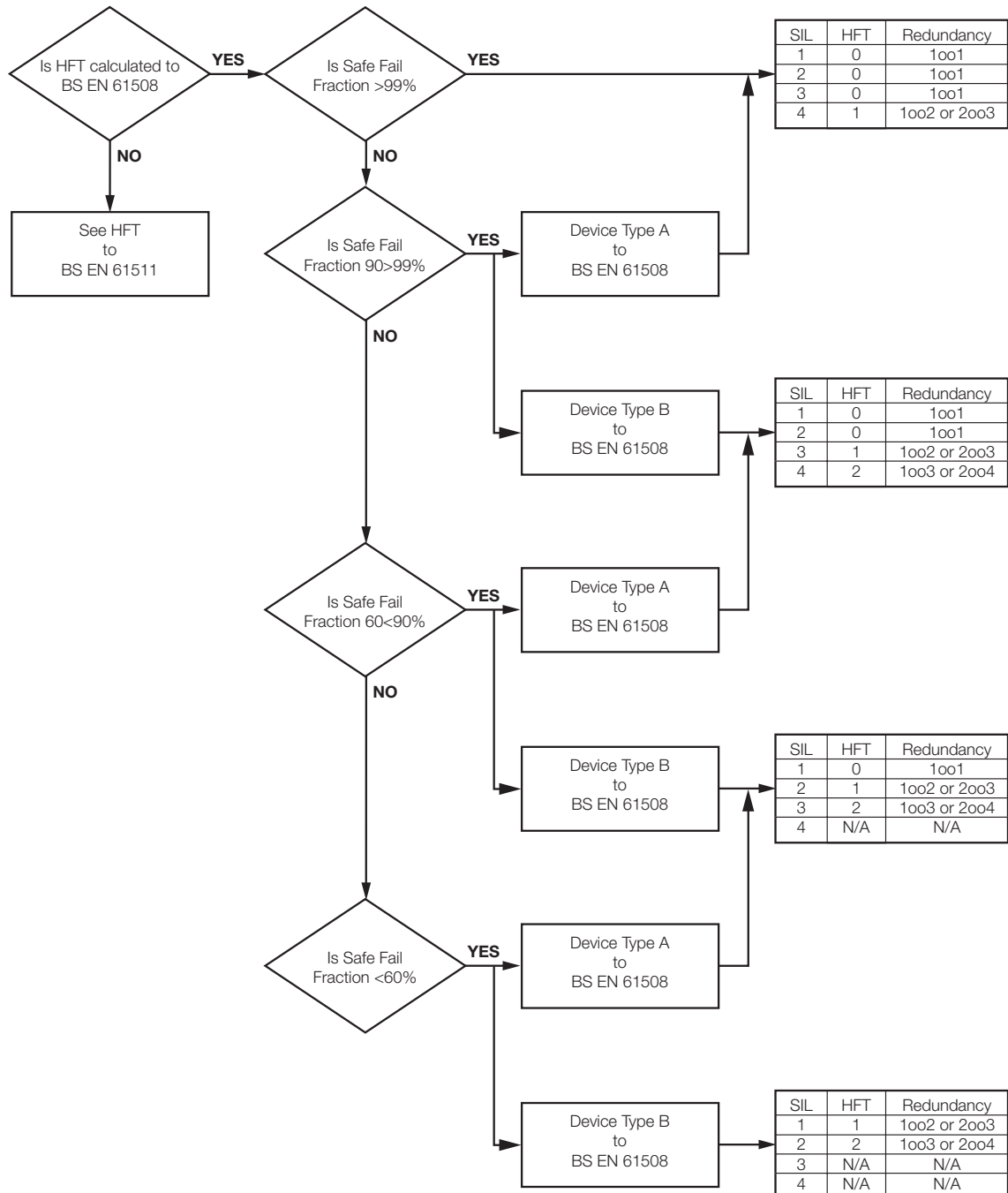
36 Users should consider the effect of the installed and process environment on the data used.

37 Manufacturers' reliability data can be used where it can be shown to be appropriate and the type, duty and environment are similar to that specified.

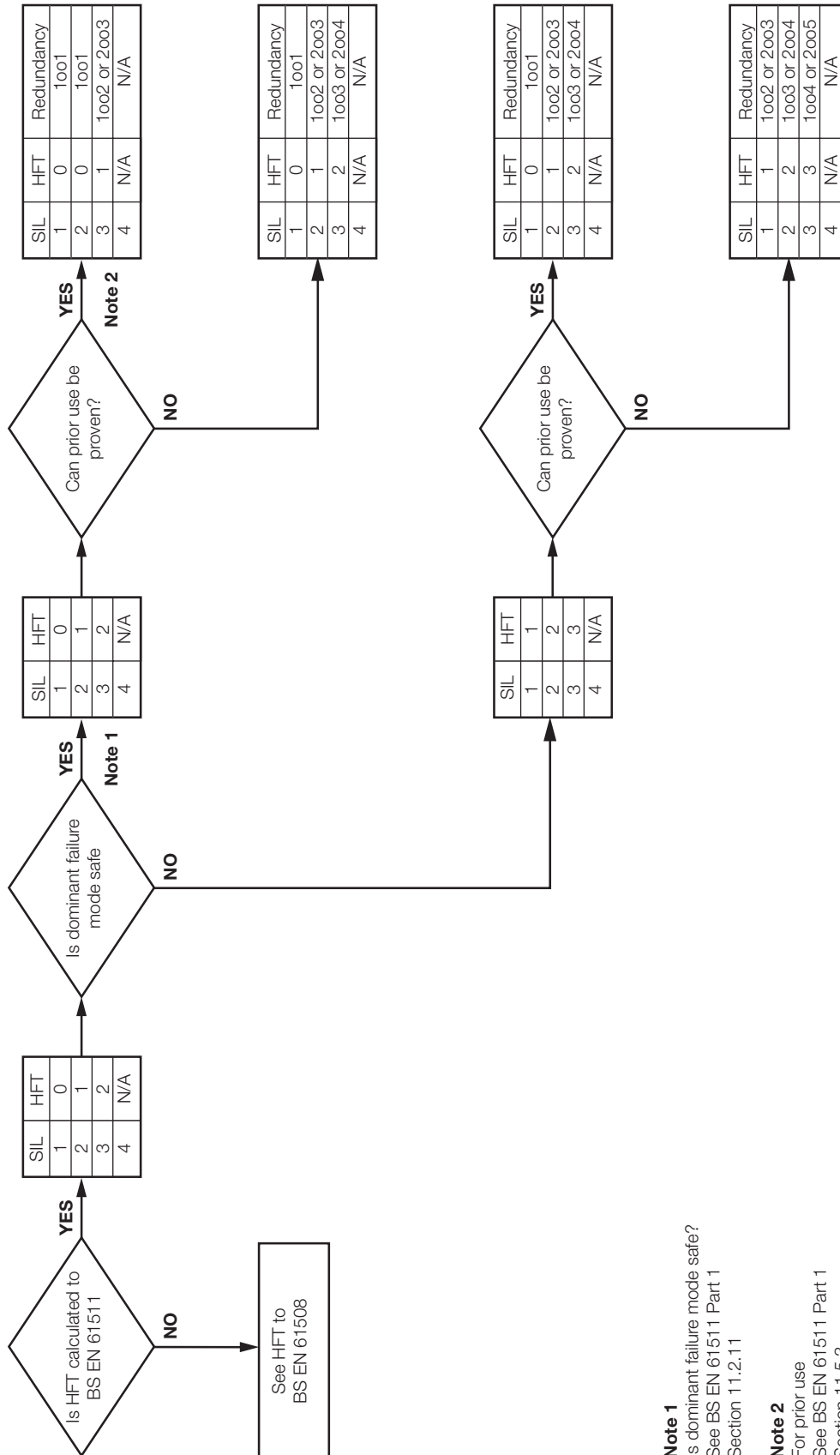
38 Suggested data sources for SIL calculations:

- *Offshore reliability data handbook 2002* OREDA 2002 release 6.1;
- Idaho Chemical Processing Plant, Failure Rate Database ICPP 1995;
- *Safety Equipment Reliability Handbook* EXIDA;
- *Association of chemical and associated industries in the Rhône-Alpes region* GICRA GT FMD 2002;
- *Database PDS data handbook* SINTEF 2006;
- *European Industry Reliability Data Bank* EIREDA 1995.

Annex 1 Hardware fault tolerance calculation to BS EN 61508 for sensors, final elements and non-programmable logic solvers



Annex 2 Hardware Fault Tolerance (HFT) calculation to BS EN 61511 (for sensors, final elements and non-programmable Logic solvers)



Note 1
Is dominant failure mode safe?
See BS EN 61511 Part 1
Section 11.2.1.1

Note 2
For prior use
See BS EN 61511 Part 1
Section 11.5.3

Annex 3 $PFD_{(avg)}$ calculation and influence of loop architecture

39 In these examples assumptions and failure rate data used in this annex are fictitious and any similarity to values used in industry is coincidental, thus the values used should not be taken from this guide and used for PFD calculations. The values used are to demonstrate the use of the example calculation method.

Average probability of failure on demand (for a low demand mode of operation)

40 The following is one example of how the average probability of failure on demand of a safety function for a given system may be derived and is based upon Annex B in BS EN 61508-6.

41 The average probability of failure on demand of a safety function for a given system is determined by calculating and combining the average probability of failure on demand for all the subsystems which together provide the safety function. Since the probabilities are likely to be small, this can be expressed by the following:

$$PFD_{SYS} = PFD_S + PFD_{LS} + PFD_{FE}$$

Where PFD_{SYS} is the average probability of failure on demand of the system

PFD_S is the average probability of failure on demand of the sensor

PFD_{LS} is the average probability of failure on demand of the logic solver

PFD_{FE} is the average probability of failure on demand of the final element

42 If the safety function depends on more than one voted group of sensors or actuators, the combined average probability of failure on demand of the sensor or final element subsystem, PFDs or PFD_{FE} , is given in the following equations, where PFD_{Gi} and PFD_{Gj} is the average probability of failure on demand for each voted group of sensors and final elements respectively:

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_j PFD_{Gj}$$

1001 architecture

43 For the example given in Figure 37 (1001 architecture) it can be shown that the average probability of failure on demand for a system with a very low failure rate is:

$$\begin{aligned} PFD_{G(1001)} &= (\lambda_{DU} + \lambda_{DD}) t_{CE} \\ &= \lambda_D \times t_{CE} \\ &= \lambda_{DU} \left(\frac{T_1}{2} + MTTR \right) + \lambda_{DD} \times MTTR \end{aligned}$$

Where $t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR$

Where $PFD_{G(1001)}$ is the average probability of failure on demand of the 1001 system

λ_{DU} is the dangerous undetected failure rate (per hour)

λ_{DD} is the dangerous detected failure rate (per hour)

T_1 is the proof test interval (in hours)

$MTTR$ is the mean time to repair (in hours)

t_{CE} is the channel equivalent mean down time (in hours) resulting from a dangerous failure (down time for all components in the channel of the subsystem)

1002 architecture

44 For the example given in Figure 38 (1002 architecture) it can be shown that the average probability of failure on demand for a system with a very low failure rate is:

$$PFD_{G(1002)} = 2(1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU}^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \left(\frac{T_1}{2} + MTTR \right)$$

Where $t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR$

And $t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR$

Where $PFD_{G(1002)}$ is the average probability of failure on demand of the 1002 system

λ_{DU} is the dangerous undetected failure rate (per hour)

λ_{DD} is the dangerous detected failure rate (per hour)

β is the fraction of undetected failures that have a common cause

β_D is the fraction of detected failures that have a common cause

T_1 is the proof test interval (in hours)

$MTTR$ is the mean time to repair (in hours)

t_{CE} is the channel equivalent mean down time (in hours) resulting from a dangerous failure (down time for all components in the channel of the subsystem)

t_{GE} is the voted group equivalent mean down time (in hours) resulting from a dangerous failure of a channel in a subsystem (combined down time for all channels in the voted group)

Example showing architectural influence on $PFD_{(avg)}$

45 To calculate the $PFD_{(avg)}$ for a complete SIF the failures all elements in the loop need to be summed – the sensor, logic solver and final element

$$PFD_{SYS} = PFD_S + PFD_{LS} + PFD_{FE}$$

46 In the example below, the same instrumentation has been used but in two configurations to achieve a minimum of SIL 1, 1oo1 and 1oo2.

47 The following assumptions have been made in order to calculate the $PFD_{(avg)}$ for the SIF:

- The $PFD_{(avg)}$ value for the logic solver is fixed at 7.11 E-4.
- The β factor for the undetected common cause failures is fixed at 2% (0.02).
- The β_D factor for the detected common cause failures is fixed at 1% (0.01).
- The proof test is a full, perfect proof test as opposed to a partial stroke test.
- The mean time to repair (MTTR) is 8 hours for all elements.
- Single devices comply to all requirements for use in a SIL 2 application.
- The proof test provides 100% coverage factor for dangerous failure detection.

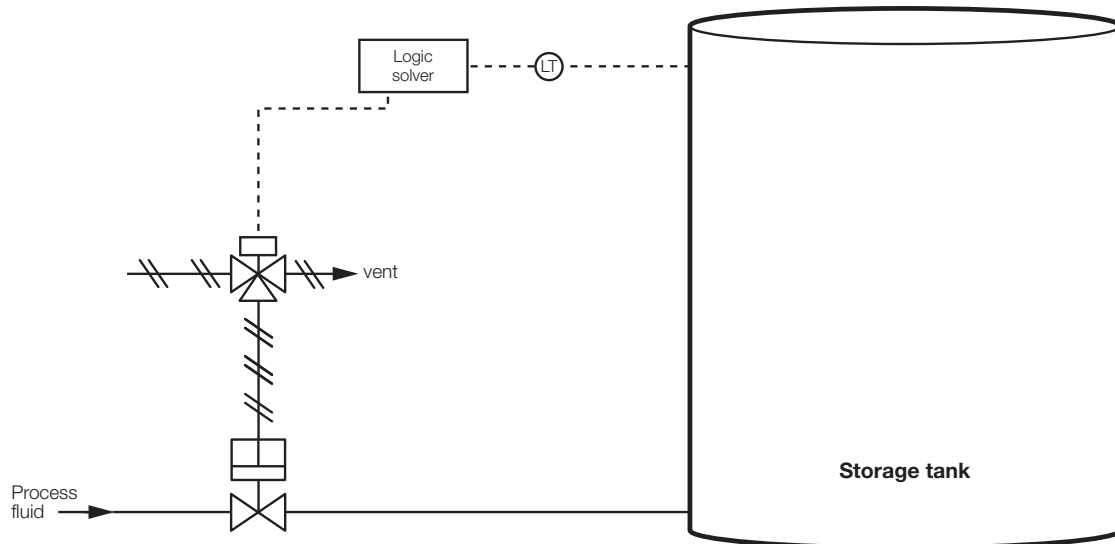


Figure 37 Typical tank overfill protection using 1oo1 architecture

48 Using the $PFD_{(avg)}$ calculations and the assumptions stated previously, the following values for the $PFD_{(avg)}$ have been calculated for the 1oo1 architecture with a proof test interval of one year.

Sensor $PFD_{(1oo1)}$	3.03E-03
Logic Solver $PFD_{(1oo1)}$	7.11E-04
Valve $PFD_{(1oo1)}$	3.15E-05
Total loop $PFD_{(avg)}$	3.77E-03

Achieved requirement for SIL2 $PFD_{(avg)}$

1oo2 architecture

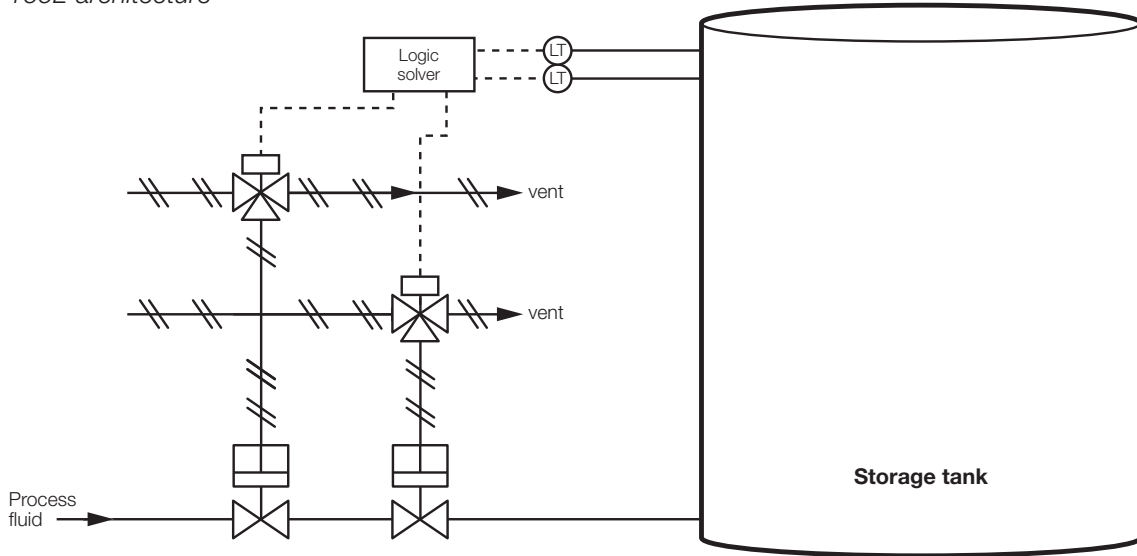


Figure 38 Typical tank overfill protection using 1oo2 architecture

49 Using the $PFD_{(avg)}$ calculations and the assumptions stated previously, the following values for the $PFD_{(avg)}$ have been calculated for the 1oo2 architecture with a proof test interval of one year.

Sensor $PFD_{(1oo2)}$	3.82E-04
Logic Solver $PFD_{(1oo1)}$	7.11E-04
Valve $PFD_{(1oo2)}$	5.72E-06
Total loop $PFD_{(avg)}$	1.10E-03

50 These two worked examples show it is possible to achieve the requirement for SIL 2 $PFD_{(avg)}$ for both configurations. These are only two examples of the possible methods of achieving SIL 2 risk reduction, although other combination of architecture on the inputs and output elements may also be equally valid.

51 It is worth noting that although the $PFD_{(avg)}$ requirement may have been achieved, architectural constraints must also be satisfied and that may result in a more complex architecture – see Annex 2.

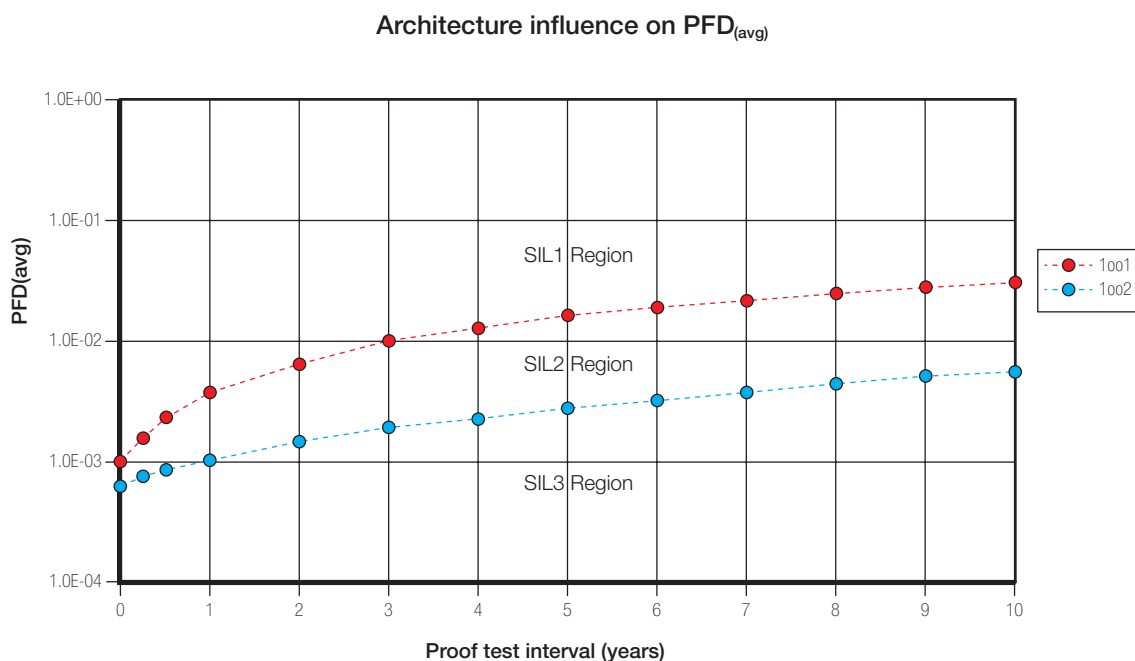


Figure 39 Effect of architecture and proof test interval on system PFD_(avg)

Annex 4 Points for consideration in meeting the requirements of BS EN 61511 so far as is reasonably practicable

52 Where an existing tank meets the requirements set out in paragraphs 73–77 of the main report in all respects other than fully complying with BS EN 61511, then the following issues may be considered:

- Sensors: Whether the high-high level device is independent of the high level alarm, the ATG system or any other high level alarm.
- Logic solvers: Whether there is sufficient independence between the overfill protection system and the tank gauging system.
- System: Whether the configuration of the automated overfill protection system is restricted and controlled as a SIS to prevent inadvertent modification.
- Final elements: Whether fail safe motorised valves (MOVs/EOVs) or the stopping of supply pumps may be an alternative to installing a new valve or modifying an existing manual valve.
- Whether the power supplies for an automated overfill system are independent from the BPCS used for tank level indication and provides redundancy for protection against common mode failure (Note that if the Final Element fails safe on loss of power, a new independent power supply may not be reasonably practicable).
- Whether the hardware fault tolerance and PFD_(avg) of the overfill protection system meets the SIL requirement and can be demonstrated by the end user.

Appendix 5 Guidance for the management of operations and human factors

Introduction

1 The purpose of this appendix is to identify the guidance necessary to address the following MIIIB *Design and operations* report recommendations:

- Recommendations 6 and 7, relating to fuel transfers by pipeline.
- Recommendation 9, record retention and review.
- Recommendation 10, process safety performance.
- Recommendation 19, high reliability organisations.
- Recommendations 23, 24 and 25, delivering high performance.

2 However, all the SMS elements and associated human factors issues that are relevant to the control of major accident hazards, and specifically tank overfill situations, are also important.

3 A high reliability organisation has been defined as one that produces product relatively error-free over a long period of time (see the Baker Report⁷⁴). Two key attributes of high reliability organisations (see 'Managing the unexpected'⁷⁵) are that they:

- have a chronic sense of unease, ie they lack any sense of complacency. For example, they do not assume that because they have not had an incident for ten years, one won't happen imminently;
- make strong responses to weak signals, ie they set their threshold for intervening very low. If something doesn't seem right, they are very likely to stop operations and investigate. This means they accept a much higher level of 'false alarms' than is common in the process industries.

4 Recommendation 19 identified a number of high reliability organisational factors that were of particular importance in the context of the Buncefield investigation.

5 This appendix aims to provide a route-map to existing good practice guidance, where such guidance exists. In situations where no such guidance has been found this appendix establishes what constitutes good practice. Examples of the latter include the industry-specific guidance relating to fuel transfer and storage.

6 This appendix is structured as follows:

- Leadership and safety culture:
 - Leadership, and development of a positive safety culture.
- Process safety:
 - Process safety management.
 - Hazard identification and layers of protection.
- Organisational issues:
 - Roles, responsibilities and competence.
 - Staffing, shift work arrangements and working conditions.
 - Shift handover.
 - Organisational change, and management of contractors.
 - Management of plant and process changes.

- Key principles and procedures for fuel transfer and storage:
 - Principles for safe management of fuel transfer.
 - Operational planning for fuel transfer by pipeline.
 - Principles for consignment transfer agreements.
 - Procedures for control and monitoring of fuel transfer.
 - Information and system interfaces for frontline staff.
- Learning from experience:
 - Availability of records for periodic review.
 - Measuring process safety performance.
 - Investigation of incidents and near misses.
 - Audit and review.

Leadership and development of a positive safety culture

7 Poor safety culture has been found to be a significant causal factor in major accidents such as those concerning Texas City, Chernobyl, Bhopal, the Herald of Free Enterprise disaster, several major rail crashes etc.

8 The leadership of senior managers, and the commitment of the chief executive, is vital to the development of a positive safety culture. The Baker Panel Report has recently drawn specific attention to the importance of:

- process safety leadership at all levels of an organisation;
- implementing process safety management systems; and
- developing a positive, trusting, and open process safety culture.

9 CSB's Investigation Report⁷⁶ into the Texas City Refinery Explosion also identifies safety culture as a key issue requiring leadership of senior executives. It was particularly critical of the lack of a reporting and learning culture, and of a lack of focus on controlling major hazard risk.

Guidance

10 The safety culture of an organisation has been described (HSG48) as the shared values, attitudes and patterns of behaviour that give the organisation its particular character.

11 The term 'safety climate' has a very similar meaning to safety culture. Put simply, the term safety culture is used to describe behavioural aspects (what people do), and the situational aspects of the company (what the company has). The term safety climate is used to refer to how people feel about safety in the organisation (HSG48, Safety culture Human Factors Briefing Note No 7⁷⁷).

12 When implementing guidance on leadership and safety culture for fuel transfer and storage activities, dutyholders should ensure that:

- clear goals and objectives are set, and made visible by leadership throughout the organisation;
- expectations are translated into procedures and practices at all levels;
- these procedures and practices are commensurate with the risk, consequence of failure, and complexity of the operation;
- all hazards are considered when implementing these expectations – personal and process safety, security and environmental;
- the workforce actively participates in the delivery of these expectations;
- all members of the workforce are – and believe they are – treated fairly in terms of their responsibilities, accountabilities, access to leaders, rewards and benefits;
- there is open communication and consultation across all levels of the organisation;
- relevant metrics are set and performance assessed at appropriate intervals to determine the effectiveness of leadership across the organisation;
- lessons from incidents/near misses are shared across the organisation.

13 When the organisation uses the services of others these additional requirements should be used, commensurate to the task they perform.

14 The Baker Panel Report includes a questionnaire used for a process safety culture survey, ie it is about process safety, and not personal safety, and could be adapted as required for a review of safety culture/climate.

15 The CSB Investigation Report includes an analysis of safety culture, in relation to the Texas City explosion, and recommendations for improvement.

16 *Reducing error and influencing behaviour* HSG48 summarises the organisational factors associated with a health and safety culture, and proposes a step-by-step approach to improving this culture.

17 HSE's Human Factors Toolkit Briefing Note 7 is a concise briefing note providing a useful summary of the characteristics of a healthy safety culture.

18 *Leadership for the major hazard industries* INDG277⁷⁸ provides very useful guidance for executive directors and other senior managers reporting to board members. It is divided into four sections:

- Health and safety culture.
- Leadership by example.
- Systems.
- Workforce.

Each section consists of brief key points followed by more detailed explanation, to refresh knowledge of effective health and safety leadership and to challenge continuous improvement of health and safety performance.

19 HSE's Research Report RR367⁷⁹ provides a review of safety culture and safety climate literature. It is a comprehensive research report that highlights key aspects of a good safety culture, as outlined below:

- **Leadership:** Key criteria of successful leadership, to promote a positive safety culture, are:
 - giving safety a high priority in the organisation's business objectives;
 - high visibility of management's commitment to safety;
 - effective safety management systems.
- **Communication:** A positive safety culture requires effective channels for top-down, bottom-up and horizontal communications on safety matters.
- **Involvement of staff:** Active employee participation is a positive step towards controlling hazards. In particular:
 - ownership for safety, particularly with provision of safety training;
 - safety specialists should play an advisory or supporting role;
 - it should be easy to report safety concerns;
 - feedback mechanisms should be in place to inform staff about any decisions that are likely to affect them.
- **A learning culture:** A learning culture, vital to the success of the safety culture within an organisation:
 - enables organisations to identify, learn and change unsafe conditions;
 - enables in-depth analysis of incidents and near misses with the sharing of feedback and lessons;
 - requires involvement at all levels.
- **A just and open culture:** Companies or organisations with a blame culture over-emphasise individual blame for human error at the expense of correcting defective systems:
 - organisations should move from a blame culture to a just culture;
 - those investigating incidents should have a good understanding of the mechanism for human error;

- management should demonstrate care and concern for employees;
- employees should feel that they are able to report issues or concerns without fear of blame or possible discipline.

20 *Involving employees in health and safety* HSG217⁸⁰ provides more detailed guidance on employee involvement.

Summary

21 Dutyholders should ensure that their executive management provides effective leadership of process safety to develop a positive, open, fair and trusting process safety culture. A review of the characteristics of their leadership and process safety culture should be carried out. The review should:

- be owned at a senior level within the company;
- be developed as appropriate for each site;
- apply to all parties operating at each site;
- lead to the development of action plans to ensure that a positive process safety culture is developed and maintained.

Process safety management

22 Process safety management involves a particular type of risk management – identifying and controlling the hazards arising from process activities, such as the prevention of leaks, spills, equipment malfunctions, over-pressures, excessive temperatures, corrosion, metal fatigue, and other similar conditions. Process safety programs focus on, among other things, the design and engineering of facilities; hazard assessments; management of change; inspection, testing and maintenance of equipment; effective alarms; effective process control; procedures; training of personnel; and human factors.

23 One of the recommendations of the Baker Panel Report following the Texas City Refinery explosion was that BP should establish and implement an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces and manages process safety risks at its US refineries. The CSB Investigation Report made similar recommendations. These recommendations are equally applicable to sites with Buncefield-type potential.

Guidance

24 The Center for Chemical Process Safety (CCPS) of the American Institution of Chemical Engineers (AIChE) guidance *Guidelines for risk based process safety*⁸¹ identifies good practice on process safety management. It is structured as follows:

- Commit to process safety:
 - process safety culture;
 - compliance with standards;
 - process safety competency;
 - workforce involvement;
 - stakeholder outreach.
- Understand hazards and risk:
 - process knowledge management;
 - hazard identification and risk analysis.
- Manage risks:
 - operating procedures;
 - safe work practices;
 - asset integrity and reliability;
 - contractor management;
 - training and performance assurance;

- management of change;
- operational readiness;
- conduct of operations;
- emergency management.
- Learn from experience:
 - incident investigation;
 - measurement and metrics;
 - auditing;
 - management review and continuous improvement;
 - implementation (of a risk-based process safety management system).

25 The HSE internal document *Process safety management systems*⁹² also identifies principles of process safety management. Although intended for process safety management of offshore installations, many of the principles are equally applicable onshore. Key points are:

- There is no single ‘correct’ model of a process safety management system; some companies have separate safety management systems for different sites, whereas others may adopt a more functional approach.
- Some companies give greater emphasis than others to corporate procedures. Each should adopt arrangements that are appropriate for its business and culture.
- In principle, different standards and procedures could be used within each of the sites or functions. In practice, however, systems need to be developed within the constraints of the corporate SMS, and there will inevitably be areas of overlap.
- There is no legal requirement for a company to have a policy statement that is specific to process safety management, but it is recognised good practice, and helps to define the management requirements.
- A good policy statement, or supporting documentation, would indicate the organization’s approach to process safety management. This would include commitment to matters such as:
 - principles of inherent safety;
 - a coherent approach to hazard and risk management;
 - communication of the hazard and risk management process;
 - ensuring competence, and adequacy of resources;
 - recognition of the role of human failure – particularly unintentional human failure – on process safety;
 - assurance that the reliability of process safety barriers that depend on human behaviour and performance are adequately assessed;
 - working within a defined safe operating envelope;
 - careful control of changes that could impact on process safety;
 - maintaining up to date documentation;
 - maintenance and verification of safety critical systems;
 - line management monitoring of safety critical systems and procedures;
 - setting of process safety performance indicators;
 - independent audits of management and technical arrangements;
 - investigation and analysis of incidents to establish root causes;
 - reviewing process safety performance on a regular (eg annual) basis;
 - continuous improvement, with regularly updated improvement plans;
 - principles of quality management, eg ISO 9000.

26 The COMAH Regulations require dutyholders to set out a Major Accident Prevention Policy (MAPP). This would be the logical place to record policies relating to process safety management. Dutyholders also need to ensure that they have effective arrangements to implement each element of the policy.

Summary

27 Dutyholders should ensure they have implemented an integrated and comprehensive management system that systematically and continuously identifies, reduces and manages process safety risks, including risk of human failure.

Hazard identification, layers of protection, and assessment of their effectiveness

28 Prior to the Buncefield incident, the *Safety Report Assessment Guide (SRAG) for highly flammable liquids*⁸³ implied that, unless there were clear areas of confinement or congestion, vapour cloud explosions (VCEs) could be ignored from detailed analysis. The current uncertainty regarding the explosion mechanism at Buncefield suggests that such an approach may no longer be valid. The SRAG has therefore been amended accordingly.

29 Developing process safety performance indicators involves identifying the risk control systems in place for each scenario, and determining which of these are important to prevent or control the various challenges to integrity (HSG254 *Developing process safety indicators*). It is therefore essential to be able to provide an overview of:

- the barriers to major accidents (ie layers of protection);
- what can go wrong; and
- risk control systems in place to control these risks.

30 Various techniques are in use within the industry to give an overview of the layers of protection and evaluate their effectiveness. There is an opportunity to extend good practice within the industry.

Guidance on the hazards of unconfined vapour cloud explosions

31 The safety report should deal with unconfined VCEs by recognising that such events can happen following major loss of containment events, and should be dealt with by demonstration that the measures to prevent, control and mitigate such loss of containment events are of sufficiently high integrity.

32 Until the Buncefield explosion mechanism is known, it is not appropriate for safety reports to contain detailed assessment or quantification of the risks from VCEs. However, estimates of extent and severity should be included. HSE guidance SPC/Permissioning/11 has been amended to include assumptions to be used, in terms of over-pressure at distances from 250 to 400 metres, for estimating the 'extent' information. Initial safety reports, five-yearly updates, and reports that are currently being assessed but have not yet gone through the 'request for further information' stage, should be updated in the light of this current guidance.

Guidance on hazard identification and risk assessment

33 One of the principles of a MAPP is that the dutyholder should develop and implement procedures to systematically identify and evaluate hazards arising from their activities (in both normal and abnormal conditions) (L111). These procedures should address human factors with the same rigour as engineering and technical issues, and should be described in the SMS. There should also be systematic procedures for the definition of measures to prevent major accidents and mitigate their consequences.

34 Techniques used within the industry to help make decisions about the measures necessary include:

- bow-tie diagrams;
- layer of protection analysis;
- fault/event trees;
- tabular records of the hierarchy of control measures.

Bow-tie diagrams

35 A bow-tie diagram is a means of representing the causes and consequences of a hazardous occurrence, together with the elements in place to prevent or mitigate the event. The 'knot' in the middle of the bow-tie represents the hazardous event itself. Such an event might be 'Loss of containment' or 'Storage tank overflow' etc.

36 There may be a number of 'causes' that may lead to this event (eg human error, corrosion) and these are each listed on the left-hand side of the diagram. For each 'cause', safety elements that will serve to prevent or reduce the likelihood of the event are represented as 'barriers'. These 'barriers' may be physical (eg cathodic protection system to prevent corrosion) or procedural (eg speed limits).

37 If the event does occur, it is likely that there will be a number of possible 'outcomes' (eg fire, explosion, toxic effects, and environmental damage). These 'outcomes' are represented on the right-hand side of the diagram. As with the 'causes', safety elements serving to mitigate the effect of the hazardous event and prevent the 'outcome' are listed for each 'outcome'. Again, these may be hardware (eg bunding, foam pourers) or procedural (eg ignition control, spill response).

38 Bow-tie diagrams have a number of advantages. They:

- provide a visual representation of causes/outcomes/barriers;
- are easily understood and absorbed;
- may be developed in a workshop setting similar to a HAZID;
- may be used to rank outcomes using a risk matrix;
- help identify 'causes' with inadequate barriers.

39 Bow-tie diagrams can be used as a stand-alone qualitative hazard identification tool or as the first step in a quantified risk assessment. Depending on the software used, the data on a bow-tie diagram may be output as a hazard register and responsibilities for ensuring that barriers are effective may be assigned.

Layer of protection analysis (LOPA)

40 In the last ten years or so, LOPA has emerged as a simplified form of quantitative risk assessment. LOPA is a semi-quantitative tool for analysing and assessing risk. This analytical procedure looks at the safeguards on a process plant to evaluate the adequacy of the existing or proposed layers of protection against known hazards. It typically builds on the information developed during a qualitative hazard evaluation, such as a process hazard analysis (PHA) and can be used to meet the risk assessment requirements of IEC 61508 and 61511. Significant scenarios are identified and frequencies are estimated for the worst-case events. Risk categories are assigned to determine the number of independent protection layers (IPLs) that should be in place. For a measure to be an IPL it should be both independent and auditable.

ARAMIS

41 A project funded by the European Commission on Accidental Risk Assessment Methodology for Industries (ARAMIS), in the context of the Seveso II Directive, has recently been completed. The project aimed to develop a harmonised risk-assessment methodology, to evaluate the risk level of industrial establishments, by taking into account the accident-prevention tools (safety devices and safety management) implemented by the operators.

42 The user guide to ARAMIS is available online at <http://mahbsrv3.jrc.it/aramis/home.html>, and has the following major steps:

- methodology for identification of major accident hazards (MIMAH);
- identification of safety barriers and assessment of their performances;
- evaluation of safety management efficiency to barrier reliability;
- identification of reference accident scenarios;
- assessment and mapping of the risk severity of reference scenarios;
- evaluation and mapping of the vulnerability of the plant's surroundings.

43 MIMAH is a standardised systematic approach for the identification of hazards. MIMAH is complementary to existing methods, such as HAZOP, FMEA, checklists etc and ensures a better exhaustiveness in terms of hazard- and safety-barrier identification. Bow-ties are the basis of MIMAH methodology in ARAMIS. LOPA is a means of assessing the performance of the safety barriers.

44 The evaluation of the SMS efficiency is based on:

- (a) the identification of the safety barriers in the technical system;
- (b) the assessment of the SMS using an audit; and
- (c) an assessment of safety culture using questionnaires.

The results from (b) and (c) are processed and modify the nominal reliability of the safety barriers, thereby linking the quality of the SMS with the quality of the barrier.

Summary

45 Dutyholders should ensure that they have suitable techniques to demonstrate and assess their layers of protection for prevention and mitigation of major accident scenarios.

46 Dutyholders should update their COMAH safety reports in the light of current guidance on extent and severity, and to describe the process for identification and assessment of control measures.

Roles, responsibilities and competence

47 Clear understanding and definition of roles and responsibilities, and assurance of competence in those roles, are essential to achieve high reliability organisations for the control of major accident hazards.

48 The final Buncefield MIIB Report⁸⁴ makes a specific recommendation for the sector to prepare guidance for understanding and defining the roles and responsibilities of control room operators (including in automated systems) in ensuring safe transfer operations. It also makes a recommendation regarding supervision and monitoring of control room staff.

49 Problems have also been found, in the past, with competence assessment in the UK hazardous industries sector. A review of practices in 2003 indicated that there was a wide variation in standards (RR086⁸⁵). In some cases companies had developed systematic approaches, and made explicit links to the COMAH risk assessment. Others relied on unstructured on-the-job reviews.

50 Elsewhere, the gas plant explosion in Longford, Australia (Lessons from Longford⁸⁶) is an example of a major incident in which organisational changes and a lack of skills or knowledge led to errors that contributed to the incident.

51 Organisational changes such as multi-skilling, layering or downsizing, in which staff are expected to take on a wider range of responsibilities with less supervision, increase the need to assure competence.

52 Dutyholders have a responsibility to ensure their medical (including mental) and physical fitness standards are suitable for the risks involved (see Human Factors Briefing Note No 7 Training and competence⁸⁷). Fitness may be impaired through, for example, drink, drugs or fatigue.

Guidance on roles and responsibilities

53 COMAH guidance L111 identifies a range of personnel for which the roles, responsibilities, accountability, authority, and interrelation of personnel should be identified. They include all those involved in managing, performing or verifying work in the management of major hazards, including contractors.

54 To help specify the roles and responsibilities of control room operators, dutyholders should identify the tasks they carry out. For fuel transfer operations, control room operation at a receiving site typically involves:

- interfacing with the planning function (shortly before transfer of a parcel of product);
- agreement in writing for the transfer into specified tanks (the Consignment Transfer Agreement, which is discussed in paragraphs 193–206);
- preparation for the transfer into the specified tanks;
- direct verbal confirmation, to a specified protocol or procedure, of key details of the transfer, and of readiness to start the transfer;
- execution of start-up and transfer;
- confirming to the sender that product is going into the correct tank(s);
- monitoring of the transfer, including stock reconciliation at set periods, through manual checks or automated systems as appropriate;
- handling any disturbances, and taking correct action in response to alarms;
- implementing contingency arrangements for abnormal occurrences;
- communication with the sender when critical stages are approaching, such as running tank changes, or when there are abnormal circumstances or trips;
- communicating with the sender regarding significant changes that may occur during transfer, and recording those changes;
- providing effective communication at shift handover (if applicable);
- ensuring a safe shutdown at the end of transfer, and confirming to the sender that movement has stopped;
- communicating/agreeing transfer quantities with the sender;
- conducting/arranging analysis as appropriate.

55 In practice, those involved in fuel transfers may also have other responsibilities, not specifically related to fuel transfer, for example: preparation for maintenance, issuing permits to work, conducting plant checks, security monitoring etc.

56 Organisational arrangements for the transfer of fuel vary considerably from site to site. The provision of dedicated control room staff, or a combined control room and field operating function, is likely to depend on the scale and complexity of the plant, as is the provision and level of supervision. In the storage industry (which is normally only involved with storage and transfers) it is generally the case that operations are controlled in the field rather than from a control room. Some receiving sites are unstaffed and controlled from the sending site.

57 However, whatever the make-up of the operating function, the precise roles and responsibilities of those involved in it need to be clearly defined, either in job descriptions or elsewhere. It is essential for the identification of training needs, and assurance of competence, that this should cover each of the above-mentioned phases of fuel transfer operations.

58 Industry guidance on human–computer interfaces (HCIs) (*Process plant control desks utilising human-computer interfaces*⁸⁸) and alarm systems (EEMUA 191 *A guide to design, management and procurement*) also discusses the role of the control room operator, and notes how this has changed as control systems have developed. This is discussed in ‘Information and system interfaces for front-line staff’ of this appendix.

59 The main source of guidance on supervision is *Successful health and safety management* HSG65.⁸⁹ This establishes the importance of supervision, stating that adequate supervision complements the provision of information, instruction and training to ensure that the health and safety policy of an organisation is effectively implemented and developed. Good supervision regimes can form a powerful part of a proper system of management control. It is for the dutyholder to decide on the appropriate level of supervision for particular tasks. The level depends on the risks involved as well as the competence of employees to identify and handle them, but some supervision of fully competent individuals should always be provided to ensure that standards are being met consistently.

60 Organisation of supervision arrangements should ensure:

- an appropriate span-of-control;
- that supervisors are accessible and have the time to actively supervise (ie they are not overloaded with administration and meetings);
- that supervisors have appropriate inter-personal skills and competence to be effective in the supervisory role.

61 Dutyholders should monitor risk control systems. HSG65 is clear that organisations need to decide how to allocate responsibilities for monitoring at different levels in the organisation, and what level of detail is appropriate. Managers and supervisors responsible for direct implementation of standards should monitor compliance in detail. Further guidance on monitoring with regard to fuel transfer is given in 'Measuring Process Safety Performance', paragraphs 260–284.

Guidance on competence

62 HSE Briefing Notes No 2,⁹⁰ CTI⁹¹ and Energy Institute Briefing Note No 7 provide useful summaries of requirements for competence management. They specifically identify the need to link the competence assurance process to control of major accident hazards.

63 Competence is a combination of practical and thinking skills, experience and knowledge. It means the ability to undertake responsibilities and to perform activities to a recognised standard on a regular basis.

64 Training and development seek to create a level of competence for the individual or team, sufficient to allow individuals or teams to undertake the operation at a basic level. Over time, as practical experience grows, operations can be carried out at a more complex level. Training is required not just for normal operation but also for abnormal/upset and emergency conditions etc.

65 Training alone is not sufficient. Dutyholders need to recognise the difference between merely recording a person's experience and training, and assessing their competence (see RR086).

66 The purpose of a competence management system is to control, in a logical and integrated manner, a cycle of activities that will assure competent performance. The aim is to ensure that individuals are clear about the performance expected of them, that they have received appropriate training, development and assessment, and that they maintain or improve their competence over time.

67 A key issue is to make sure that on-the-job training is sufficiently well structured, and that the training and assessment is by competent people. In practice this relies heavily on the quality of the procedures for safety-critical tasks. A key piece of evidence for this would be a well-structured plan for training and assessment. ('Guidance on procedures for control' and monitoring of fuel transfer' is included in this appendix).

68 Ongoing assurance of competency (eg through refresher training), is also important, as is validation of the understanding of the training provided.

69 The Office of Rail Regulation (ORR) guide *Developing and Maintaining Staff Competence*⁹² is a particularly useful text on competence management. (This supersedes HSE's HSG197, which had the same title.) It was written for the rail industry, but it is equally applicable to many other industries. The competence management system (CMS) described consists of 15 principles linked under five phases, as follows:

- Establishing the requirements of the CMS.
- Designing the CMS.
- Implementing the CMS.
- Maintaining competence.
- Audit and review of the CMS.

70 The guidance on maintaining competence includes requirements for monitoring, and reassessing, the performance of staff to ensure performance is being consistently maintained and developed. Guidance is also given on updating of the competence of individuals in response to relevant changes.

71 The integrity of the competence management system will only be maintained if it is regularly checked against the design, and improvements made when needed. Some form of verification and audit of the system should be undertaken. Verification should support the assessors, check the quality of the competence assessments at a location and individual level, including the competence of the managers operating the system, and ensure the assessment process remains fit for purpose. Audit should inspect the whole competence management system and judge compliance against the defined quality assurance procedures.

72 The ORR guide can be used from any point in the cycle for improving existing systems, or for setting up and implementing new competence management systems. It describes:

- the principles and factors that should be considered in any CMS;
- how to ensure that the competence of individuals and teams satisfy the requirements of existing legislation;
- guidance and responsibilities relating to medical and physical fitness.

73 Appendix 1 of the ORR guide defines what is meant by fitness. It provides an outline of fitness assessments, and of the roles of those involved in the process (eg the responsible doctor). These principles are similarly applicable here.

74 The ORR guide refers to the need for directors and senior managers responsible for the overall policy of the company to be aware of the general objectives and benefits that may result from the use of the guidance. However, implementation is more likely to be successful if directors and senior managers are more than just 'aware', but demonstrate commitment to the process.

75 A key issue for dutyholders to consider is the competence of staff in relation to the control of major accident hazards, and how this is identified, assessed and managed. Major accident hazard competency needs to be appropriately linked to the major accident hazard and risk analysis and key procedures. The aim is to assure competence in safety critical tasks, and associated roles and responsibilities.

76 Competency in major accident hazard prevention is necessary at all levels in the organisation, not just the front line. There should be standards set for competency at all levels, and these should be process/job specific.

77 The research report *Competence Assessment for the Major Hazard Industries* RR086 is also a very useful reference for COMAH sites. This aims to provide:

- an authoritative view of what comprises good practice in the field of competence assessment in relation to control of major accident hazards; and
- a model of good practice.

78 The National or Scottish Vocational Qualification (NVQ/SVQ) system can provide some general and some site-specific competencies, but they are not usually linked to major accident hazards. Dutyholders of COMAH sites need to adjust their systems to make this link.

79 Cogent, in conjunction with the petroleum industry, has developed National Occupational Standards (NOS) for:

- Bulk Liquid Operations (Level 2); and
- Downstream Field Operations (Level 3);
- Downstream Control Room Operations.

80 Draft documents have been produced describing job profiles (duties and responsibilities), and proposed requirements for Gold Standard Qualifications.

81 A further job role for operational planning, titled 'Products Movements Scheduler', has also been developed.

82 The Level 2 Bulk Liquid Operations NVQ has been used at several fuel storage terminals in the UK. It is used for field operations, and consists of the following units:

- Monitor and maintain equipment and infrastructure.
- Prepare pipelines and hoses.
- Control the transfer of bulk liquid products.
- Provide product control information.
- Establish and maintain effective working relationships.
- Contribute to the safety of bulk liquid operations.
- Cleaning measurement and test equipment.
- Clean and clear bulk liquid storage tanks
- Package bulk liquid products.

83 In respect of fuel transfer operations, the following Level 2 units are applicable to the various stages of product transfer:

- Pre-receipt activities:
 - Notification processes:
 - Unit 3 Control the transfer of bulk liquid products.
 - Unit 5 Establish and maintain effective working relationships.
 - Stock reconciliation activities:
 - Unit 4 Provide product control information.
 - Sampling.
 - Tank dipping/gauging.
- Pre-receipt operational activities:
 - Unit 2 Prepare pipelines and hoses:
 - Rig lines and set valves on pipelines.
 - Unit 3 Control the transfer of bulk liquid products.
 - Unit 6 Contribute to the safety of bulk liquid operations.
- Initial receipt:
 - Unit 2 Prepare pipelines and hoses:
 - Fill pipelines with product.
 - Unit 3 Control the transfer of bulk liquid products.
 - Unit 6 Contribute to the safety of bulk liquid operations.
- During receipt:
 - Unit 3 Control the transfer of bulk liquid product
 - Unit 6 Contribute to the safety of bulk liquid operations
- Post receipt:
 - Unit 2 Prepare pipelines and hoses:
 - Displace pipeline and hose contents.
 - Unit 3 Contribute to the control of bulk liquid products.
 - Unit 4 Provide product control Information.
 - Unit 6 Contribute to the safety of bulk liquid operations.

84 The Level 3 Downstream Field and Control Room Operations S/NVQs have not been extensively applied in fuel storage terminals but, if applied correctly, these National Occupational Standards could be equally well applied to control room (automatic control systems) or field operations (manual control systems and/or a mix of the two control systems).

85 The Level 3 S/NVQ consists of the following units:

- Contribute to the safety of processing equipment.
- Respond to incidents, hazardous conditions, and emergencies.
- Work effectively as a team.
- Start-up equipment.
- Monitor and maintain process and equipment conditions.
- Handle non-routine information on plant condition.
- Shut down equipment.
- Prepare for maintenance.
- Carry out maintenance within agreed scope of authority.
- Provide samples for analysis.
- Analyse samples.
- Provide on-plant instruction.

86 These new versions of the Level 3 standards, adapted from the previous (2005) Refinery Control Operations and Refinery Field NOS, are awaiting approval by the scheme's regulator, but are unlikely to change significantly.

87 Importantly, the schemes (Level 2 or Level 3) define the key performance criteria required to safely perform the task of receiving bulk liquid product into storage, and can therefore be used as effective gap analysis tools when considering individual companies' management systems and training provisions.

88 In the Level 3 NOS, the link to major accident hazards should be made in Unit 6 (Handling non-routine plant information) and Unit 2 (Response to incidents, hazardous conditions and emergencies).

89 The Cogent standards are quoted as an example of a system that has been adopted by the industry (at Level 2 at least), and generally been found suitable.

90 Although this report gives considerable prominence to the S/NVQ option, it is recognised that there may well be other competence assurance systems, including in-house systems that are also effective.

Summary

91 Dutyholders should ensure that they have:

- clearly identified the roles and responsibilities of all those involved in managing, performing, or verifying work in the management of major hazards, including contractors;
- in particular, defined the roles and responsibilities of control room operators (including in automated systems) in ensuring safe fuel transfer operations;
- defined the roles and responsibilities of managers and supervisors in monitoring safety-critical aspects of fuel transfer operations.

92 Dutyholders should ensure that they have implemented a competence management system, linked to major accident risk assessment, to ensure that anyone whose work impacts on the control of major accident hazards is competent to do so.

Staffing, shift work arrangements, and working conditions

93 Staffing, shift work arrangements and working conditions are critical to the prevention, control and mitigation of major accident hazards.

94 Inadequate staffing arrangements were a factor in the explosion at Longford, Australia in 1998. Some high hazard organisations in the UK were setting staffing levels based on steady-state operations.

95 Staffing levels should be sufficient to react effectively to foreseeable events and emergencies. Dutyholders should be able to demonstrate that there are sufficient alert, competent personnel to deal with both normal operation and hazardous scenarios arising from abnormal events. Contract Research Report CRR 348/2001⁹³ was commissioned by the HSE to provide a method to demonstrate that staffing arrangements are adequate for hazardous scenarios as well as normal operations.

96 Fatigue has been cited as a factor in numerous major accidents including Three Mile Island in 1979, Bhopal in 1984, Challenger Space Shuttle in 1986, Clapham Junction in 1988, Exxon Valdez in 1989, and Texas City in 2005 (HSG256,⁹⁴ the US Chemical Safety and Hazard Investigation Board's *Investigation Report, Refinery Explosion and Fire*⁹⁵). Sleepiness is also thought to be the cause of one in five accidents on major roads in the UK with shift workers being second after young men for risk ('Vehicle accidents related to sleep'⁹⁶). Shift work arrangements, and working conditions, should be such that the risks from fatigue are minimised.

Guidance on safe staffing arrangements

97 CRR 348/2001 gives a practical method for assessing the safety of staffing arrangements and is supplemented by a user guide: *Safe Staffing Arrangements – User Guide for CRR 348/2001 Methodology*.⁹⁷ Other methodologies could also be used, provided they are robust.

98 The CRR 348/2001 method provides a framework for dutyholders to assess the safety of their staffing arrangements with focus on assessing the staffing arrangements for capability to detect, diagnose and recover major accident scenarios. It is a facilitated team based approach taking several days for each study and using control room and field operators as team members.

99 The method has three key elements:

- definition of representative scenarios (preparation for study);
- physical assessment of the ability of staff to handle each scenario by working through eight decision trees for each scenario (approximately two hours per scenario);
- benchmarking of 11 organisational factors using 'ladders' – this is a general assessment by the team and not scenario based (approximately one hour per ladder).

100 Note that both CRR 348/2001 and associated User Guide are required for the method since the Guide gives an additional benchmarking ladder for assessing automated plant/equipment.

101 The effectiveness of the method is dependent on selecting a suitably experienced and competent team. The User Guide gives guidance on the team including suggested membership:

- facilitator (familiar with the method);
- scribe;
- three experienced operators (including control room and field operators);
- management, shift supervisors and technical specialists as required on a part-time basis.

102 The basis for the method can be found in HSG48 as an assessment of individual, job and organisational factors. The physical assessment using the eight decision trees for each scenario focus on job factors:

- Decision trees 1–3 assess the capability of the operators to detect a hazardous scenario eg is the control room continuously manned?
- Decision trees 4 and 5 assess the capability of the operators to diagnose a hazardous scenario.
- Decision trees 6–8 assess the capability of the operators to recover a hazardous scenario including assessment of communications.

103 The general benchmarking uses the team to make judgements of performance against a series of graded descriptions (ladders) on 11 factors including:

- situational awareness (workload);
- alertness and fatigue (workload);
- training and development (knowledge and skills);
- roles and responsibilities (knowledge and skills);
- willingness to initiate major hazard recovery (knowledge and skills);
- management of operating procedures (organisational factors);
- automated plant and/or equipment (added by User Guide).

Guidance on safe shift work arrangements

104 An overview is given in Note 10 of HSEs *Human Factors Toolkit*.⁹⁸ More comprehensive guidance is given in *Managing shift work* HSG256, and in the oil and gas industry guide *Managing Fatigue in the Workplace*.⁹⁹

105 The introduction to *Managing shift work* HSG256 outlines the aim of the guidance to improve safety and reduce ill health by:

- making employers aware of their duty under law to assess any risks associated with shift work;
- improving understanding of shift work and its impact on health and safety;
- providing advice on risk assessment, design of shift work schedules and the shift work environment;
- suggesting measures... to reduce the negative impact of shift work;
- reducing fatigue, poor performance, errors and accidents by enabling employers to control, manage and monitor the risks of shift work.

106 The main principle of the Health and Safety at Work Act is that those who create risk from work activity are responsible for the protection of workers and the public from any consequences. Generically, the risk arising from fatigue derives from the probability of sleepiness and the increased probability of error.

107 Consistent with this and *Successful health and safety management* HSG65, HSG256 details a systematic approach to assessing and managing the risks associated with shift work under the following five headings:

- **Consider the risks of shift work and the benefits of effective management.** For example, fatigue particularly affects vigilance and monitoring tasks particularly on night shifts.
- **Establish systems to manage the risks of shift work.** The need for senior management commitment is highlighted.
- **Assess the risks associated with shift work in your workplace.**
- **Take action to reduce these risks.** The guidance includes a number of useful tables giving non-sector specific examples of factors relating to the design of shift work schedules, the physical environment and management issues such as supervision.
- **Check and review your shift-work arrangements regularly.** Includes suggested performance measures such as the HSE Fatigue and Risk Index Tool¹⁰⁰ and Epworth sleepiness scale.

108 HSG256 is a comprehensive and practical guide with appendices covering a summary of legal requirements and practical advice for shift workers along with a listing of assessment tools such as the HSE Fatigue and Risk Index Tool. HSG256 should be supplemented by any sector-specific guidance, eg the Energy Institute's *Improving alertness through effective fatigue management*,¹⁰¹ or the oil and gas industry guide *Managing Fatigue Risks in the Workplace*.

109 *Managing fatigue risks in the workplace* is intended primarily as a tool to assist oil and gas industry supervisors and occupational health practitioners to understand, recognise and manage

fatigue in the workplace. It sets out to: explain the health and safety risk posed by fatigue; provide the necessary background information on sleep and the body clock; and describe the main causes of fatigue and provide strategies for managing the causes.

110 Implementation of a fatigue management plan (FMP) in accordance with established guidance is recommended. *Managing fatigue in the workplace* describes an FMP as a framework designed to maintain, and when possible enhance safety, performance, and productivity, and manage the risk of fatigue in the workplace. FMPs typically contain the components of:

- policy (including a requirement for auditing processes);
- training (to help identify signs and symptoms of fatigue, and to adopt coping strategies);
- tracking incidents/metrics; and
- support (including medical and wellbeing support).

111 Monitoring of actual shifts worked and overtime, on an individual basis, is a key practical point for dutyholders and managers.

Control room working conditions

112 Control room issues should focus on ensuring operators (both individually and as teams) can develop, maintain and communicate shared situation awareness.

113 It is well established that shift work and fatigue may affect safety (eg HSG48, HSG256) and failure to provide suitable and sufficient breaks is a contributory factor. Guidance on rest and meal breaks is given in HSG256, which states that frequent short breaks can reduce fatigue, improve productivity and may reduce the risk of errors and accidents, especially when the work is demanding or monotonous.

114 Breaks are better taken away from the immediate workplace ie in this case, away from the control room and the immediate work station(s). It is recognised that there may need to be some flexibility in doing this, but the flexibility should not override the principle of allowing adequate rest and meal breaks away from the job.

115 EEMUA 201 notes that the overall environment of the control room can also contribute heavily to the effectiveness of control room staff. This includes, for example:

- different users of the control room;
- dividing into primary and secondary users;
- considering the needs of each set of users;
- ensuring there is no conflict between users;
- controlling access;
- environment;
- blast resistance;
- lighting;
- heating and ventilation;
- noise levels;
- furnishings and colour schemes;
- console design;
- many factors to take into account (see EEMUA 201# for detail);
- safety requirements;
- fire prevention, control and emergency exits;
- other operational support requirements;
- meeting room/office facilities;
- PCs (if not incorporated into the console).

Summary

116 Dutyholders should ensure they can demonstrate that staffing arrangements are adequate to detect, diagnose and recover any reasonably credible hazardous scenario.

117 Dutyholders should develop a fatigue management plan, to ensure that shift work is adequately managed to control risks arising from fatigue.

118 Dutyholders should review working conditions, in particular for control room staff, and develop a plan.

Shift handover

119 Transfer of volatile fuels into storage frequently continues across shift changes, and there is little doubt that unreliable communications about plant or transfer status at shift change could potentially contribute to a tank overflow. It has been a contributory factor in several previous major accidents, including Piper Alpha, Longford and Texas City.

120 *Reducing error and influencing behaviour* HSG48 discusses how unreliable communications can result from a variety of problems. It identifies some high-risk communication situations, and some simple steps that can be used to improve communications in the workplace.

121 HSE's Safety Alert review of oil/fuel storage sites in early 2006 indicated that many sites had structured shift handover formats in place, but some relied on event-type logs or unstructured logs that did not clearly specify the type of information that needed to be communicated.

122 The minimum provision is a handover procedure that specifies simple and unambiguous steps for effective communications at shift and crew change. These include carefully specifying what information needs to be communicated, using structured easy-to-read logs or computer displays, ensuring key information is transmitted both verbally and in writing, and encouraging two-way communication.

Guidance

123 The handover procedure should be based on the principles described in HSG48 or similar guidance available via the HSE website in *Human factors: Safety critical communications*.¹⁰² It should:

- carefully specify what key information needs to be communicated at shift and crew change, at key positions in the organisation. The requirements may well be different for different positions, but should consider issues such as:
 - product movements, both ongoing and planned;
 - control systems bypassed;
 - equipment not working or out of commission;
 - maintenance and permitry;
 - isolations in force;
 - trips defeated;
 - critical or high priority alarms activated and actions taken;
 - health, safety or environment incidents or events;
 - modifications;
 - personnel on site;
- use suitable aids, such as logs, computer displays etc to provide a structured handover of key information, while aiming to cut out unnecessary information;
- capture key information that needs to be carried forward across successive shifts (eg equipment out of service);
- allow sufficient time for handover, including preparation time;
- ensure that key information is transmitted both verbally and in writing;
- encourage face-to-face, and two-way communication, with the recipient asking for confirmation, repetition, clarification etc. as appropriate;
- specify ways to develop the communication skills of employees.

124 The procedure should take account of situations that are known to be especially liable to problems, including:

- during maintenance, if the work continues over a shift change;
- during deviations from normal working;
- following a lengthy absence from work (either as a result of a regular long shift break, or individual absence);
- handovers between experienced and inexperienced staff.

125 Techniques that have been reported from the industry, and that dutyholders may wish to consider in development of their procedures, include:

- use of electronic logs, with password systems for acceptance;
- systems to project electronic logs onto a screen (for team briefing);
- use of team briefings, eg with staggered shift changes between supervisors and operators;
- use of pre-printed paper logs in a structured format;
- use of white boards for recording systems that may be out of service for several shifts.

126 Dutyholders must have the facilities and management arrangements necessary to ensure that the procedures set are indeed complied with. These include:

- arrangements to minimise distractions during handover;
- instruction and training of employees in handover procedures;
- supervision, audit and review to ensure that the procedure is complied with and the necessary information is communicated and understood.

127 Safety-critical tasks, such as commencement of fuel transfer, tank changeover, and end of transfer, should generally be scheduled to avoid shift handover times.

Summary

128 Dutyholders should set and implement arrangements for effective and safe communication at shift and crew change handover.

129 Top-tier COMAH sites should include a summary of the arrangements for effective and safe communication at shift and crew change handover in the next revision of the safety report.

Organisational change and management of contractors

130 Effective management of change, including organisational change as well as changes to plant and processes, is vital to the control of major accident hazards. This section deals with organisational change, particularly change involving contracting out of core business activities. Management of changes to plant and processes is discussed in 'Management of plant and process changes' within this appendix.

131 Organisational changes that can adversely affect the management of major hazards include various types of internal restructuring, re-allocation of responsibilities, changes to key personnel, and contractorisation.

132 Failure to manage organisational change adequately was found to be a factor in major accidents at Castleford in 1992 and at Longford, Australia in 1998.

133 In high-hazard industries policies regarding use of contractors or outsourcing need to be clear. If safety-critical work is to be contracted out then the company should ensure that it remains an 'intelligent customer'. In other words, it should retain adequate technical competence to judge whether, and ensure that, work is done to the required quality and safety.

Guidance

134 *A guide to the Control of Major Accident Hazard Regulations 1999* L111 summarises the range of changes, including changes to people and the organisation, which should be subject to management of change control procedures.

135 HSE's Information Sheet *Organisational change and major accident hazards* CHIS7¹⁰³ sets out a framework for managing organisational changes, and is recommended for high-hazard industries.

136 *Principles for the assessment of a licensee's intelligent customer capability*¹⁰⁴ and *Contractorisation*¹⁰⁵ are documents used internally by HSE's Nuclear Directorate to assess and inspect contractorisation and intelligent customer issues.

137 *Managing contractors* HSG159¹⁰⁶ is a guide for employers in managing contractors in the chemical industry.

138 *The use of contractors in the maintenance of the mainline railway infrastructure*¹⁰⁷ is an HSC review of contractorisation in the railways (primarily) and other high hazard industries, including nuclear, offshore, and onshore chemicals.

139 *Health and safety management systems interfacing*¹⁰⁸ provides a methodology for interfacing/integrating safety management systems between clients and contractors.

140 Information about the Client Contractor National Safety Group Safety Passport scheme can be found online at www.ccmsg.com.

Organisational change

141 CHIS7 describes the types of organisational change that can affect the management of major accident hazards. These include:

- business process engineering;
- de-layering;
- introduction of self-managed teams;
- multi-skilling;
- outsourcing/contractorisation;
- mergers, demergers and acquisitions;
- downsizing;
- changes to key personnel;
- centralisation or dispersion of functions;
- changes to communication systems or reporting relationships.

142 The main focus of CHIS7 is on changes at operational and site level and it is specifically about major accident prevention. It sets out a three-step framework for managing change, as follows:

- Step 1 – Getting organised for change.
- Step 2 – Assessing risks.
- Step 3 – Implementing and monitoring the change.

Contractorisation, and intelligent customer capability

143 A principle, well known within the nuclear industry, is that dutyholders should maintain the capability within their own organisations to understand, and take responsibility for, the major hazard safety implications of their activities. This includes understanding the Safety Case for their plant and the limits under which it must be operated. It is known as 'intelligent customer capability'. (See *Principles for the assessment of a licensee's intelligent customer capability* and *Contractorisation*.)

144 As an intelligent customer (in the nuclear industry), the management of the facility should know what is required, should fully understand the need for a contractor's services, should specify requirements, should supervise the work and should technically review the output before, during and after implementation. The concept of intelligent customer relates to the attributes of an organisation rather than the capabilities of individual post holders. (See *Principles for the assessment of a licensee's intelligent customer capability*.)

145 CHIS7 extends this principle more widely to high hazard industries, stating that, if you contract out safety-critical work, you need to remain an 'intelligent customer'.

146 An organisation that does not have intelligent customer capability runs the risk of:

- not understanding its safety report, and operating unsafely;
- not having appropriate staff to adequately deal with emergencies;
- procuring poor safety advice, or wrongly implementing advice received;
- not recognising that significant plant degradation or safety critical events are arising, or not addressing them correctly;
- not identifying the requirements for safety-critical projects, modifications or maintenance, or carrying them out inadequately;
- employing inadequate contractors or agency staff.

147 A dutyholder who proposes to contract out should have organisational change arrangements in place to review the proposal and demonstrate that safety will not be jeopardised. Choices between sourcing work in-house or from contractors should be informed by a clear policy that takes due account of the potential major accident implications of those choices. The approach to identifying and managing core competencies and sustaining an intelligent customer capability should be set out in the safety management system.

148 The guidance (*Principles for the assessment of a licensee's intelligent customer capability and Contractorisation*) makes no reference to the concept of 'contracting-in' an intelligent customer resource eg for the evaluation of other contractors. Wherever practicable, this resource should be in-house.

149 *Managing contractors* HSG159 is aimed at small to medium sized chemicals businesses. It primarily focuses on ensuring safe working practices of contractors when on site to do specific jobs. A weakness of this guidance is that it does not deal specifically with the principle of contracting out of core business on major hazard sites, or of intelligent customer capability. However, it does contain a checklist to help dutyholders to gain an overview of health and safety in managing contractors, and this contains statements that would infer some requirement for intelligent customer capability, such as:

- staff know their responsibilities for managing contractors on site;
- staff responsible have enough knowledge about the risks and preventative measures for all jobs involving contractors; and
- staff responsible know what to look for when checking that contractors are working safely, and know what action to take if they find problems.

150 A report by the Health and Safety Commission (HSC) in 2002 into the use of contractors in the maintenance of the mainline railway infrastructure came to the conclusion that:

- contractorisation is a feature of all industrial sectors worldwide;
- it is entirely possible to run a safe operation using contractors so long as management systems are good; and
- it is not invariably true that an in-house operation is better managed.

151 There are now well-established principles for good contractor management that, if followed, will provide the basis for safe operation. Dutyholders cannot contract out their responsibilities and must accept that they are responsible for taking appropriate steps to ensure the overall safety of the operation.

152 This report also reviewed contractorisation in other high-hazard industries, including nuclear, offshore, and onshore chemicals.

153 A national passport scheme (the Client Contractor National Safety Group Safety Passport – www.ccnsg.com) is used widely to provide levels of assurance of the quality of contractor staff against a broad health and safety framework, rather than for specific contractor disciplines.

Retention of corporate memory

154 The dutyholder also needs to have adequate arrangements for retention of corporate memory. *Principles for the assessment of a licensee's intelligent customer capability* discusses requirements for retention of corporate memory in the context of the nuclear industry, and CHIS7 briefly refers to it in the wider context of organisational change and major accident hazards.

155 The most common circumstances under which the loss of corporate memory could occur are:

- Staff turnover: The accumulated knowledge of the experienced staff, which is often extensive, can be lost when knowledge is not transferred from the outgoing to the incoming staff.
- Unavailability of information: This occurs when information is not recorded, or not archived appropriately, or when information is not provided through pre-job briefing. Of particular importance is the availability of the as-built design knowledge that changes over the life of the facility.
- Ineffective use or application of knowledge: Despite the existence of information within the organisation, individuals may not be aware or may not understand they had access to information.

To counter the above, dutyholders should develop succession plans to respond to situations involving staff movements and have in place formal arrangements for knowledge archiving and transfer of information.

Management systems interfacing

156 HSG159 includes a checklist of items (organised under the headings of: Policies; Organising; Planning and implementing; Monitoring; Reviewing and learning) to give an overview of a client's arrangements for managing contractors.

157 This checklist deals with relevant elements of an SMS that need to be considered when engaging contractors. It doesn't deal specifically with how the SMS of the client might interface with that of the contractor, but it is a useful starting point.

158 On major hazard sites, the more the contractor becomes involved with managing core business activities of the site, the more important it becomes for formal interfacing/integration of the SMS of the client with that of the contractor.

159 *Principles for the assessment of a licensee's intelligent customer capability* states that 'where complex management arrangements and several dutyholders contribute to complying with the requirements, HSE will usually expect a dutyholder to describe the arrangements for 'interfacing' with others'. However, it provides no further guidance on how this might be done.

160 The UK offshore industry has developed guidance for interfacing health and safety management systems between dutyholders involved in shared activities. The guidance deals with all the elements of an SMS including issues such as:

- identifying minimum training needs and competencies;
- identifying responsibilities for training and competence;

- agreement of criteria and mechanisms for handling changes;
- responsibility for hazard identification and risk assessment of changes;
- identifying key safety performance indicators.

161 The extent to which the guidance needs to be applied is a function of the risk associated with the shared activities. Thus, before developing SMS interfacing arrangements, a risk assessment must be undertaken by the parties involved. This may be a simple matter of making a judgement about the degree of hazard and duration of activity.

162 It would seem to be potentially useful (with minor tailoring) for onshore application, particularly where a significant element of core business activity is contracted out (eg maintenance).

Summary

163 Dutyholders should ensure that there is a suitable policy and procedure for managing organisational changes.

164 Dutyholders should ensure that there is a suitable policy and procedure for retention of corporate memory.

165 Dutyholders should ensure that they retain adequate technical competence and 'intelligent customer' capability when work impacting on the control of major accident hazards is outsourced or contractorised.

166 Dutyholders should ensure that suitable arrangements are in place for management and monitoring of contractor activities.

167 Dutyholders should ensure that in addition to retaining intelligent customer capability, they consider using industry guidance for interfacing safety management systems where core business is contracted out.

168 HSE should consider reviewing its guidance *Managing contractors* HSG159 to ensure that it is appropriate for major hazard sites and consistent with other relevant guidance (eg CHIS7) in terms of requirements to maintain 'intelligent customer' capability. Guidance on SMS interfacing between clients and contractors should also be considered.

Management of plant and process changes

169 Experience (for example the Flixborough disaster in 1974) has shown management of change (MOC) to be an essential factor in the prevention and control of major accidents. This section discusses plant and process changes. Management of organisational change is discussed under 'Organisational change and management of contractors' in this appendix.

170 Dutyholders should adopt and implement management procedures for planning and control of all changes in plant, processes and process variables, materials, equipment, procedures, software, design or external circumstances which are capable of affecting the control of major accident hazards.

171 This approach should cover permanent, temporary, and urgent operational changes, including control of overrides/inhibits, as well as changes to the management arrangements themselves (see L111).

Guidance

172 *Guide to the COMAH Regulations* L111 summarises the range of changes that should be subject to management of change control procedures.

173 Each site should have guidance to help its personnel to determine the difference between like-for-like replacement and a change. This should cover items such as:

- valves;
- piping and flanges;
- vessels/tanks;
- rotating machinery;
- instrumentation;
- software;
- process materials;
- operational changes;
- maintenance procedures;
- purchasing changes;
- equipment relocation.

174 As part of its commitment to process safety leadership, UKPIA has developed guidance and a self assessment tool for MOC.¹⁰⁹ This provides a means by which organisations can assess themselves against a common framework of excellence in process safety. It is specifically intended for UKPIA members at their refinery and fuel storage facilities in the UK but is available to non-UKPIA members involved in the fuel transfer and storage business.

175 MOC processes which align to current good practice may be further improved using the UKPIA self-assessment tool, which provides a suitable methodology for advancing an organisation's MOC processes to achieve excellence in process safety.

176 The self-assessment tool is divided into five phases, as follows:

- **Phase 1 – Definition and scope:** The purpose of this phase is to determine if the MOC process has been robustly developed to address each category of change, and the roles and responsibilities of each person involved in the change.
- **Phase 2 – Types of change:** This phase is to determine if all the potential types of change have been identified, and that any specific requirements for dealing with these changes have been addressed. It covers the range of changes described above (including organisational change as well as plant and process changes).
- **Phase 3 – Key steps:** This phase is to determine if the MOC process has a clearly defined structure and workflow and, where appropriate, controls in place to ensure that each change is raised, reviewed, approved, implemented, verified, and closed in accordance with a documented procedure.
- **Phase 4 – Audit:** This phase is to determine if audits take place at appropriate intervals, against defined criteria, and that auditing reviews the status of corrective actions. It also considers any changes that have been made without engaging MOC.
- **Phase 5 – Metrics, training and improvement plans:** This phase is to review the strategy for measuring the performance of MOC, through key performance indicators and, where necessary, implementing improvements to the process.

177 The self-assessment tool uses a scoring system for each item examined, with scores ranging from 0 (Awareness building, where practice is essentially non-existent or ad-hoc) to 4 (Optimising, where an effective and efficient system is in place). A weighting is applied to each of the items before aggregating into an overall score.

Summary

178 Dutyholders should ensure they have suitable guidance for their staff about what constitutes a plant or process change, and that they have suitable arrangements in place for management of the range of permanent, temporary, and urgent operational changes.

Principles for safe management of fuel transfer

179 The Initial Report¹¹⁰ of the Buncefield MIIB identified an issue with regard to safety arrangements, including communications, for fuel transfer. No authoritative guidance was found that adequately describes these principles. To address this, the set of principles for safe management of fuel transfer were developed. These include the adoption of principles for consignment transfer agreements.

Guidance

180 These guiding principles should be developed into specific procedures and protocols by all organisations involved in the transfer of fuel to ensure that at all times the operation is carried out in a safe and responsible manner without loss of containment.

181 All parties involved in the transfer of fuel must ensure that:

- responsibility for the management of the safe transfer of fuel is clearly delineated;
- there are suitable systems and controls in place to adequately manage the safe transfer of fuel commensurate with the frequency and complexity of the operation;
- there is clear accountability and understanding of all tasks necessary for the transfer operation;
- there are sufficient, adequately rested, competent persons to safely execute all stages of the operation;
- shift handover procedures comply with latest available industry guidance.
- receiving site operators:
 - positively confirm that they can safely receive the fuel before transfer commences;
 - positively confirm that they are able to initiate emergency shutdown of the fuel transfer;
- there is clear understanding of what events will initiate an emergency shutdown of the fuel transfer operation;
- as a minimum the following information is communicated between all relevant parties prior to commencing fuel transfer:
 - grade/type;
 - consignment size (including common understanding of units used);
 - flow rate profiles (significant (all parties to agree what constitutes a 'significant' change for their operation) unplanned changes in flow rate during the transfer should be communicated);
 - start time;
 - estimated completion time;
 - any critical operations/periods when transfer could adversely affect other operations (eg slow load requirements, roof on legs);
- there is an appropriate degree of integrity in the method of communication (eg telephone, radio, facsimile, e-mail, common server) with positive confirmation of all critical exchanges;
- there is an agreed process to communicate changes to the plan in a timely manner;
- there is clearly understood nomenclature;
- key performance indicators are in place to monitor and review performance.

Checklist of job factors for safe fuel transfer

182 The following checklist comprises a set of job factors identified in a review of the various safety-critical stages in fuel transfer operations: it is intended for use as an aide-memoire in reviews of systems and procedures.

Planning tools

- Provision of clear information on short-term and long-term outages of plant or instrumentation.
- Provision of job aids for calculating availability, eg when filling multiple tanks.
- Provision of equipment to allow effective communication between all parties.
- Provision of user-friendly plans to communicate and agree plans between planners/senders and receivers.
- Good planning tools to predict end of transfer.

Site facilities

- Clear information on expected and actual flows and rates.
- Clear displays of levels/ullages.
- Manageable alarm and information systems – good practice applied in design.
- Clear labelling of plant and equipment, in the field and in the control room.
- Labelling systems to avoid confusing tanks, pipes and pumps.
- Adequate lighting.
- Facilities/arrangements to minimise distractions at shift handover.
- Reliable equipment, eg valves that work.
- Adequate maintenance of facilities.

Job design

- Jobs designed to keep operators motivated.
- Operators not overloaded/distracted from responding.

Information, instructions and procedures

- Clear, unambiguous, user-friendly information and diagrams of plant.
- Instructions/job aids for line setting allowing operators to see clearly all valves needing to be checked.
- Procedures for non-routine settings.
- Procedures to transfer product from sender to receiver.
- Procedures for verification that the correct movement has begun.
- Arrangements to identify unauthorised line movement.
- Procedures for monitoring flow and fill.
- Clear unambiguous displays of levels/alarms and plant status.
- Clear instructions to take on alarm.
- Procedures for changeover.
- Feedback to confirm correct operation of valves.
- Check lists for complex, infrequently used, or critical systems.
- Contingency procedures for abnormal situations.
- Ability to recover current or established settings after a system crash.

Emergency response systems and procedures

- Emergency procedures taking account of power/air failures, fires/explosions and floods.
- Systems for emergency shutdown.
- Reliable communication links, including inter-site links.
- Emergency control centre with adequate equipment and information aids.
- Criteria for activating emergency response plans.
- Suitable means of raising the alarm, onsite and offsite.
- Efficient call-out system (eg automated phone system, duty rota).
- Suitable PPE.
- Suitable muster areas, including safe havens, and equipment.
- Suitable means of detection, including patrols, CCTV, gas detection.
- Suitable isolations.
- Clear identification and labelling of plant.
- Suitable site access arrangements.
- Planning for recovery after an event.

Summary

183 Dutyholders involved in the transfer and storage of fuel should adopt good practice principles for safe management of fuel transfer.

184 Dutyholders involved in the transfer and storage of fuel should review 'job factors' to facilitate safe fuel transfer.

Operational planning for fuel transfer by pipeline

185 Human factors issues are important at various safety-critical stages in fuel transfer operations including operational planning.

Guidance

186 Operational planning takes into account all stages of the plan development and approval, up to the stage of implementation via the consignment note.

187 The planning process will generally not be triggered by a request for a delivery of fuel by the receiving site; such a plan will generally be contract-driven and involve many parties.

Job factors

188 Job factors for effective planning include:

- provision of a clear stock control policy, eg maximum and minimum working levels, maximum flow rates, maximum number of parcels, strategic stock levels, workable contractual rules, tank throughput per year etc;
- clear communication protocols between planning/sender and receiver (eg the consignment transfer agreement);
- effective tools to communicate receiver plant information to planners (INPUT);
- effective tools/programmes to communicate plans to receivers (OUTPUT);
- reliability of equipment and systems;
- availability of suitable planning procedures;
- jobs designed to keep staff motivated;
- flexibility in the planning arrangements.

Person factors

189 Person factors include the following characteristics, skills and competencies:

- understanding of the site;
- numeracy;
- communication skills (including command of English and IT systems);
- negotiation skills;
- ability to work under pressure and multi-task;
- job interest/motivation.

Organisational factors

190 Factors important to organisational success include:

- the safety culture of all parties involved;
- use of suitable stock control policies;
- provision of adequate resources to cover all modes eg absence of key staff, out-of-hours issues, changes to plan, emergencies;
- defining clear roles and responsibilities, and providing adequate supervision;
- defining clear communication channels between sender and receiver;
- identifying potential conflicts, and providing mechanisms to resolve them;
- ensuring staff (eg shift team members) are not fatigued and have a manageable work load;
- empowering people to stop imports if necessary.

Note: As discussed under 'Roles, responsibilities and competence', Cogent, in conjunction with the industry, is currently developing job profiles and standards for competence assurance of products movements schedulers.

Assurance factors

191 Factors important to assuring overall success include:

- setting key performance indicators for deviations from plan (eg hitting the high level alarm, number of stock outs, number of in-line amendments, highest level etc);
- investigation of incidents and near misses arising from planning failures, and sharing the lessons across all parties;
- ensuring there is a mechanism for feedback from the receiver to the sender on the quality of operational plans;
- including the examination of operating practice against the policy and procedure as part of audit arrangements.

Summary

192 Dutyholders that are receivers of fuel should develop procedures for successful planning and review them with their senders and all appropriate intermediates. The stages to be considered in the planning process should include:

- contract strategy for deliveries of fuel (long-term planning process);
- development and agreement of monthly movement plans;
- amendments to monthly plans;
- development of weekly and daily operational plans;
- amendments to weekly and daily operational plans;
- 'in line' amendments.

Principles for consignment transfer agreements

193 The Initial Report of the Buncefield MIIB identified an issue with regard to safety arrangements, including communications, for fuel transfer. To address this, a set of principles was developed for safe management of fuel transfer, as detailed in paragraphs 179–184. These include the adoption of principles for consignment transfer agreements, as described below.

Guidance

194 The following principles apply to pipeline transfers where separate parties control:

- the supply of material to a tank or tanks; and
- the tank or tanks.

This includes, for example, transfers between sites belonging to one business. It does not apply to transfers where a single person or team controls both 'ends' of the transfer, although an equivalent standard of control is necessary.

195 For the purposes of these agreements the sender is the party primarily responsible for the final transfer of fuel to the receiving terminal.

196 For transfers from ships into tanks, the current edition of the *International Safety Guide for Oil Tankers and Terminals (ISGOTT)* is considered to be the appropriate standard.

197 The agreement involves three stages:

- *Stage 1:* a common written description of what is to be transferred.
- *Stage 2:* direct verbal confirmation (eg by telephone landline) to a specified protocol or procedure, of:
 - key details of the transfer from the written material; and
 - the decision to ‘start’ by the receiver.An analogy is flight control, where there is a written flight plan, but permission to ‘take off’ is always verbally confirmed by the control tower.
- *Stage 3:* a procedure for handling significant change during a transfer

Stage 1: Agreed description of transfer

198 Agreed in writing, between sender and receiver, as close as practicable to Stage 2 (for example, during the current or previous shift).

199 The common written description of the transfer should, so far as possible, be kept free of clutter; for example, it should not generally include a significant amount of product quality data. It should include (but not necessarily in this order):

- nominated batch number (schedules/sequential);
- product grade/type (in agreed terms);
- density (if required to enable conversion of volume to weight and vice versa);
- amount to be transferred, stating units;
- expected rate of transfer, including initial rate, steady cruise rate, and changes during plan;
- date and expected time of start (note: should include the need to agree verbally);
- estimated completion time;
- notes regarding abnormal conditions that may affect product transfer and mitigations in place, including risk assessment;
- name of sender (named individual);
- name of receiver (named individual);
- other responsibilities for involvement in the transfer and receipt process, as agreed locally;
- arrangements for receipt terminal to stop the flow in the event of an emergency;
- target tank/s for receipt.

200 Receiving terminal to sign draft consignment (after considering any abnormal conditions) and return to sending terminal to provide confirmation that product can be safely received.

Stage 2: Verbal confirmation and decision to receive

201 Following consignment agreement a verbal agreement should be made, confirming details on the consignment note and the receiver giving permission to start. This should include confirmation of:

- batch number(s) being ready;
- the product grade/type and quantity, including a check of units;
- no significant changes to the written agreement that may affect safe receipt;
- receiving party ready to receive.

Stage 3: Procedure for handling significant change

202 Significant changes should be communicated between sender and receiver, and recorded by both parties.

203 The appropriate party should also record actions taken.

Summary

204 Dutyholders involved in the transfer of fuel by pipeline should develop consignment transfer agreement procedures consistent with good practice principles.

205 Dutyholders involved in inter-business transfer of fuel by pipeline should agree on the nomenclature to be used for their product types.

206 Dutyholders receiving ship transfers should, for each relevant terminal, carry out a review to ensure compliance with the current edition of the *International Safety Guide for Oil Tankers and Terminals (ISGOTT)*.

Procedures for control and monitoring of fuel transfer

207 Procedural problems are frequently cited as the cause of major accidents, contributing to some of the world's worst incidents, such as Bhopal, Piper Alpha and Clapham Junction. In the major hazard industries, fit-for-purpose procedures are essential to minimise errors, and to protect against loss of operating knowledge (eg when experienced personnel leave).

Guidance on written procedures

208 Procedures are agreed safe ways of doing things. Written procedures usually consist of step-by-step instructions, and related information, to help carry out tasks safely. They may include checklists, decision aids, diagrams, flow-charts and other types of job aids. They are not always paper documents, and may appear as 'on screen' help in control system displays.

209 Procedures should be robust, followed in practice and audited: otherwise, input values in risk assessments (eg human reliability input data to LOPA studies for safety critical equipment) may be invalidated.

210 *Revitalising procedures*¹¹¹ provides guidance for employers responsible for major hazards on how to develop procedures that are appropriate, fit-for-purpose, accurate, 'owned' by the workforce and, most of all, useful. It is commended as a source of good practice, describing:

- the linkage between procedural problems and major accidents;
- what procedures are, and why they are needed;
- procedural violations, and why people do not always follow them;
- how to encourage compliance with procedures;
- different types of procedures;
- involvement of procedure users;
- where procedures fit into risk control;
- links between training, competency and procedures;
- a three-step approach to improving procedures;
- review of procedures;
- presentation – formatting and layout (including use of warnings to explain what happens if...).

Guidance on procedures for fuel transfer by pipeline

211 Procedures should be consistent with the sections of this appendix 'Principles for safe management of fuel transfer' (paragraphs 179–184) and 'Principles for consignment transfer agreements' (paragraphs 193–206).

212 The **sender's** procedures should specify:

- the minimum communications required, including:
 - confirmation of start of movement;
 - deviations from plan;
- the correct sequence of operations to avoid over-pressure or surge;
- arrangements to monitor flow (based on risk assessment);
- circumstances where transfer must stop, eg:
 - no confirmation is received of tank changeover when expected;
 - when the agreed parcel has been sent.

213 The **receiver's** written instructions should cover all key phases of its operations, including:

- preparation and start-up;
- monitoring the transfer and stock reconciliation, including response to alarms if required;
- tank changeover;
- closing/shutting down;
- routine checks;
- contingencies for abnormal occurrences.

Further details of the requirements for each phase are given below.

Preparation and start-up

214 This requires an effective means of communication between sender and receiver, which should be achieved by means of a **consignment transfer agreement**.

215 In addition the receiver should have written procedures in place to ensure that the necessary preparatory checks and line setting are carried out effectively. These procedures should specify clearly defined routings for all standard transfers, including alignment of valves etc **except** when risk assessment determines that this is not necessary, taking consideration of the complexity, frequency and criticality of the task.

216 If a non-standard routing is to be used there should be a clear, detailed specification of the required route.

Monitoring and reconciliation, including response to alarms

217 Procedures for monitoring and reconciliation should include initial verification that the fuel movement phase is as expected, by initial dip/telemetry as appropriate, after around 15–20 minutes (determined by transfer speed and capacity etc). If 'Yes' this should be confirmed to the consignor/sender.

218 If 'No' it should be treated as an abnormal situation and contingency arrangements should be specified. Robust arrangements, based on a risk assessment of local circumstances, must be made to identify 'unauthorised' movements.

219 There should be continuous verification at **set periods** (within defined tolerances) through manual checks or automated systems as appropriate. Checking at set periods is necessary to check that the 'mental model' is correct or if there has been an unexpected change (eg an unexpected process change, or a measurement error due to a stuck instrument). The set periods and tolerances should be defined and clear to operators, and be derived from risk assessment, taking account of:

- fill and offtake rates;
- capacity;
- degree of automated control of movement;
- potential speed of response;
- planned staffing cover arrangements/if a problem;
- anticipated completion time.

220 Communication requirements must be specified, including the need for the receiver to contact the sender when critical steps are approaching, such as 'running' tank changes or when there are abnormal circumstances or trips.

221 Procedures should specify that all filling operations must be terminated at or before the normal fill level, which should be set sufficiently far below the LAH to avoid spurious activation of the alarm. (In this context alarms do not include alerts for process information).

222 Procedures should also be clear about the response required on LAH and LAHH. If the LAH is reached, then appropriate action should be taken to reduce the level to below the alarm setting in a controlled and timely manner. If the LAHH is reached, immediate action must be taken to terminate the transfer operation and reduce the level to, or below, the normal fill level.

Tank changeover

223 There may well be a plan to change tanks during the transfer. In this situation there should be clear designated routings for the changeover. Procedures must detail arrangements for verification and communication in the period up to an anticipated tank change, again clearly based upon risk assessments of local circumstances. The receiver retains primacy in a decision to cease the transfer at any time.

224 Unless a process risk assessment shows it to be unnecessary, operational procedures should require the receiver to communicate with the sender:

- when changeover is imminent; and
- when the changeover has been completed.

Then go to the monitoring and reconciliation procedure.

Closing/shutting down

225 Procedures should detail the actions to take to ensure safe isolation, and to prevent damage to plant and equipment, after completion of the transfer. They should require the receiver to confirm to the sender that movement has stopped.

Routine plant checks

226 All tank farms should ensure that there is a physical site check, to define routes or activities, which can pick up sounds, odours etc. that may indicate a problem. All parts of the tank farm should be inspected at an adequate frequency (eg 2 x per day and 2 x per night) with guidance on what to look for (eg source of ignition, breaches in containment, leaks, unattended machinery, security breaks etc). This, together with any anomalies found and actions taken should be recorded.

227 Operators of normally unstaffed installations should consider, through an assessment of risks, how they would carry out routine plant checks, record and act on the findings

Contingencies for abnormal occurrences

228 For each phase of the operation credible abnormal occurrences should be identified, such as:

- loss of critical equipment;
- unable to use receipt tank or swing tank valves;
- incapacity or unavailability of staff;
- unable to contact key personnel etc.

229 Written instructions, based on an assessment of risks, should give clear guidance for staff on the action to take to take to mitigate such occurrences.

Summary

230 Dutyholders should ensure that written procedures are in place, and consistent with current good practice, for safety-critical operating activities in the transfer and storage of fuel.

231 The above notes on 'Procedures for fuel transfer by pipeline' provide further information on the scope and standards expected of the review, which should be conducted against *Revitalising procedures* or similarly effective guidance.

Information and system interfaces for front-line staff

232 Control room design and ergonomics, as well as effective alarm systems, are vital to allow front line staff, particularly control room operators, to reliably detect, diagnose, and respond to potential incidents. They should comply with recognised good practice appropriate to the scale of the operation.

Guidance on human-computer interfaces

233 In the past, most control rooms consisted of hard-wired equipment laid out on large metal panels and desks, which required the operator to patrol the panels, monitoring key plant variables, adjusting set-points and operating equipment. These have now commonly been replaced by computer screen based ('soft-desk') systems, through which the operator both views the plant and operates it. In the majority of such cases there is no hard-wired facility at all. This is known as a human-computer interface (HCI) (or human-system interface (HSI)).

234 In the fuel transfer and storage industry, there is a range of equipment still found, from hard-wired panel-based equipment with a high degree of manual control, to computer-screen based control systems with a high degree of automatic control. Refineries typically have computer-screen based systems. However, most tank storage terminals do not, and the majority of control actions are still carried out by the operator.

235 EEMUA 201 discusses the changing nature of control centres, and how these changes have affected the role of the control room operator. It is the primary and authoritative industry guide to HCIs, and is intended to help those involved in the design, procurement, operation, management and maintenance of these systems. It includes material derived from cooperation with the US-based Abnormal Situation Management Consortium (ASM). ASM publications should be consulted where further information is required.

236 HCIs provide the vital means by which the operator obtains information on the state of the plant, enters operational data, and by which any automatic control action can be overridden and manual control of the plant be taken.

237 As plants have become more automated, the automatic system, rather than the operator, performs the majority of the control actions. The operator tends to have a more reactive role, devoting more time to analysing potential problems or dealing with shortfalls in performance. Major intervention by the operator is only required when the plant moves away from its normal operating parameters.

238 Therefore a modern HCI is required to perform satisfactorily for two very different situations. For most of the time the plant will be operating normally and the HCI must be designed to aid the operator maximise plant efficiency, but when an abnormal situation arises the HCI must aid the operator in returning the plant to normal operation as soon as possible.

239 Design of the system is crucial to the operator's role, including the number of screens, the design of displays, and the means of navigation around the system. The HCI to a process control system is critical in allowing an operator:

- to develop, maintain and use an accurate and up-to-date awareness of the current and likely future state of the process; and
- to interact with the system quickly and efficiently under all plant conditions.

240 To achieve this, the following categories of operation, in order of importance, need to be considered:

- Category 1: Abnormal situation handling, including start-up and shutdown.
- Category 2: Normal operation.
- Category 3: Optimisation.
- Category 4: General information retrieval.

241 Many issues need to be taken into account, ranging from the detailed design of display formats, and the way these formats fit together in the hierarchy, through to the actual desk layout, number of screens, and the overall operational environment. This interface is the nerve centre of the operator's work, and its design is very much a human factors issue.

242 In order to design the HCI it is imperative that the operator's activities are well understood, and all the different operational circumstances considered. EEMUA 201 details a number of steps that should be taken including:

- task analysis, to capture the full remit of the operator's role;
- end-user involvement in the system design;
- ensuring that the number of screens allows for complete access to all the necessary information and controls under all operational circumstances;
- ensuring that the design allows for a permanently viewable plant overview;
- providing continuous access to alarm indications;
- providing the capability to expand the number of screens.

243 The guide provides further advice on issues that have to be considered in taking these steps, including:

- the physical layout and number of screens;
- use of multi-windows;
- use of large screen displays;
- navigational requirements – based on a hierarchy of screens;
- information access;
- management of abnormal situations;
- automation;
- plant size;
- process complexity;
- staffing levels, and multi-unit operation;
- reliability/redundancy/system failure.

244 BS EN ISO 11064¹¹² sets a standard for ergonomic design of control centres. It is divided into seven parts, as follows:

- Part 1: Principles for the design of control centres.
- Part 2: Principles for the arrangement of control suites.
- Part 3: Control room layout.
- Part 4: Layout and dimensions of workstations.
- Part 5: Displays and controls.
- Part 6: Environmental requirements for control centres.
- Part 7: Principles for the evaluation of control centres.

245 In the absence of a more up-to-date company standard, procedure or specification, projects should follow this standard and EEMUA 201 for new control rooms, and they can be usefully referred to for modifications and upgrades to existing ones, especially where there are known problems.

246 Part 1 sets up a generic framework relating to ergonomic and human factors in designing and evaluating control centres, with the view to eliminating or minimising the potential for human errors. It includes requirements and recommendations for a control centre design project in terms of philosophy and process, physical design and design evaluation. It can be applied to the elements of a control room project, such as workstations and overview displays, as well as to the overall planning and design of entire projects.

247 Other parts of BS EN ISO 11064 deal with more detailed requirements, and may be considered as advanced references.

Guidance on alarm systems

248 Management of abnormal situations often concerns the effectiveness of the alarm system. Increased automation provides a relatively calm operating scenario when the plant is in a steady state. However, given the importance of alarms in times of upset, the display of alarm information has to be given high priority. Even if there are relatively few alarms on the system and the system is not a distributed control system (DCS) the same principles apply, to ensure a reliable response to alarms.

249 Dutyholders should proactively monitor control systems, such as the tank gauge system, so that designated level alarms etc do not routinely sound. (This does not exclude the use of properly managed variable alarms or warnings set below the established alarm levels).

250 The Energy Institute's *Alarm handling*,¹¹³ and HSE's *Alarm handling*¹¹⁴ and *Better alarm handling*¹¹⁵ provide useful summaries of alarm handling issues with case studies.

251 EEMUA 191 covers the topic fully, and is referenced as good practice guidance in each of the above summaries. It identifies the following characteristics of a good alarm:

- Relevant: not spurious or of low operational value.
- Unique: not duplicating another alarm.
- Timely: not long before response needed, or too late.
- Prioritised: indicating importance to the operator.
- Understandable: message clear and easy to understand.
- Diagnostic: identifying the problem that has occurred.
- Advisory: indicative of action to be taken.
- Focusing: drawing attention to the most important issues.

252 EEMUA 191 provides a roadmap to direct different users to different parts of the guide, relevant to their particular needs. There are separate roadmaps for:

- where an alarm system is already in operation; and
- where an alarm system is in the conceptual phase.

253 For situations where an alarm system is already in operation, users are provided with guidance on how to review:

- the alarm system philosophy;
- the principles of alarm system design, especially:
 - the design process;
 - generation of alarms;
 - structuring of alarms;
 - designing for operability;
- implementation issues, especially:
 - training;
 - procedures;
 - testing;
- alarm system improvement.

Summary

254 Dutyholders should ensure that their control room information displays, including human-computer interfaces and alarm systems, are reviewed in relation to recognised good industry practice.

255 Where reasonably practicable, dutyholders should put plans in place to upgrade control room information displays, including human-computer interfaces and alarm systems, to recognised good industry practice.

256 Dutyholders should ensure that modifications or development of new control rooms or HCIs comply with recognised industry good practice both in their design, and their development and testing.

Availability of records for periodic review

257 Retention of relevant records is necessary for the periodic review of the effectiveness of control measures, and the root cause analysis of those incidents and near misses that could potentially have developed into a major incident.

Guidance

258 The following records are considered to be particularly relevant:

- Stock records to demonstrate compliance with a stock control policy.
- Operational plans.
- Consignment transfer agreements.
- Local records of changes to consignment transfers.
- Stock reconciliation records.
- Incidences of high level alarm activation.
- Incidences of high-high level/trip activation.
- Maintenance/proof testing for high level trip and alarm systems.
- Faults discovered on high level alarm or protection systems.
- Communications failures between sender and receiver.
- Plant/process changes.
- Organisational changes.
- Approval/operation of inhibits/overrides of safety systems.
- Competence/training records.
- Shift work/overtime records.
- Shift handover records.
- Routine plant tour records.
- Permits to work.
- Risk assessments.
- Method statements.
- Active monitoring records.

Summary

259 Dutyholders should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially develop into a major incident. The records should be retained for a minimum period of one year.

Measuring process safety performance

260 Measuring performance to assess how effectively risks are being controlled is an essential part of a health and safety management system (see L111 and HSG65). **Active monitoring** provides feedback on performance before an accident or incident, whereas **reactive monitoring** involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes.

261 The presence of an effective personal safety management system does not ensure the presence of an effective process safety management system. *The Report of the BP US Refineries Independent Safety Review Panel* (the 'Baker Panel report'), following the Texas City refinery explosion in 2005, found that personal injury rates were not predictive of process safety performance at five US refineries.

262 Used effectively process safety indicators can provide an early warning, before catastrophic failure, that critical controls have deteriorated to an unacceptable level. The use of process safety performance indicators fits between formal, infrequent audits and more frequent inspection and safety observation programmes. It is not a substitute for auditing, but a complementary activity.

263 The main reason for measuring process safety performance is to provide ongoing assurance that risks are being adequately controlled. In order to measure safety performance, many dutyholders have incorporated leading and lagging indicators, also known as 'metrics' or 'key performance indicators', into their safety management systems. Managers use these metrics to track safety performance, to compare or benchmark safety performance.

264 Many organisations rely on auditing to highlight system deterioration. However, audit intervals can be too infrequent to detect rapid change, or the audit may focus on 'compliance', ie verifying that the right systems are in place rather than ensuring that systems are delivering the desired safety outcome (see HSG254).

265 Many organisations do not have good information to show how they are managing major hazard risks. This is because the information gathered tends to be limited to measuring failures, such as incident or near misses. System failures following a major incident frequently surprise senior managers, who believed the controls were functioning as designed (see HSG254).

API RP 754 on process safety performance indicators

266 Recommendation 10 of the MIIB's Design and operations report asks the sector to 'agree with the CA on a system of leading and lagging performance indicators for process safety...in line with HSG254'. This is similar to the US Chemical Safety Board's (CSB's) recommendation post-Texas City asking 'API, ANSI, USW to develop a new consensus ANSI standard which identifies leading and lagging indicators for nationwide public reporting as well as indicators for use at individual facilities. Include methods for the development and use of performance indicators'.

267 Given the multinational nature of the industry there are clear advantages to a common approach internationally, capable of consistent use throughout an international company and across refining, chemical and storage sectors, and it was agreed that on behalf of PSLG, UKPIA should accept API's invitation to participate in the committee to develop the standard, known as RP 754. HSE's guidance HSG254 is well-recognised in the US, and this theme has been further developed in guidelines published by the Centre for Chemical Process Safety in December 2007.

268 The API committee has sought to build on the CCPS guidelines and develop a standard for ballot and completion by end 2009. The model of a 'safety triangle' has been successful in helping improve the management of occupational safety, and the model proposed for process safety involves four tiers – ie significant events, other lesser loss of containment, challenges to safety systems, and management system issues. The lower tiers represent near misses and are likely to be helpful indicators.

Guidance

Active monitoring

Active monitoring is primarily a line management responsibility (see HSG65). It should be distinguished from the requirement for 'independent' audits, which are a separate activity. HSG65 refers to auditing as the structured process of collecting independent information on the efficiency, effectiveness, and reliability of the total health and safety management system, and drawing up plans for corrective action.

269 Active monitoring should include inspections of safety-critical plant, equipment and instrumentation as well as assessment of compliance with training, instructions and safe working practices.

270 Active monitoring gives an organisation feedback on its performance before an incident occurs. It should be seen as a means of reinforcing positive achievement, rather than penalising

failure after the event. It includes monitoring the achievement of specific plans and objectives, the operation of the SMS, and compliance with performance standards. This provides a firm basis for decisions about improvements in risk control and the SMS.

271 Dutyholders need to decide how to allocate responsibilities for monitoring at different levels in the management chain, and what level of detail is appropriate. In general, managers should monitor the achievement of objectives and compliance with standards for which their subordinates are responsible. Managers and supervisors responsible for direct implementation of standards should monitor compliance in detail. Above this immediate level of control, monitoring needs to be more selective, but provide assurance that adequate first line monitoring is taking place.

272 Various forms and levels of active monitoring include:

- examination of work and behaviour;
- systematic examination of premises, plant and equipment by managers, supervisors, safety representatives, or other employees to ensure continued operation of workplace risk precautions;
- the operation of audit systems;
- monitoring of progress towards specific objectives, eg training/competence assurance objectives.

273 Many of these topics are not specific to process integrity, but are equally applicable to all areas. Topics of particular relevance to process integrity include:

- change control;
- process safety study (eg HAZOP or PSA) close out;
- control of process plant protection systems/inhibits etc;
- control of alarms/alarm system status;
- operating procedures, including consignment transfer procedures and stock reconciliation procedures;
- shift handover procedures;
- management of fatigue and shift work;
- maintenance of safety-critical systems;
- control of contractors.

274 They should also include other key systems that are equally relevant to preventing a major incident, such as:

- workplace risk assessments;
- permit to work systems;
- isolation standards;
- controls at high pressure/low pressure interfaces;
- control of relief devices etc.

Reactive monitoring

275 Reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes (see L111 and HSG65). It includes:

- identification and analysis of injuries/causes of ill health;
- identification and analysis of other incidents, near misses, and weaknesses or omissions in performance standards;
- assessing incident/near miss potential;
- investigation and identifying remedial actions to deal with root causes;
- communication of lessons learned;
- tracking of remedial actions arising from incidents/near misses etc;
- contributing to the corporate memory.

Process safety performance indicators

276 HSE guidance *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries* HSG254 outlines six main stages needed to implement a process safety management system. It provides a methodology for leading and lagging indicators to be set in a structured way for each critical risk control system within the process safety management system.

277 OECD has also developed *Guidance on Safety Performance Indicators*¹¹⁶ to assess the success of chemical safety activities.

278 **Leading indicators** are a form of active monitoring focused on a few critical risk control systems to ensure their continued effectiveness. They require a routine systematic check that key actions or activities are undertaken as intended. They can be considered as measures of process or inputs essential to deliver the desired safety outcome.

279 **Lagging indicators** are a form of reactive monitoring requiring the reporting or investigation of specific incidents and events to discover weaknesses in that system. These incidents represent a failure of a significant control system that guards against or limits the consequences of a major incident.

280 **The six key stages** identified in the guidance are:

Stage 1 – Establish the organisational arrangements to implement the indicators

Stage 2 – Decide on the scope of the measurement system; consider what can go wrong and where

Stage 3 – Identify the risk control systems in place to prevent major accidents. Decide on the outcomes for each and set a lagging indicator

Stage 4 – Identify the critical elements of each risk control system (ie those actions or processes that must function correctly to deliver the outcomes) and set leading indicators

Stage 5 – Establish the data collection and reporting system

Stage 6 – Review

Worked example

281 A worked example for developing process safety performance indicators, using HSG254 methodology, for a terminal fed by pipeline and by ship is included as Annex 1 of this appendix.

282 The example identifies potential leading and lagging indicators for challenges to integrity such as:

- over-pressure of ship-to-shore pipework;
- accidental leakage from ship to water;
- bulk tank overfilling (ie above safe operating limits);
- accidental leakage during tanker loading;
- tank subsidence;
- leak from pumps;
- pump/motor overheating;
- corrosion of tanks;
- high pressure in terminal pipework during pipeline delivery;
- static discharge;
- physical damage.

Summary

283 Dutyholders should ensure that a suitable active monitoring programme is in place for key systems and procedures for the control of major accident hazards.

284 Dutyholders should develop an integrated set of leading and lagging performance indicators for effective monitoring of process safety performance.

Investigation of incidents and near misses

285 As technical systems have become more reliable, the focus has turned to human causes of accidents. The reasons for the failure of individuals are usually rooted deeper in the organisation's design, decision-making, and management functions.

286 HSG48 gives several examples of major accidents where failures of people at many levels (ie organisational failures) contributed substantially towards the accidents. Human factors topics of relevance to process integrity include:

- ergonomic design of plant, control and alarm systems;
- style and content of operating procedures;
- management of fatigue and shift work;
- shift/crew change communications; and
- actions intended to establish a positive safety culture, including active monitoring.

287 Investigation procedures should address both immediate and underlying causes, including human factors.

Guidance

288 HSG65 is a suitable reference on investigation of incidents and near misses. Not all events need to be investigated to the same extent or depth. Dutyholders need to assess each event (for example using a simple risk-based approach) to identify where the most benefit can be obtained. The greatest effort should concentrate on the most significant events, as well as those that had the potential to cause widespread or serious injury or loss.

289 HSG65 Appendix 5 describes one approach that may be used as a guide for analysing the immediate and underlying causes of effects. Various other approaches are also available, and widely used within the industry. These include various in-house or proprietary systems.

290 Other suitable references include *Human factors in accident investigations*¹¹⁷ and *Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents*.¹¹⁸

Summary

291 Dutyholders should ensure they have suitable procedures for:

- identifying incident/near miss potential;
- investigating according to the identified potential;
- identifying and addressing both immediate and underlying causes;
- sharing of lessons learned;
- tracking of remedial actions.

Audit and review

292 The terms 'audit' and 'review' are used for two different activities (see L111 and HSG65).

293 In addition to the routine monitoring of performance (ie active monitoring) the dutyholder should carry out periodic audits of the SMS as a normal part of its business activities.

294 An audit is a structured process of collecting independent information on the efficiency, effectiveness, and reliability of the total SMS. It should lead to a plan for corrective action. In this context 'independent' means independent of the line management chain.

295 Reviews are a management responsibility. They need to take account of information generated by the measuring (active and reactive monitoring) and auditing activities, and how to initiate remedial actions.

296 The requirements for audit and review are well established. The main issue is to ensure that process safety is adequately included in audit and review programmes.

Guidance on auditing

297 Auditing provides an independent overview to ensure that appropriate management arrangements (including effective monitoring) are in place, together with adequate risk control systems and workplace precautions.

298 Various methods can achieve this. AIChE guidelines (*Guidelines for auditing process safety management systems*¹¹⁹ and *Guidelines for technical management of chemical process safety*¹²⁰) draw a distinction between process safety auditing, and process safety management systems (PSMS) auditing.

299 The focus of process safety auditing is the identification and evaluation of specific hazards (eg inspecting hardware and finding the absence of a relief device, or an independent trip system). PSMS auditing, however, involves assessment of the management systems that ensure ongoing control (eg the management systems in place to ensure that pressure relief devices have been designed, installed, operated, and maintained in accordance with company standards).

300 Both types of audit are important. The process safety audit addresses a particular hazard found at a specific time. It could lead to correction of the hazard without addressing the underlying reason why the hazardous condition came to exist. The PSMS audit addresses the management systems intended to preclude the creation of hazards.

301 The audit programme should include a selection of range of controls in place for preventing or mitigating the risk of a Buncefield-type scenario. These include, but are not limited to:

- commitment to process safety management;
- application of principles for safe management of fuel transfer;
- risk assessment procedures;
- effectiveness of process safety barriers;
- definition of roles and responsibilities;
- ensuring competence;
- assessment of staffing arrangements;
- management of fatigue associated with shift work;
- safety-critical communications, including shift handover;
- management of organisational change;
- management of contractors;
- retention of intelligent customer capability;
- retention of corporate memory;
- operational planning, and consignment transfer procedures;
- safety-critical operating procedures;
- provision of information;
- document control procedures;
- control of overrides/inhibits of safety-critical instrumentation systems;
- alarm systems;
- inspection and maintenance of safety-critical systems;
- permit to work and isolation arrangements;
- detection measures for loss of containment;
- integrity of secondary and tertiary containment measures;
- control of ignition sources;
- fire protection measures;
- management of plant and process changes;
- maintenance of records;
- active monitoring arrangements;
- reactive monitoring arrangements;

- setting and reviewing of process safety performance indicators;
- investigation procedures/analysis of underlying causes;
- sharing of lessons learned;
- emergency procedures/testing of emergency plans;
- review arrangements/improvement plans.

302 Such audits are formal and infrequent. Dutyholders may decide to audit a small range of activities on a more frequent basis (eg yearly), or a more extensive range on a less frequent basis (eg 3–5 years). The dutyholder should decide the range and scope of its audit programme, taking into account such factors as audits/inspections imposed by others (eg the CA, parent companies or joint venture partners, insurers, trade associations), and the extensiveness of the active monitoring programme.

303 Audits that focus primarily on ‘compliance’ (ie verifying that the right systems are in place rather than ensuring that they deliver the right safety outcome) are not sufficient.

Guidance on review

304 Reviewing should be a continuous process undertaken at different levels in the organisation. An annual review should be the norm, but dutyholders may decide on a system of intermediate reviews at, for example, department level. The result should be specific remedial actions which establish who is responsible for implementation, with deadlines for completion.

305 Issues to be considered in the review process include:

- the major accident prevention policy;
- audit programme achievement and findings;
- active monitoring records and findings;
- process safety performance indicators;
- incident/near miss history;
- relevant lessons from incidents etc elsewhere;
- analysis of root/basic causes of incidents and near misses;
- issues from safety committees;
- tracking of safety actions;
- risk assessment status, including reviews against changing standards.

Summary

306 Dutyholders should adopt and implement audit plans defining:

- the areas and activities to be audited, with a particular focus on process; safety/control of major accident hazards;
- the frequency of audits for each area covered;
- the responsibility for each audit;
- the resources and personnel required for each audit;
- the audit protocols to be used;
- the procedures for reporting audit findings; and
- the follow-up procedures, including responsibilities.

307 Dutyholders should ensure that they have implemented suitable arrangements for a formal review of arrangements for control of major accident hazards, including:

- the areas and activities to be reviewed, with a particular focus on process safety/control of major accident hazards;
- the frequency of review (at various levels of the organisation);
- responsibility for the reviews;
- the resources and personnel required for each review;
- procedures for reporting the review findings; and
- arrangements for developing and progressing improvement plans.

Annex 1 Process safety performance indicators: Example workbook for a fuel storage terminal with pipeline and jetty filling

(Previously published as Appendix 5 of the BSTG report)

308 This is a worked example of process safety performance indicators developed using *Developing process safety performance indicators: A step-by-step guide* HSG254. The steps follow the key steps in HSG254.

Description of the site and activities

309 This example is based on a typical operational terminal with both pipeline and jetty filling. The site boundary at the point of jetty operations was selected – ship and marine activities were out of scope.

310 Fuel products are delivered to site from ships or via cross-country pipeline and loaded into bulk tanks. Product from bulk tanks are loaded onto road tanker for dispatch.

Overview of Steps 2–4

311 The main stages in selecting process safety indicators are:

- Step 2.2: Identify the scope:
 - identify the hazard scenarios which can lead to a major incident;
 - identify the immediate causes of hazard scenarios.
- Step 3: Identify the risk control systems and describe the outcome for each – set a lagging indicator:
 - identify the risk control systems (RCS) in place to prevent or mitigate the effects of the incidents identified;
 - identify the underlying causes;
 - identify outcomes of each RCS;
 - set a lagging indicator for each RCS.
- Step 4: Identify critical elements of each RCS and set a leading indicator:
 - identify the most critical elements of the risk control system and set leading indicators for each element;
 - set a tolerance for each leading indicator;
 - select the most relevant indicators for the site or activities under consideration.

Step 2.2: Identify the scope

Step 2.2.1: Identify the hazard scenarios which can lead to a major incident

312 Describing the main incident scenarios helps to maintain a focus on the most important activities and controls against which indicators should be set. The scenarios form a useful cross-check later on in Step 4 when the critical elements of risk control systems to be measured are determined.

313 For this site the main process safety incident scenarios are loss of containment (LOC) of flammable liquid or liquid fuel dangerous to the environment, particularly to the estuary. These events may lead to:

- a pool fire, vapour cloud ignition, or for gasoline a vapour cloud explosion;
- a major accident to the environment.

Step 2.2.2: Identify the immediate causes of hazard scenarios

314 The immediate cause is the final failure mechanism that gives rise to a loss of containment. These usually can be considered as the factors which challenge the integrity of plant or equipment.

315 For this site immediate causes could be, for example:

- accidental leakage – valve left open, coupling not made correctly;
- flexible hose failure;
- pipeline failure;
- valve, pump, flange, or coupling failure;
- bulk tank failure;
- road tanker failure;
- overfilling.

Step 2.2.3: Identify the primary causes

316 This step is important as it is a prerequisite to deciding which risk control systems are important to prevent or control the challenge to integrity. For this site primary causes could be:

- under pressure;
- lightning strike;
- over-pressure;
- corrosion;
- joint flange gasket aging;
- wrong material;
- physical damage;
- subsidence;
- wrong product;
- wear;
- wrong installation;
- vibration;
- overheating;
- static discharge;
- wrong specification;
- quality of material.

Step 3.1: Identify the associated risk control systems

317 Draw up a risk control matrix as illustrated in Table 15, to help decide which risk control systems are the most important in controlling the challenges to integrity identified within the incident scenarios.

Table 15 Risk control matrix

Risk control systems	Challenges to integrity						
	Overfilling	Accidental leakage	Over-pressure	Corrosion	Wear	Physical damage	Subsidence
Control and instrumentation							
Operational procedures							
Competence							
Inspection and maintenance							
Design							
PTW							
Plant change							
Control of contractors							

Step 3: Identify the outcome and set a lagging indicator

318 It is vital to discuss and agree the reason why each risk control system is in place and what it achieves in terms of the scenarios identified. Without this agreement it will be impossible to measure success in delivering this outcome.

319 It's best to phrase 'success' in terms of a positive outcome – supportive of the safety and business priorities. The indicator can then be set as a positive or negative metric to flag up when this is achieved or when not. As success should be the normal outcome then choosing a negative metric guards against being swamped by data (reporting by exception).

320 The following questions may be helpful:

- Why do we have this risk control system in place?
- What does it deliver in terms of safety?
- What would be the consequence if we didn't have this system in place?

321 The indicator set should be directly linked to the agreed risk control system outcome and should be able to measure a company's success/failure at meeting the outcome.

Step 4: Identify the critical elements of each risk control system and set leading indicators

322 There are too many elements to a risk control system for each to be measured. It is not necessary to monitor every part of a risk control system. Consider the following factors when determining the aspects to cover:

- Which activities or operations must be undertaken correctly on each and every occasion?
- Which aspects of the system are liable to deterioration over time?
- Which activities are undertaken most frequently?

From this the critical elements, of each risk control system important in delivering the outcome, can be identified.

1 Over-pressure ship-to-shore transfer

System outcomes:

- pressure less than 10 bar.

Potential lagging indicators:

- number of times pressure in the line exceeds 10 bar when offloading.

Critical elements of the risk control system:

- valves not closed against ship's pump;
- correct line up;
- ship-to-shore checks done;
- set correct discharge rate (maximum pressure and rate);
- sequence of discharge;
- set up manifold;
- emergency communications;
- radio communications;
- agreed shut down plan in place – signed both parties;
- English speaker on board ship;
- trained/competent discharge crew.

Leading indicators:

- number of times ship is unloaded where the ship-shore checks are not completed correctly;
- number of times when any item is not met by ship calling at a terminal.

2 Ship-to-shore transfer accidental leakage

System outcomes:

- no leaks into water.

Lagging indicators:

- number of times a ship is offloaded where there is a leak to water.

Critical elements of the risk control system:

- ship-to-shore checks completed correctly;
- inspection and maintenance of marine arms;
- trained jetty crew;
- coupling done up correctly/manifold bolted up properly;
- start pump slowly;
- walk the lines;
- lines drained down correctly/stripped.

Potential leading indicators:

- number of times the planned inspection and maintenance of marine arms not done to time;
- number of times the ship-to-shore checks not completed correctly, especially;
- new gaskets used;
- lines walked before discharge commences.

3 Bulk tank overfilling

System outcomes:

- not filled above safe operating limits.

Potential lagging Indicators:

- number of times the tank is filled above the safe operating limits.

Critical elements of the risk control system:

- ullage control checklist/scheduling system;
- tank gauging and associated equipment working;
- competent people undertaking tasks;
- shift handover control;
- supply handover;
- configuration of valves and associated interlocks;
- inspection and maintenance of tank gauging system;
- inspection and maintenance of line product sensors;
- for pipeline deliveries – cross-check and fax confirmation between central operations and terminal operations OCC monitoring tank level independently.

Potential leading indicators:

- number of times ullage checks not done correctly before product transfer begins;
- number of times inspection and maintenance of tank gauging system not carried out to required frequency.

4 Accidental leakage during tanker loading

Outcomes:

- during product transfer no leaks;
- breaking couplings after transfer – not more than 1 litre.

Potential lagging indicators:

- number of times there is a leak of more than 1 litre following product transfer or any leak during the transfer.

Critical elements of the risk control system:

- reliable equipment – couplings and faucet (hours of use and change-out time);
- operator error – stretch, position of vehicles;
- mistreatment;
- maintenance and inspection of vacuum breaker/faucet/coupler;
- truck maintenance;
- maintenance.

Potential leading indicators:

- % of STOP observations on loading bay operations where drivers are not following procedures;
- % failure of truck API inspections.

5 Tank subsidence

Outcomes:

- tank configuration within relevant API or EEMUA;
- any detectable signs of adverse distortion or movement.

Lagging indicator selected:

- number of tanks where there is adverse distortion or movement.

Critical elements of the risk control system:

- inspection and maintenance of tanks;
- appropriate and timely action follow-up;
- independent review of findings.

Leading indicators:

- number of tanks inspected to schedule;
- number of corrective actions completed to time.

6 Leaks from pumps

System outcomes:

- no pump leakage due to seal failure.

Seal failure:

- wear;
- cavitation;
- incorrect installation;
- running dry;
- incorrect material;
- misalignment/vibration.

Potential lagging indicators:

- number of (detectable) leaks from pumps due to seal failure. (Any detectable leak from pump seals, picked up during normal terminal walk-round patrol, to be reported.)

Critical elements of the risk control system:

- correct design of seals for the application;
- correct installation of seals;
- vibration monitoring of pumps;
- correct operation of the pumps – running only with adequate supply.

Potential leading indicators:

- number of product pump vibration checks undertaken to schedule;
- number of remedial actions raised following vibration monitoring not completed.

7 Pump/motor overheating

System outcomes:

- no pump/motor overheating

Potential lagging indicators:

- number of times fire loop activated by overheating of pump/motor;
- number of near misses referring to overheating of pump/motor.

Critical elements of the risk control system:

- correct design of pump/motor for the application;
- correct installation;
- vibration monitoring of pumps;
- correct operation of the pumps – running only with adequate supply.

Potential leading indicators:

- number of product pump vibration checks undertaken to schedule;
- number of remedial actions raised following vibration monitoring not completed.

8 Corrosion of tanks

System outcomes:

- minimum thickness of tanks (wall/floor) left not exceeded due to corrosion.

Potential lagging indicators:

- number of tanks where the minimum thickness of metal has been reached/exceeded during routine inspection.

Critical elements of the risk control system:

- water draw-off;
- effective tank repairs;
- tank inspection as per expected frequency;
- microbial growth management;
- record retention/management;
- coated tanks – damage and necessary repair.

Potential leading indicators:

- number of water draw-offs carried out to schedule;
- number of tanks exceeding the scheduled tank inspection interval.

9 High pressure in terminal pipework during pipeline delivery

System outcomes:

- terminal pipework not exceeding ~5 to ~10 bar during pipeline delivery. (High pressure alarm on SCADA at 12.5 bar – recorded in computerised event log. Can set analogue alarm/indication on terminal control system.)

Potential lagging indicators:

- number of deliveries where terminal pipework pressure exceeded (5 bar) during pipework deliveries.

Critical elements of the risk control system:

- alignment of valves – logic interlock;
- control valves;
- competence of staff;
- maintenance of safety critical instrumentation – surge protection/interlock logic/control valves;
- ‘Station Not Ready’ interlock.

Potential leading indicators:

- number of job observations undertaken of terminal staff carrying out management of pipeline delivery/terminal distribution activities (tell me/show me) undertaken on time (more frequent for newly recruited staff);
- inspection and maintenance of ‘Low MV signal direct’ control loop carried out to schedule.

10 Static discharge

System outcomes:

- no static discharges in tanks or road tankers.

Potential lagging indicators:

- number of static discharges – not detectable.

Critical elements of the risk control system:

- earth permissive system;
- loading procedures – no splash loading;
- incorrect filters installed;
- incorrect design of equipment – tank nozzles/pipework;

- flow rate too high;
- tank earthing system;
- tank dipping equipment and procedures.

Potential leading indicators:

- number of times inspection of system maintenance overdue/shows failures;
- number of times inspection of tank earthing overdue/shows failures;
- number of times job observations (tell me/show me) on tank dipping are completed on time.

11 Physical damage

System outcomes:

- no material physical damage to equipment.

Potential lagging indicators:

- number of incident reports where physical damage has occurred.

Critical elements of the risk control system:

- driver induction and training;
- competence of permanent contractors;
- control of non permanent contractors – induction;
- correct use of work control system;
- protection of ‘at risk’ equipment;
- traffic control system – layout, speed detection.

Potential leading indicators:

- number of near-miss reports where equipment damage is a potential;
- number of drivers not trained as required;
- number of significant work control system deficiencies found.

Table 16 Suite of process safety performance indicators

Challenge to integrity	Lagging indicator	Leading indicator
1 Over-pressure ship-to-shore transfer*	Number of times pressure in the line exceeds 10 bar when offloading	Number of times ship is unloaded where the ship–shore checks are not completed correctly. Number of times when any item is not met by ship calling at a terminal.
2 Ship-to-shore transfer accidental leakage*	Number of times a ship is offloaded where there is a leak to water	Number of times the planned inspection and maintenance of marine arms not done to time. Number of times the ship-to-shore checks not completed correctly.
3 Bulk tank overfilling*	Number of times the tank is filled above the safe operating limits	Number of times ullage checks not done correctly before product transfer begins. Number of times inspection and maintenance of tank gauging system not carried out to required frequency.

Challenge to integrity	Lagging indicator	Leading indicator
4 Accidental leakage during tanker loading*	Number of times there is a leak of more than 1 litre following product transfer or any leak during the transfer	% of STOP observations on loading bay operations where drivers are not following procedures. % failure of truck API inspections.
5 Tank subsidence	Number of tanks where there is adverse distortion or movement	Number of tanks inspected to schedule. Number of corrective actions completed to time.
6 Leaks from pumps*	Number of (detectable) leaks from pumps due to seal failure	Number of product pump vibration checks undertaken to schedule. Number of remedial actions raised following vibration monitoring not completed.
7 Pump/motor overheating*	Number of times fire loop activated by overheating of pump/motor	Number of product pump vibration checks undertaken to schedule. Number of remedial actions raised following vibration monitoring not completed.
8 Corrosion of tanks*	Number of tanks where min thickness of metal is reached/ exceeded at routine inspection	Number of water draw-offs carried out to schedule. Number of tanks exceeding the scheduled tank inspection interval.
9 High pressure in terminal pipework during pipeline delivery	Number of deliveries where terminal pipework pressure exceeded (5 bar) during pipework deliveries	Number of job observations undertaken of terminal staff carrying out management of pipeline delivery/terminal distribution activities (Tell me/Show me) undertaken on time (more frequent for newly recruited staff). Inspection and maintenance of 'Low MV signal direct' control loop carried out to schedule.
10 Static discharge*	Number of static discharges – not detectable	Number of times inspection of system maintenance overdue/ shows failures. Number of times job observations (tell me/show me) on tank dipping are completed on time.
11 Physical damage	Number of incident reports referring to physical damage	Number of drivers not trained as required. Number of significant work control system deficiencies found.

* Denotes the challenges to integrity for which process safety KPIs were selected for monitoring.

Annex 2 Further guidance for human factors practitioners and managers

Control of Major Accident Hazard Regulations 1999

A guide to the Control of Major Accident Hazards Regulations 1999 (as amended). Guidance on Regulations L111 HSE Books 2006 ISBN 978 0 7176 6175 6

The safety report assessment manual Open document under 'Code of Practice on Access to Government Information' HSE www.hse.gov.uk/comah/sram/s2-7.pdf

Major accident prevention policies for lower-tier COMAH establishments Chemical Information Sheet CHIS3 HSE Books 1999 www.hse.gov.uk/pubns/comahind.htm

Assessing Compliance with the Law in Individual Cases and the Use of Good Practice HSE ALARP Suite May 2003 www.hse.gov.uk/risk/theory/alarp2.htm

Health and safety management (general)

Successful health and safety management HSG65 (Second edition) HSE Books 1997
ISBN 978 0 7176 1276 5

Management of health and safety at work. Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and guidance L21 (Second edition) HSE Books 2000
ISBN 978 0 7176 2488 1

Managing health and safety: An open learning book for managers and trainers HSE Books 1997
ISBN 978 0 7176 1153 9 (out of print)

Formula for health and safety: Guidance for small and medium-sized firms in the chemical industry HSG166 HSE Books 1997 ISBN 978 0 7176 0996 3

HID CI / SI Inspection Manual Open document under 'Code of Practice on Access to Government Information' HSE 2001 www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf Chapters on 'Risk Control Systems' including RCS 11 Assessing Auditing on pages 184–187

Process safety management (general)

Guidelines for Risk Based Process Safety Center for Chemical Process Safety 2007
ISBN 978 0 470 16569 0

Guidelines for Implementing Process Safety Management Systems Center for Chemical Process Safety 1994 ISBN 978 0 8169 0590 4

Guidelines for Auditing Process Safety Management Systems Center for Chemical Process Safety 1993 ISBN 978 0 8169 0556 8

Guidelines for Technical Management of Chemical Process Safety Center for Chemical Process Safety 1989 ISBN 978 0 8169 0423 5

Plant Guidelines for Technical Management of Chemical Process Safety Center for Chemical Process Safety 1992 ISBN 978 0 8169 0499 0

Process safety management systems SPC/TECH/OSD/13 OSD Internal Document HSE
www.hse.gov.uk/foi/internalops/hid/spc/spctosd13.pdf

Developing process safety indicators: A step-by-step guide for chemical and major hazard industries HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0

Guidance on safety performance indicators OECD <http://www2.oecd.org/safetyindicators>

Human factors (general)

Reducing error and influencing behaviour HSG48 (Second edition) HSE Books 1999
ISBN 978 0 7176 2452 2

Human factors integration: Implementation in the onshore and offshore industries RR001 HSE 2002
www.hse.gov.uk/research/rrhtm/rr001.htm

The promotion of human factors in the onshore and offshore hazardous industries RR149
HSE Books 2003 ISBN 0 7176 2739 X

Mutual misconceptions between designers and operators of hazardous installations RR054
HSE Books 2003 ISBN 0 7176 2622 9

Development of human factors methods and associated standards for major hazard industries
RR081 HSE Books 2003 ISBN 0 7176 2678 4

Leadership and safety culture

Leadership for the major hazard industries Leaflet INDG277(rev1) HSE Books 2004 (single copy free or priced packs of 15 ISBN 978 0 7176 2905 3) www.hse.gov.uk/pubns/indg277.pdf

Managing Human Error Number 156 Parliamentary Office of Science and Technology June 2001
www.parliament.uk/post/pn156.pdf

Safety Culture HSE Human Factors Briefing Note No 7
www.hse.gov.uk/humanfactors/comah/07culture.pdf

Involving employees in health and safety: Forming partnerships in the chemical industry HSG217
HSE Books 2001 ISBN 978 0 7176 2053 1

Health and Safety Climate Survey Tool (electronic publication) HSE Books 1998
ISBN 978 0 7176 1462 2

A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit RR367 HSE Books 2005 ISBN 0 7176 6144 X

Key performance indicators

Developing process safety indicators: A step-by-step guide for chemical and major hazard industries HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0

Guidance on safety performance indicators OECD <http://www2.oecd.org/safetyindicators>

Staffing, shift work arrangements, and working conditions

Assessing the safety of staffing arrangements for process operations in the chemical and allied industries CRR348 HSE Books 2001 ISBN 0 7176 2044 1

Safe Staffing Arrangements – User Guide for CRR348/2001 Methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated plant and/or equipment Energy Institute 2004 ISBN 0 85293 411 4
www.energyinst.org.uk/humanfactors/staffing

Managing shift work: Health and safety guidance HSG256 HSE Books 2006
ISBN 978 0 7176 6197 8

Fatigue HSE Human Factors Toolkit: Note 10. www.hse.gov.uk/humanfactors/comah/10fatigue.pdf

The development of a fatigue/risk index for shiftworkers RR446 HSE Books 2006
www.hse.gov.uk/research/rrhtm/index.htm

Horne JA and Reyner LA 'Vehicle accidents related to sleep: A review' *Occupational and Environmental Medicine* 1999 56 (5) 289–294

Improving alertness through effective fatigue management Energy Institute, London
September 2006 ISBN 978 0 85293 460 9 www.energyinst.org.uk/

Fatigue Human Factors Briefing Note No 5 Energy Institute 2006 www.energyinst.org.uk/

EEMUA 201 *Process Plant Control Desks Utilising Human-Computer Interfaces – A Guide to Design, Operational and Human Interface Issues* Publication 201 (Second edition) Engineering Equipment Materials Users' association 2009 ISBN 978 0 85931 167 0

Management of change

Organisational change and major accident hazards Chemical Information Sheet CHIS7
HSE Books 2003 www.hse.gov.uk/pubns/comahind.htm

Organisational change and transition management HSE Human Factors Toolkit: Specific Topic 3
www.hse.gov.uk/humanfactors/comah/specific3.pdf

'Assessing Risk Control Systems – RCS5 Management of Plant and Process Change' in *HID CI/SI Inspection Manual* HSE 2001 pages 135–145 www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf

Guidelines for the Management of Change for Process Safety CCPS 2008 ISBN 978 0 470 04309 7

Management of Change UKPIA Ltd Self Assessment Module 1 and Appendix 1 www.ukpia.com

Competence

Competence assessment for the hazardous industries RR086 HSE Books 2003 ISBN 0 7176 2167 7

Developing and maintaining staff competence Railway Safety Publication 1 (Second edition) Office of Rail Regulation (ORR) www.rail-reg.gov.uk/upload/pdf/sf-dev-staff.pdf

Competence HSE Human Factors Briefing Note No. 2
www.hse.gov.uk/humanfactors/comah/02competency.pdf

Competence assurance HSE Core Topic 1 www.hse.gov.uk/humanfactors/comah/core1.pdf

'Assessing Risk Control Systems – RCS12 Assessing Competence' in *HID CI/SI Inspection Manual* HSE 2001 pages 188–191 www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf

Training and Competence EI Human Factors Briefing Note No 7 Energy Institute 2003
www.energyinst.org.uk/humanfactors/bn

Cogent National Occupational Standards *Bulk Liquid Operations* Level 2

Cogent National Occupational Standards *Downstream Operations* Level 3

Management of contractors

Backs for the future: Safe manual handling in construction HSG149 HSE Books 2000
ISBN 978 0 7176 1122 5

'Assessing Risk Control Systems – RCS7 Selection and Management of Contractors' in *HID CI/SI Inspection Manual* HSE 2001 pages 150–155
www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf

Contractorisation Technical Assessment Guide T/AST/052 HSE 2002
www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast052.pdf

Principles for the assessment of a licensee's 'intelligent customer capability' Technical Assessment Guide T/AST/049 Issue 002 23/10/2006 HSE 2006 www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast049.pdf and Draft Revision of T/AST/049 (also replacing T/AST/052) 20 Mar 2009)

Managing contractors: A guide for employers. An open learning booklet HSG159 HSE Books 1997
ISBN 978 0 7176 1196 6

The use of contractors in the maintenance of the mainline railway infrastructure: A report by the Health and Safety Commission May 2002 HSC 2002
www.rail-reg.gov.uk/upload/pdf/contrail.pdf

Health and Safety Management Systems Interfacing 2003 download available from Step Change in Safety website <http://stepchangeinsafety.net/stepchange/>

The Client Contractor National Safety Group Safety Passport www.ccnsg.com/

Safety-critical communications and written procedures

Interface Management – Effective Communication to Improve Process Safety CCPS AIChE 2004
www.aiche.org/uploadedFiles/CCPS/Publications/SafetyAlerts/CCPSAlertInterface.pdf

International Safety Guide for Oil Tankers and Terminals (ISGOTT) (Fifth Edition) International Chamber of Shipping 2006 ISBN 978 1 85609 292 0

'Effective Shift Communication' – extract from *Reducing error and influencing behaviour* HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2 (reprinted 2003) pages 38–39

Human factors: Safety critical communications HSE
www.hse.gov.uk/humanfactors/comah/safetycritical.htm

Safety-critical communications Human Factors Briefing Note No 8 HSE
www.hse.gov.uk/humanfactors/comah/08communications.pdf

Reliability and usability of procedures Core Topic 4 HS
www.hse.gov.uk/humanfactors/comah/core4.pdf

Revitalising Procedures HSE www.hse.gov.uk/humanfactors/comah/procinfo.pdf

Improving compliance with safety procedures: Reducing industrial violations HSE Books 1995
HSE Books 1995 www.hse.gov.uk/humanfactors/comah/improvecompliance.pdf

'Assessing Risk Control Systems – RCS3 Operating Procedures' in *HID CI/SI Inspection Manual* HSE 2001 pages 114-125 www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf

Storage and transfer (general)

The storage of flammable liquids in tanks HSG176 HSE Books 1998 ISBN 978 0 7176 1470 7

The bulk transfer of dangerous liquids and gases between ship and shore HSG186
HSE Books 1999 ISBN 978 0 7176 1644 2

Safe use and handling of flammable liquids HSG140 HSE Books 1996 ISBN 978 0 7176 0967 3

Procedures for offloading products into bulk storage at plants and terminals RC 106 Chemical Industries Association 1999 ISBN 978 1 85897 087 5 www.cia.org.uk/newsite/

Control and alarm systems

Out of control: Why control systems go wrong and how to prevent failure HSG238 HSE Books
ISBN 978 0 7176 2192 7

Better alarm handling in the chemical and allied industries Chemical Information Sheet CHIS6
HSE Books 2000 www.hse.gov.uk/pubns/comahind.htm

Alarm handling Human Factors Briefing Note No 2 Energy Institute 2003
www.energyinst.org.uk/humanfactors/bn

Alarm handling HSE Human Factors Briefing Note No 9 HSE
www.hse.gov.uk/humanfactors/comah/09alarms.pdf

EEMUA 191 *Alarm Systems – A Guide to Design, Management and Procurement* Publication 191 (Second edition) Engineering Equipment Materials Users' association 2007 ISBN 978 0 85931 155 7

EEMUA 201 *Process Plant Control Desks Utilising Human-Computer Interfaces – A Guide to Design, Operational and Human Interface Issues* Publication 201 (Second edition) Engineering Equipment Materials Users' association 2009 ISBN 978 0 85931 167 0

BS EN ISO 11064: Parts 1-7 *Ergonomic design of control centres* British Standards Institution

Accident investigation

Human factors in accident investigations HSE www.hse.gov.uk/humanfactors/comah/hfaccident.htm

Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents Energy Institute May 2008 ISBN 978 0 85293 521 7
www.energyinst.org.uk/humanfactors/incidentandaccident

Reports of major accidents

Hopkins A *Lessons from Longford: The Esso Gas Plant Explosion* CCH Australia Ltd 2000
ISBN 978 1 86468 422 3

Investigation Report, Refinery Explosion and Fire Report No 2005-04-I-TX U.S. Chemical Safety and Hazard Investigation Board 2007 www.csb.gov/assets/document/CSBFinalReportBP.pdf

The Report of the BP U.S. Refineries Independent Safety Review Panel January 2007 (The Baker Panel Report)

Buncefield Major Incident Investigation Board *The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board* Volume 1 HSE Books 2008 ISBN 978 0 7176 6270 8
www.buncefieldinvestigation.gov.uk

Appendix 6 Emergency planning guidance

Part 1 Route map to emergency planning guidance

- 1 Legal requirements for the production of on-site emergency plans for major hazard sites are laid down in the Control of Major Accident Hazards Regulations (1999 (COMAH) (as amended by the Control of Major Accident Hazards (Amendment) Regulations 2005).
- 2 Regulation 9 lays down the requirements for top-tier COMAH establishments to write an on-site emergency plan, and regulation 10 requires the relevant local authority to produce an off-site plan. Full details of the COMAH Regulations and guidance on the legal requirements are given in *A guide to the Control of Major Accident Hazards Regulations 1999 (COMAH). Guidance on Regulations L111*.
- 3 For these top-tier establishments, specific guidance on the reasons for and constituents of the on-site emergency plan are given in *Emergency planning for major accidents: Control of Major Accident Hazards Regulations 1999 (COMAH) HSG 191*.
- 4 Regulation 7 of the COMAH Regulations requires that top-tier COMAH establishments write a safety report. The safety report must include details of the on-site emergency plan arrangements, and must contain the information required to enable the local authority to write the off-site plan. Detailed requirements for what must be included are listed in Chapter 7 of *Preparing safety reports: Control of Major Accident Hazards Regulations 1999 (COMAH) HSG 190*.¹²¹
- 5 For lower-tier establishments, COMAH regulation 5 requires that a Major Accident Prevention Policy (MAPP) be written. The MAPP must include details of the on-site emergency arrangements in place at the establishment. See *Major accident prevention policies for lower-tier COMAH establishments* Chemical Information Sheet CHIS3.¹²² However, this document highlights the requirements in HSG191 as guidance for emergency plans.
- 6 The importance of working together on the preparation of emergency plans and the roles of the different agencies involved is laid down in *Emergency response and recovery*¹²³ (available from Emergency Planning College) and in *Dealing with disasters together* (Second edition),¹²⁴ available from the Scottish Executive Office.
- 7 A brief summary of the key requirements from the main HSE publications is given overleaf. Numbers refer to paragraph numbers in the relevant documents.

Regulation 5(1), 5(2)

Lower-tier (LT)/top-tier (TT) sites.

8 Requirement for MAPP to give high level of protection to people.

L111	HSG191	HSG190
<p>125: All operators must have MAPP – LT must be separate document.</p> <p>126: Details of when MAPP must be produced.</p> <p>128: Links MAPP to safety management system (SMS) and refers to Schedule 2 for what must be included in SMS. MAPP must be in writing.</p> <p>131–132: Links MAPP to other health and safety policies.</p> <p>133: MAPP should be short and simple – refer to other documentation.</p>	<p>11–16 and 26: Details requirements for LT sites. The MAPP should include information on procedures for identifying foreseeable emergencies, and the level of planning should be proportional to probability of an accident occurring.</p>	<p>209–212: Specifies contents of MAPP.</p> <p>209(d)(v): Requires arrangements for identifying foreseeable emergencies by systematic analysis, and for preparing, testing and reviewing emergency plans in response to such emergencies.</p>

Other documents

9 Health and Safety At Work Etc Act 1974,¹²⁵ Management of Health and safety at Work Regulations 1999.¹²⁶

Regulation 5(3)

10 MAPP document shall:

- take account of the principles specified in paragraphs 1 and 2 of Schedule 2; and
- include sufficient particulars to demonstrate that the operator has established an SMS which takes account of the principles specified in paragraph 3 and 4 of that Schedule.

11 Specifically, schedule 2(e) requires that the SMS addresses planning for emergencies – adoption and implementation of procedures to:

- identify foreseeable emergencies by systematic analysis;
- prepare, test and review emergency plans to respond to such emergencies; and
- provide specific training for all persons working in the establishment.

L111	HSG191	HSG190
<p>Schedule 2 requirements relevant to on-site plan:</p> <p>427-428: MAPP must demonstrate SMS in place</p> <p>429-456: Detail of requirements of SMS.</p> <p>431: Roles and responsibilities (control of emergencies).</p> <p>434-436: Identification of hazards/emergencies.</p> <p>446-449: MAPP/SMS requirements for emergency planning are detailed for LT sites.</p>		<p>189-208: Specifies general requirements of MAPP/SMS.</p> <p>199: Figure 2 shows how MAPP and on-site plan fit with overall risk control systems.</p> <p>209-212: Specifies contents of MAPP.</p> <p>209 (d)(v): Requires arrangements for identifying foreseeable emergencies by systematic analysis, and for preparing, testing and reviewing emergency plans in response to such emergencies.</p> <p>220: Requires details of responsibilities for controlling emergencies.</p>

Other documents

12 CHIS3. HSE guidance document on MAPP for LT sites. Reinforces need to identify and control emergencies. Refers to COMAH regulation 5 and Schedule 2, and to HSG191 for help.

Regulation 5(4)

13 MAPP shall be reviewed and revised where necessary in the event of significant modifications.

L111	HSG191	HSG190
<p>138: Reinforces when changes are required and references guidance under regulation 8(4) on what constitutes significant change.</p>		

Regulation 5(5)

14 The operator shall implement the policy set out in their MAPP.

L111	HSG191	HSG190
<p>139: Emphasises must implement the policy in the MAPP.</p>		

Regulation 5(6)

15 MAPP not required separately for top-tier sites.

L111	HSG191	HSG190
140–141: Emphasises TT do not require separate MAPP, but that LT sites must have separate document.		

Regulation 7

16 TT: Requirement to have safety report and when it must be submitted.

L111	HSG191	HSG190
<p>Schedule 4 Part 1 referenced – details objectives of safety report.</p> <p>Schedule 4 Part 2 referenced – details information required in safety report.</p> <p>(See separate section relating to emergency plans below.)</p>	<p>8–10: Repeat top-tier operator duties on emergency planning, provision of information and writing of safety report.</p>	<p>214: Requires safety report to detail arrangements for co-operation with emergency services/local authority etc.</p> <p>240: Requires arrangements for communications with local authority, emergency services, other establishments, the public etc.</p> <p>241: Requires safety report to detail organisation for managing emergencies.</p> <p>247(c)(vi): Requires identification of possible emergencies.</p> <p>259, 256–259: Requires SMS to describe risk control systems for planning for emergencies.</p>

Regulation 9(1)

17 Every operator of an establishment shall prepare an on-site emergency plan which shall be adequate for securing the objectives specified in Part 1 of Schedule 5 and shall contain the information specified in Part 2 of that Schedule.

L111	HSG191	HSG190
<p>235–236: Adequate emergency plans – in writing, proportional to risk.</p> <p>238: Objectives of on-site and off-site emergency plans in accordance with Schedule 5 Part 1 (see below).</p> <p>239–242: Require communication to the public and emergency services, systems for managing information, definition of roles and responsibilities, and provision for restoration and clean up.</p>	<p>18: COMAH requires operators of TT sites to prepare on-site emergency plans.</p> <p>19: Repeats objectives to be achieved by on-site plan.</p> <p>21: Requires production of on-site plan in writing.</p> <p>22: Requires dovetailing with off-site plan.</p> <p>29–33: Give reasons for the emergency planning.</p> <p>34: Highlights it is the responsibility of the operator.</p> <p>35: Requires the involvement of all parties in the preparation.</p> <p>48–57: Describe the emergency planning process and how to prepare plans.</p> <p>58: Requires documentation of plan in writing.</p> <p>78–80: Cover scope of on-site emergency plan – the operator’s complete response to a major accident. Concentrate on events identified as being the most likely. Level of planning proportional to the probability. Plan should have flexibility to allow it to be extended and increased to deal with extremely unlikely consequences.</p> <p>The plan should detail how the operator prepares people for an emergency, and how to control, contain and mitigate the effects of an emergency.</p>	<p>120–122: Require development of the range of hazardous scenarios and prediction of their frequency and consequence for use in emergency planning.</p> <p>125: Requires provision of information.</p>

Regulation 9(2)

18 Timing of preparation of on-site plan.

L111	HSG191	HSG190
243–244: Further details of timing.	62–68: Repeat detail of timing for production.	

Regulation 9(3)

19 The operator shall consult:

- persons working at the establishment;
- the agency;
- the emergency services; and
- the health authority.

L111	HSG191	HSG190
245–247: Details on reasons for consultation and roles of agencies involved.	38, 40–42: Details of consultees for on-site plan – employees/emergency services/ local authority. 60–61: Suggest ways of working together on the plans.	

Other documents

20 RCS8-41:¹²⁷ refers to consultation with relevant statutory consultees.

Regulation 9(4)

21 The operator shall consult the local authority (except where the local authority is exempted from requirement for preparation of an off-site plan).

L111	HSG191	HSG190
248: Requires consultation during the preparation of the on-site plan.	38–42: Require consultation with local authority.	

Regulation 10(1)

22 The local authority, in whose area there is an establishment, shall prepare an off-site emergency plan and such a plan shall be adequate for securing the objectives specified in Part 1 of Schedule 5 and shall contain the information specified in Part 3 of that Schedule.

L111	HSG191	HSG190
<p>249: Plan in writing.</p> <p>250: Must meet objectives in Schedule 5 Part 1 (see below) – and include consideration to people, property and the environment.</p> <p>251–253: Must provide for restoration, clean up with appropriate remedial measures. Must consider effects on food chain.</p> <p>254: Plan can be generic if for establishments in close proximity.</p>	<p>103: Requires Competent Authority to notify local authority of need for off-site plan.</p> <p>58: Requires documentation of plan in writing.</p> <p>48–57: Describe the emergency planning process and how to prepare plans.</p> <p>21: Requires off-site plan to be produced in writing.</p> <p>22: Requires dovetailing with on-site plan.</p> <p>34: Highlights it is the responsibility of the local authority to prepare the plan.</p> <p>35: Requires the involvement of all parties in the preparation.</p> <p>60–61: Suggest ways of working together on the plans.</p> <p>104: Plan needs to co-ordinate different responders' plans.</p> <p>108: Plan specific to establishment – perhaps as appendix to general plan.</p> <p>109: Close liaison with domino groups.</p>	

Regulation 10(2)

23 Timing of preparation of off-site plan.

L111	HSG191	HSG190
<p>255–257: Guidance on timing, consultation and interim arrangements while plan is being prepared.</p>	<p>62–68: Repeat detail of timing for production.</p>	

Regulations 10(3), (4)

24 Operator must supply information to local authority to allow off-site plan to be drawn up.

25 Information must be provided by the date the on-site plan is due to be completed.

L111	HSG191	HSG190
<p>259: Only provide information required for off-site plan by the date the on-site plan must be produced by.</p> <p>260–261: Information to other sites (domino sites) who may be affected.</p>	<p>74–76: Detail information required in the on-site plan.</p> <p>77 and Appendix 2: Give information required by the fire service under Section (1) of the Fire Services Act 1947, for the development of their arrangements for dealing with a major hazard accident.</p> <p>103: Requires operator to supply information. Operator to keep record of information supplied. Operators should co-operate as much as possible with the fire service in the collection of this information.</p>	<p>506–507: Describe in detail the information that must be included in the safety report on emergency response. Includes a checklist of all the information briefly covering details of the site, details of the dangerous substances and their properties, details of the off-site areas that can be affected, details of the emergency organisation and equipment available on site to deal with them, details of warning systems.</p>

Regulation 10(5)

26 Operator must supply any further information requested by the local authority.

L111	HSG191	HSG190
<p>263: Information must be relevant to preparation of the off-site plan.</p>	<p>103: Requires operator to supply further information, operator to keep record of information supplied.</p>	

Regulation 10(6)

27 The local authority shall consult the operator, the Competent Authority, the agency, the emergency services, the health authority and appropriate members of the public on the preparation of the off-site emergency plan.

L111	HSG191	HSG190
264–270: Guidance on reasons for consultation, roles of consultees and how to consult with public.	39, 43–47, 105: Detail consultation required on the off-site plan – operator, Competent Authority, emergency service, health agency, members of the public. 105: Requires sharing of information obtained by local authority with other responders.	

Other documents

28 *Dealing with disasters together.*

Regulation 10(7), (8)

29 Exemptions from preparation of off-site plan.

L111	HSG191	HSG190
271: Requires request to and approval by Competent Authority.	122: Repeats process for derogation from requirement to have off-site plan.	

Regulation 11(1)

30 On-site and off-site emergency plans shall (by the preparer of the plan), at suitable intervals not exceeding three years:

- be reviewed and where necessary revised; and
- be tested with reasonable steps taken to arrange for the emergency services to participate in the test to such extent as is necessary.

L111	HSG191	HSG190
<p>273–274: Guidance on reviewing.</p> <p>275–286: Guidance on testing.</p> <p>287–289: Guidance on on-site testing.</p> <p>290–296: Guidance on off-site testing.</p> <p>297–298: Guidance on revising plans post-exercises.</p>	<p>200: Regulation 11 of COMAH requires that, at least once every three years, the on-site and off-site emergency plans for a TT COMAH establishment should be reviewed and, where necessary, revised.</p> <p>201: Lists a number of items that should be taken into account in the review.</p> <p>202: All appropriate changes that may affect the emergency response should be communicated to the other parties (ie local authority and emergency services).</p> <p>203–204: Review following significant modification/changes in organisation.</p> <p>205: Objectives for emergency exercises to test effectiveness of plan and focus post-exercise reviews.</p> <p>177: Emergency plans should be tested at least once every three years. This sets a minimum standard.</p> <p>178: This testing is to give confidence that the plans are accurate, complete, and practicable.</p> <p>179: Testing should be based on an accident scenario identified in the safety report. Tests should address the response during the initial emergency phase.</p> <p>180: The overall testing regime should consider, over a period of time, the full range of hazards capable of producing a major accident.</p> <p>181: Testing on-site and off-site plans at the same time can produce significant benefits.</p> <p>182: The objectives of testing the plan should be to give confidence in:</p>	

L111	HSG191	HSG190
	<ul style="list-style-type: none"> – completeness, consistency and accuracy of the plan; – adequacy of equipment and facilities; and – competence of staff. <p>183: Lists various aspects that the overall testing regime would be expected to examine.</p> <p>184: Exercises to test on-site and off-site emergency plans form part of the ongoing training of key personnel in preparation for dealing with an emergency. These exercises include:</p> <ul style="list-style-type: none"> – drills; – seminar exercises; – walk-through exercises; – tabletop exercises; – control-post exercises; and – live exercises. <p>186: There are many different ways, using combinations of the tests described, to address the elements of emergency plans that require testing.</p> <p>187: It is important to draw up a programme of emergency plan tests, prepared jointly and agreed by all the agencies expected to participate.</p> <p>189: The aims and objectives of testing emergency plans should always be made clear at the outset. The lessons learnt should be communicated to all stakeholders involved.</p> <p>191: It is important to evaluate the lessons learnt, to determine whether modifications are required to the emergency plan, and to promote good practice. Each organisation may wish to establish its own self-evaluation criteria.</p> <p>192: The evaluation process needs to include the dissemination of information and the lessons learnt, to the relevant response organisations. This will include any recommendations arising from the testing and the progress of actions.</p>	

Regulation 11(2)

31 Local authority shall try to reach agreement with the operator and the emergency services on off-site plan testing.

L111	HSG191	HSG190
299: Expands on this and allows consideration of other tests being undertaken. Must be focused on COMAH scenarios.		

Regulation 12

32 Implement plan when required because of major accident or because of potential escalation to a major accident.

L111	HSG191	HSG190
300: Requires decision-making criteria to be in place. 301: Requires specification of who can initiate alarms and plans.	69–73: Cover requirements for use of emergency plans when required, and during testing. 196–199: Cover initiation of the emergency plans. 198: The emergency plan should identify who has the responsibility for initiating the emergency plan, and when this should be done. The plan should also include when the emergency services should be alerted.	

Regulation 13

33 Allows for local authority to charge for writing and testing off-site plan.

L111	HSG191	HSG190
302–308: Further guidance on detail of charging and how it can be applied.		

Regulation 14

34 Requires information to be given to the public as detailed in Schedule 6.

L111	HSG191	HSG190
<p>Schedule 6 includes informing the public of any warning alarms/ information.</p> <p>Schedule 6(10) requires reference to the off-site emergency plan to be included.</p>	<p>206–209: Cover provision of information to the public.</p> <p>210: Covers warning of the public.</p>	

Regulation 16(3)

35 Pass information to other establishments in domino groups to allow them to assess effects on their on-site plans.

L111	HSG191	HSG190
<p>339: Information must be appropriate.</p>		

Regulation 18(2)

36 Competent Authority may prohibit operation if reports and information required by Regulations not supplied.

L111	HSG191	HSG190
<p>360: Allows prohibition if information not supplied to local authority to allow preparation of off-site plan.</p>		

Schedule 4 Part 1(4)

37 For TT sites, the purpose of safety reports is to demonstrate that on-site emergency plans have been drawn up. Supplying information to enable the off-site plan to be drawn up allows the necessary measures to be in place in the event of a major accident.

L111	HSG191	HSG190
<p>468: Reinforces requirements of regulations 9 and 10 to prepare internal emergency plans and to provide information to the local authority to prepare off-site plans.</p>		<p>37: Sets out purpose of safety report that demonstration is made that MAPP/on-site plan and SMS are drawn up.</p>

Schedule 4 Part 2

38 Sets out information required to be included in safety report for TT sites.

39 Specifically, (5) requires information on measures of protection and intervention to limit the consequences of an accident:

- description of the equipment installed in the plant to limit the consequences of major accidents;
- organisation of alert and intervention;
- description of mobilisable resources, internal or external;
- summary of elements described in sub-paragraphs (a), (b) and (c) necessary for drawing up the on-site emergency plan.

L111	HSG191	HSG190
492: Gives more detail on requirements.		38: Requires the information in this schedule to be included in the safety report. 504–507: Repeat requirements and list all of the information that needs to be included in the on-site plan.

Schedule 5 Part 1

40 Detailed objectives of on-site plan are laid down.

L111	HSG191	HSG190
Schedule 5 Part 1 specifies objectives: <ul style="list-style-type: none"> – containing and controlling incidents so as to minimise the effects, and to limit damage to persons, the environment and property; – implementing the measures necessary to protect people and the environment from the effects of major accidents; – communicating the necessary information to the public and to the emergency services and authorities concerned in the area; and – providing for the restoration and clean-up of the environment following a major accident. 	19: Objectives listed as L111. <ul style="list-style-type: none"> – containing and controlling incidents; – implementing the measures necessary to protect persons and the environment; – communicating the necessary information; and – providing for restoration and clean-up. 	457–458: Require consideration of: <ul style="list-style-type: none"> – the equipment to limit consequences of major accidents; – the organisation of the alert and intervention; and – the on-site and off-site resources that can be mobilised. <p>More detail on these is given in:</p> <p>459: Fixed equipment. 460: Organisation. 461–463: Resources available.</p>

Schedule 5 Part 2

41 Lay down information required to be included in on-site plan.

L111	HSG191	HSG190
<p>1: Persons authorised to set emergency procedures in motion, in charge of co-ordinating the on-site mitigatory action.</p>	<p>93: The plan should include the command structure for managing the on-site response. Appropriate arrangements should be made for circumstances where senior managers are not available.</p>	<p>460a: Requires information on the functions of the different roles in managing an emergency, including who has authority to initiate plan.</p> <p>460f: Requires details for how site response personnel, the emergency services and the local authority are alerted and mobilised.</p> <p>465–466: Require full details of the mobilisable resources and demonstration of their adequacy.</p>
	<p>81–82: The plan should identify nominated key personnel by name or job title.</p> <p>COMAH requires the on-site plan to include the names or positions of people authorised to set emergency procedures in motion, and of the person in charge of co-ordinating the on-site mitigatory response. These functions are usually carried out by the site incident controller (SIC) and the site main controller (SMC).</p> <p>On smaller sites the SIC and SMC roles can be assigned to the same person.</p>	
	<p>83: The SIC is responsible for taking control at the scene of the incident. Round-the-clock cover to fill this role is essential.</p> <p>84: Details the responsibilities of the SIC.</p>	
	<p>85: The SMC has overall responsibility for directing operations from the on-site emergency control centre (ECC).</p> <p>86: Details the responsibilities of the SMC.</p>	
<p>2: Person with responsibility for liaison with the local authority.</p>	<p>94: Normally person responsible for preparing the on-site plan.</p>	<p>460a: Requires this.</p>

L111	HSG191	HSG190
<p>3: Actions to be taken to control an event and to limit consequences, including a description of the safety equipment and the resources available.</p>	<p>95: This is the principal component of the on-site emergency plan, and should include:</p> <ul style="list-style-type: none"> – types of foreseeable accidents; – the intended strategy; – details of personnel with roles to play, and their responsibilities; – details of the availability and function of special emergency equipment; and – details of the availability and function of other resources. 	<p>460b: Requires details on arrangements for controlling and limiting the consequences of an accident through isolation, fire fighting and preventing domino effects.</p> <p>459a: Requires detail of fixed equipment in place.</p> <p>467–468: Require details of the equipment on site, that there is sufficient equipment in usable condition.</p> <p>497–498: Require details of maintenance of equipment to ensure it is usable when required.</p> <p>469–471: Require details of PPE availability.</p> <p>472–475: Require details of the adequacy of firefighting resources – personnel, foam, firewater etc, including dealing with firewater run off.</p> <p>476–485: Require details of equipment and actions to minimise effects of releases to air and water.</p> <p>486–490: Require details of arrangements for sampling and monitoring.</p> <p>491–493: Require details of equipment for restoration and clean up.</p> <p>494–495: Require details of any specialist/ancillary equipment.</p>
<p>4: Arrangements for giving warnings and the action people are expected to take on receipt of a warning.</p>	<p>96: This should include the systems, equipment and facilities for early detection of a developing major accident, and the responsibilities for initiating the suitable responses by on-site personnel (to evacuate, shelter, use PPE etc).</p>	<p>460c: Requires details of the arrangements for alerting people on site, the public and neighbouring establishments.</p> <p>460d: Requires details of communications are established and maintained.</p>

L111	HSG191	HSG190
	<p>87: The ECC is the principal facility from which operations, to manage the emergency response, are directed and co-ordinated. This will normally be occupied by the SMC, other key personnel as appropriate, and by the senior officers of the emergency services.</p> <p>88: The on-site ECC should have good communication links with the SIC and all other installations on the establishment, as well as appropriate points off site.</p> <p>89: The on-site ECC requires facilities to record the development of the incident.</p> <p>90: On-site ECCs generally have:</p> <ul style="list-style-type: none"> – equipment for adequate external off-site communications; – equipment for adequate internal communications; and – site plans and maps (to show a range of systems as recorded in the guidance). <p>91: Careful consideration should be given to the location of the on-site ECC, which should be designed to be operational in all but the most severe emergency.</p>	
<p>5. Arrangements for providing initial and updated information and warning to the local authority.</p>	<p>97: Arrangements for alerting and providing the information they will require to respond.</p>	
<p>6: Arrangements for training staff in the duties they will be expected to perform, and where necessary co-ordinating this with the emergency services.</p>	<p>98: This should include arrangements for training and instructing the on-site personnel and the arrangements for liaising with the off-site emergency services.</p> <p>175: The safety report requires evidence of suitable arrangements for training individuals in emergency response.</p>	<p>499–500: Require that the safety report includes details of training for all personnel involved in emergency response or who may be affected by it.</p>

L111	HSG191	HSG190
	<p>176: This training should be kept up-to-date, with suitable refresher training. All those involved in testing emergency plans should have had some previous training to introduce them to their role.</p> <p>All relevant staff from every shift should receive full training in their expected response.</p> <p>The aims and objectives of training should be clear, and the effectiveness of the training should be reviewed and evaluated.</p>	
<p>7. Arrangements for providing assistance with off-site mitigatory action.</p>	<p>99: Details of any specialist equipment or expertise and role of operator staff in briefing media.</p>	

Other documents

42 IP19:¹²⁸ details of pre-planning requirements for firefighting.

Schedule 5 Part 3

43 Details information required in off-site plan.

L111	HSG191	HSG190
<p>Schedule 5 Part 3 requires the following information to be in the off-site plan:</p> <ul style="list-style-type: none"> – people authorised to set emergency procedures in motion and authorised to take charge of and co-ordinate off-site action; – arrangements for receiving early warning of incidents, alert and call-out; – procedures; – arrangements for co-ordinating resources necessary to implement the off-site emergency plan; – arrangements for providing assistance with on-site mitigatory action; – arrangements for off-site mitigatory action; – arrangements for providing the public with specific information relating to the accident and the behaviour which it should adopt; – arrangements for the provision of information to the emergency services of other member states in the event of a major accident with possible transboundary consequences. 	<p>101–102: Lays down scope of off-site plan.</p> <p>111: Covers organisation, arrangements for restoration and clean-up and emphasises working as a team.</p> <p>112: How warnings received and cascaded.</p> <p>113: Covers mobilisation of, communications and co-ordination between roles and responsibilities and rendezvous of responders.</p> <p>114: Arrangements required to link with on-site plan and resources to manage on-site response.</p> <p>115: Arrangements for mitigation of off-site effects, traffic and access control, protection of public.</p> <p>116–117: Arrangements for warning and advising public on action, arrangements for dealing with the media.</p> <p>118: Requires discussion with Competent Authority if this arises.</p>	

Part 2 Emergency response arrangements

1 This section covers the recommendations relating to on-site emergency response arrangements and the interface between on-site and off-site emergency response arrangements. Further recommendations will follow dealing with any additional issues in these areas that have been identified in the MIIB’s emergency preparedness, response and recovery report, as well as consideration of off-site issues. This further work is currently under development by the Buncefield CAP-EPLG (EPRR) Working Group 3. An overview of emergency planning requirements can be found in part 1 of this appendix.

Principles

2 All sites in scope should prepare in writing a suitable on-site emergency plan as required by the COMAH Regulations. For lower-tier COMAH sites the plan should be prepared as part of the MAPP.

3 The emergency plans should consider the response to and mitigation of a multiple tank fire following an explosion. The plan should cover the on-site consequences of such an event and the assistance available in the form of off-site mitigatory actions (reference should be made to HSG191 paragraph 115 for examples of such off-site mitigatory actions).

4 The incident-specific emergency response plans should consider fire management requirements in response to, and mitigation of, a multiple tank fire. The plan should cover the

on-site consequences of such an event and the assistance available in the form of off-site mitigatory actions. Any plan deemed necessary to deal with such an event must be capable of operating effectively even in the event of a preceding explosion.

5 The emergency response plan (for a multiple tank fire) should be tested on a schedule to be agreed with the local CA inspectors. Site-specific guidance should be produced as to what is required to exercise the firefighting arrangements.

6 During preparation of the on-site plan, the operator should consult with the local authority emergency planning unit, the Environment Agency (or SEPA) and the local emergency services, particularly the local Fire and Rescue Service, on the content of the on-site plan to ensure the off-site response available is adequate to deal with the incident.

7 The operator should provide all information (relating to the site) required by the COMAH Regulations to the local emergency planning unit to allow the off-site plan arrangements to dovetail with the on-site plan.

8 The operator should keep the on-site plan up to date and should ensure that any significant changes are communicated to the local authority and other concerned agencies.

9 The operator should ensure the on-site plan is functionally tested at least every three years. Site-specific guidance should be produced as to what is required to exercise the plan.

10 Trained, knowledgeable and competent personnel must be involved in the exercise of the firefighting plan (the firefighting plan being a sub-set and one specific aspect of an overall emergency response plan, which specifically covers firefighting tactics and equipment etc. needed to deal with a fire, or to allow a controlled burn) and in the testing of the on-site plan. They must fulfil the tasks they will be expected to fulfil during an incident.

11 Whenever a plan is reviewed/tested or if there has been a material change in an aspect of an emergency arrangement, the operator should inform all contributors to the plan of any changes to arrangements and verify that the arrangements are still adequate. All contributors to the plan should be encouraged to inform the site operator proactively of any material changes affecting their contribution.

On-site emergency plan

12 A template for an on-site emergency plan can be found in part 3 of this appendix. It is envisaged that sites will complete this template and that it will then act as a high-level document providing an overview of the site's arrangements. Underpinning this document will be a series of detailed plans relating to specific incidents.

13 Planning should consider the scenario of a multiple tank fire following an explosion. The magnitude and extent of the Buncefield explosion has been investigated and discussed in the 'Buncefield explosion mechanism phase 1: Volumes 1 and 2 RR718 HSE Books 2009' report, however further research is currently ongoing as part of phase 2 of this work. Once accurate information is available this will be disseminated. In the meantime, operators should make a reasonable estimate of the scale of explosion that may occur on their site and plan accordingly. Refer to paragraphs 35-49 for guidance on planning emergency arrangements.

Firefighting planning and preparation

14 This topic comprises of two elements; firstly, the actions that should be put in place before an event occurs and secondly, actions that should be carried out once an event has occurred. These arrangements should be agreed by all parties involved, including off-site responders.

15 Planning aids the firefighting operations immensely by determining what is needed to extinguish the fire or manage a controlled burn, and how to deliver the required resources and manage firewater to prevent environmental impact.

16 Scenario-based incident-specific emergency response plans can identify incident control resources required for accidental release, spillages and fire and emergency response. They can also provide guidance on control and deployment of the necessary resources and importantly, can be used as a tool to exercise against, thus closing the loop from preparation to planned and exercised response.

17 Sometimes a 'controlled burn' strategy may be appropriate. Controlled burn is where the fire is not extinguished deliberately to allow the fuel to burn away in a controlled fashion. In such cases, firefighting resources will still be required, primarily to cool adjacent tanks and facilities to prevent escalation.

18 A controlled burn strategy may be appropriate if, for example:

- firewater run-off or fuel would cause significant pollution to sensitive environmental receptors such as surface and groundwater abstractions and/or designated habitats;
- the site is remote from centres of population or a controlled burn is the best option for air quality;
- the site is not capable of containing the required quantities of firefighting water and foam; or
- there is a significant risk to firefighter safety.

19 A controlled burn strategy may not be appropriate if:

- smoke plumes could result in a risk to public health, and/or large areas require evacuation;
- major transport routes require closing. If a transport route is threatened, a risk assessment will be required to determine the consequences of environmental damage against the impact on transport routes;
- there is a significant risk of the fire escalating.

20 Such deliberations should form part of the environmental and safety risk assessment carried out by the operator when producing the on-site emergency plan. This should be in consultation with the environment agencies, the local authorities, the emergency services (particularly the Fire and Rescue Service) and other stakeholders.

21 Further guidance on the use of controlled burn is available in the Environment Agency's PPG 28¹²⁹ and the Fire and Rescue Service's *Manual on environmental protection*.¹³⁰

22 If it is decided to extinguish the fire then EI 19 *Fire precautions at petroleum refineries and bulk storage installations* is considered to be 'relevant good practice' under COMAH, and operators should comply fully with this good practice. New sites should comply fully with EI 19. Existing operators should comply with this relevant good practice where it is reasonably practicable to do so. In effect, this means that existing operators should undertake a gap analysis between the requirements in this code and those measures present on site. Any measures not in place but which are specified in the code should be implemented if it is reasonably practicable to do so.

23 The following is a list of the steps needed to plan for tank related fire and emergency scenarios, which have been drawn from EI 19 to aid operators. It states the questions that need to be considered and points to the relevant section in the code for further detail.

24 **Step 1** Determine the worst-case scenario for the fire event. For fuel depots this is considered to be either the largest tank in a single bund, or the largest group of tanks in a single bund. If the plan adequately covers the resources for the worst-case scenario, it can be considered capable of dealing with lesser similar events, eg fires in smaller tanks etc. (EI 19 sections 2.5–2.7, section 3.2.)

25 **Step 2** Assume a full surface tank fire and bund fire.

26 **Step 3** Determine the radiant heat hazard ranges using appropriate consequence modelling (and including weather factors) to determine safe locations for the firefighting resources deployment. (EI 19 section 2.6.) This also determines the size of monitor necessary to achieve the required throw to reach the tank roof. The actual distance from the monitor to the involved tank only depends on the effective reach of the monitor used. It is important to determine the wind direction because the monitor should be placed to allow the wind to carry the foam to the fire. Changes in wind direction will have to be accommodated in the plan. Fire monitor performance is available from the manufacturer, but be aware the figures quoted will relate to best performance. Operators should base their plan on perhaps 20% reduction in performance to counter this, and then test it appropriately to prove the effectiveness.

27 **Step 4** Determine the amount of foam concentrate and water necessary to firefight the worst-case scenario. (EI 19 Annex D.)

28 **Step 5** Assess whether the necessary foam stocks are available on site. If not, consider how quickly these stocks can be brought to the site and by whom – what arrangements have been made with the Fire and Rescue Service, foam manufacturers and/or neighbouring sites. Ideally operators should have the means and quantity of foam on site to cope with a fire in the largest bund immediately. Operators will also need to consider how foam stocks can be transported around the site.

29 **Step 6** Is the water supply sufficient in terms of quantity, pressure and flow rate? (EI 19 Annex D6.) The pressure required is back-calculated starting at the monitor. Most monitors require 7 to 9 bar, then add in the frictional losses from the monitor to the pumps. Operators need to remember that the system demands will not just be at the monitors; water drawn from any fixed system applications and cooling streams will also need to be considered. It is important to determine the required volumes and pressures used. Dynamic system demand testing will provide the evidence that the system can deliver the required resources.

30 **Step 7** If high volume pumps or high pressure pumps are necessary to achieve the required water capacities, where will these be provided from and how long will they take to arrive and be set up? The possibilities include fixed firewater pumps at the site, mobile firewater pumps purchased by the site, pre-arranged mutual aid from other nearby facilities or the Fire and Rescue Service. All resources will need to be considered in the plan so they can be logistically arranged for relay pumping purposes. Remember to build in redundancy to cover for the nearest resources being already in use or in repair etc.

31 **Step 8** What means are there for delivering the required foam/water to the fire? How many and what size monitors are necessary? This is determined by the area at risk and the application rates required to secure and extinguish this risk. Remember the need for compatibility where hardware is brought from a variety of sources.

32 **Step 9** How much and what size and pressure rating of hose is required? Where will this quantity of hose be obtained from? The size and quantity of hose required on the flow rate, pressure and distance from the water supply. The greater the flow rate, pressure or distance from the water supply, the larger the diameter and pressure rating of the hose needed.

33 **Step 10** How will any firewater run-off be dealt with? Hose and pumps will be necessary to transfer firewater run-off from the bund to another bund or catchment area. Alternatives include purpose-built bund overflows to a remote tertiary containment system, or increasing the capacity of an existing bund. Transfer could be by pumps or via gravity flow.

Firefighting incident management

34 The following actions should be carried out:

- Operators should contact the local authority Fire and Rescue Service in accordance with the pre-incident management agreement between the operator and the Fire and Rescue Service.
- The local authority Fire and Rescue Service should rendezvous at a predetermined holding point for the company concerned.
- Fire and Rescue Service Incident Commander should formally liaise with the company on-scene commander (and site fire officer if applicable), obtaining information regarding the incident, whether or not people are involved, the resources in place and the hazards and risks associated with the particular event. These persons will form the incident control team (ICT) along with any others required by the circumstances.
- Establish immediate priorities and the potential for escalation. Local scenario-specific emergency response plans (ERPs) for the plant or area should at this time be made available to, and be used by, the ICT.
- Lines of supervisory authority and the means of communication should be clearly established within the ERPs to assist in effective reporting and incident control.
- The ICT must ensure the safety of all personnel. This team should have:
 - completed a dynamic risk assessment (DRA) and if there has been time, a written record needs to be handed to the Fire and Rescue Service IC on their arrival;
 - arranged for the DRA to be recorded and constantly reviewed. The DRA also needs to be communicated and the tactical mode declared, implemented and recorded;
 - ensured that safety officers are appointed with their responsibilities clearly established.
- The ICT should also:
 - establish the incident command position;
 - determine the operational objectives and the incident plan, including tactical and strategic considerations;
 - identify from the ERPs, the equipment, material and resources required, coordinating effort into sourcing equipment and materials to the incident;
 - obtain additional support/equipment/resources if required (via mutual aid partnerships if in existence);
 - implement the mutually agreed strategy by bringing resources on-site from the rendezvous point at this stage;
 - monitor and review the implemented plan for ongoing potential hazards and the continued effectiveness of the plan at predetermined intervals. If the plan cannot be followed or if a deviation is required from it at any time then a DRA must be carried out, communicated to all concerned and recorded;
 - establish welfare arrangements for all at incident scene; and
 - ensure that media issues are addressed.

Guidance for planning emergency arrangements

35 The event that operators should plan for, with respect to emergency arrangements, is that of a multiple tank fire following an explosion. Emergency arrangements will need to be capable of operating effectively following such an event.

36 The overpressure within the cloud was generally greater than 200kPa; the maximum overpressure was probably much higher. These high levels of overpressure were seen in all areas; there was no distinction between different terrain (car parks, tank farms, open grassland and belts of trees). Overpressure diminished rapidly with distance away from the edge of the cloud; evidence suggests overpressures in the region of 5-10kPa within ~150m.

37 Table 17 details typical effects of over-pressure. The effects of over-pressure are not exact and sensible interpretation erring on the side of caution should be employed.

Table 17 Typical effects of blast over-pressure on people, buildings and plant

Damage details	Incident equivalent peak over-pressure in mBar
Effects on people	
Threshold for ear drum rupture.	138
Minimum pressure for penetration injury by glass fragments	55.2
Threshold of skin laceration by missiles	69–138
Persons knocked to the ground	103–200
Possible death of persons by being projected against obstacles	138
50% probability of eardrum rupture	345–480
90% probability of eardrum rupture	690–1034
Threshold of internal injury from the blast	490
50% fatality from serious missile wounds	276–345
Near 100% fatality from serious missile wounds	483–689
Threshold of lung haemorrhage	837–1034
Immediate blast fatalities	4826–13790
Building damage details	
Nearly 100% of exposed glass panes broken	46–110
Partial demolition of houses – made uninhabitable	69
Nearly complete destruction of houses	345–483
Probable total destruction of houses	689
Effects on plant	
Most pipes fail	300
Steel cladding of buildings ruptured	400
Brisk panels in steel or concrete frame rupture	500
Reinforced structures distort and unpressurised tanks fail	210–340
Wagons and plant items overturned	340–480
Extensive damage to chemical plant	>480
Failure of a pressurised sphere	>700

Note: the information in this table has been compiled by HSE's risk assessment unit, based on WW2 data on blast effects.

38 At Buncefield, the damage from the VCE occurred out to approximately 250 m from the tank wall of the tank that was overfilled (Note: the distances are radii from the tank wall as this is the location of the overflow. Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach). While the behaviour of vapour clouds can be directional, the movement of the cloud is heavily dependent on factors such as site topography, degree of congestion and weather conditions. Attempting to predict the travel of a potential vapour cloud with the necessary level of reliability in view of its potential effects is not a practical proposition with existing knowledge. Hence the effects of the explosion should be considered as being 250 m from the tank wall, assuming that the cloud could travel in any direction.

39 Further information on the predictive assessment of COMAH safety reports in light of the Buncefield incident can be found in *COMAH safety reports: Technical policy lines to take for predictive assessors*.

40 The methodology below is for dutyholders to evaluate the potential impact of a VCE on the emergency arrangements at their site. These arrangements will include fixed equipment such as fire pumps and hydrants as well as foam stocks, site ingress and egress points for off-site emergency resources, control rooms and critical equipment.

41 Dutyholders should carry out individual site assessments based on the following methodology:

- identify the critical equipment and resources necessary to respond to a credible incident scenario following a VCE. Typically this would be a multi-tank fire initiated by the VCE;
- for those resources identified, plot the location on a site plan of those that are installed at the facility or provided as part of a mutual aid or common user scheme;
- apply the over-pressure area of 250 m radius from the tank wall (Note: the distances are radii from the tank wall as this is the location of the overflow. Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach) (note: it is possible that this area will cover the whole site and may extend to include areas where mutual aid or common user equipment is held);
- the effects of blast over-pressure should be applied to all items of critical equipment and resources within the designated area. Decide whether the equipment or resource would remain usable or not (note: apply the precautionary principle and if in doubt treat as unusable);
- for each item of critical equipment or resource that is likely to be damaged in the event of a VCE, the facility should consider:
 - moving the equipment outside the area likely to be affected;
 - duplicating the equipment by providing an alternative outside the area;
 - providing protection in the form of blast shielding (note: if site power and control systems are lost there may be little advantage in protecting pumps or other equipment that cannot be used);
 - reducing the consequence of the damage. For example, if a fire pump is lost in the blast, but an underground hydrant system is still usable, then additional inlet points for mobile pumps from open water could restore operation of the system;
 - using off-site emergency equipment and resources, eg by providing mobile equipment from the Fire and Rescue Service or mutual aid scheme;
 - for access and egress points used by the emergency services, provide alternate routes in case the main roads and gates are affected by the incident.

42 The results of the assessment should be documented and incorporated into the on-site and off-site emergency plans. These results should be used to plan the emergency arrangements for the site. Any dependency on mutual aid or external resources should be agreed, and these arrangements regularly tested and reviewed. The template for completion of the on-site plan for COMAH sites is provided in part 1 of this appendix. The template can be completed and used as the basis for the on-site emergency plan. This approach may be of benefit to lower-tier COMAH sites.

43 The blank template can be used as a checklist against which to verify an existing on-site plan.

44 Each emergency plan should be specific to an individual site. Dutyholders should review their on-site emergency plan to ensure that there are enough people with the right training and competence to deal with an emergency.

45 The following factors should be considered:

- Have all the risks been identified for the site with respect to the credible emergency scenarios?
- Have response plans been developed to deal with these risks?
- Do the response plans identify actions and resources needed especially people?

- Do the response plans identify escalation measures including the resources needed to action the plan?
- Are there sufficient resources to action these plans? This can be done by a gap analysis of the staff and other resources. Consider the following:
 - Time: Can staff be released in an emergency? Have they time to do all that they need to under the plan?
 - Tools: Do staff have access to the correct equipment/information?
 - Ability: Can they use the equipment/understand the information and do what they need to properly?
 - Sustainability (for longer duration scenarios): Are suitably competent relief staff available to maintain the emergency plan over a realistic response period.

46 This can be summarised as ‘does the site at all times have enough staff who are able to do what they need to in the time available to make the plan work?’

47 Each member of staff should be competent to implement the emergency plan. Competency should be checked during training and testing of emergency plans. Can each person do what they need to – if not train and evaluate? Refresher training is vital to maintain competence and there needs to be realistic testing to ensure that staff demonstrate competence. Dutyholders should record all reviews, analysis, training and testing.

48 Table 18 is derived from the Energy Institute guidance in EI 19. It provides an example of the competencies required by a typical emergency response team member. The areas where competencies are necessary have been identified by analysing the tasks that the person will fulfil as their part in the plan. The same process can be applied to all tasks and the competencies required identified.

49 It is essential to consider tasks such as drainage, firewater management, pollution control and site recovery when deciding on training and competencies.

Table 18 Emergency response team member – example competency profile

Operations	Maintenance	Procedures	Skills
1.1 Inspect and test fire vehicles	2.1 Inspect and test site portable/mobile fire equipment	3.1 Execute assigned duties	4.1 Respond to emergencies
1.2 Inspect and test fire station communications	2.2 Inspect and test site fixed fire systems	3.2 Working safely	4.2 Fixed systems/fire tender work in incident area
1.3 Exercise emergency response	2.3 Inspect and test site fire hydrants		4.3 Carry out firefighting or incident control operations
1.4 Fire prevention			4.4 Rescue personnel
			4.5 Reinstate resources
			4.6 Training and instruction

Source: EI 19 Annex E – an example ERT member competency profile based on four units.

50 Dutyholders should evaluate the siting and protection of emergency response facilities, and put in place contingency arrangements either on or off site in the event of failure. This should include identifying and establishing an alternative emergency control with a duplicate set of plans and technical information.

51 EI 19 provides good practice guidance on protection of safety-critical equipment and resources.

52 Fire protection and other critical emergency equipment and resources should be located in non-hazardous areas so far as is reasonably practicable. Dutyholders should consider the consequence of a major incident to determine where to locate such items as they may constitute sources of ignition. Locate equipment and resources to enable access at all times during incidents. They should be capable of functioning despite the effects of fire and explosion, for example, fire pumps should be located at a safe distance away from any possible explosion/fire consequences.

53 The framework in Figure 40 can be used to evaluate the vulnerability and siting of emergency response equipment and resources.

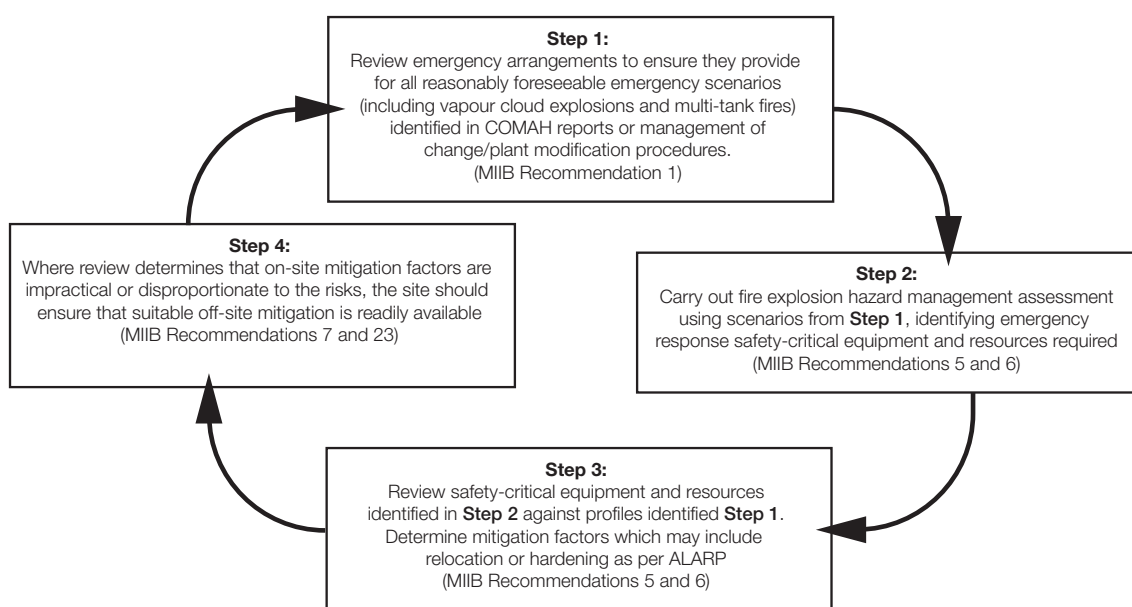


Figure 40 Example framework to evaluate the vulnerability and siting of emergency response equipment and resources

54 **Step 1** Dutyholders should consider and list worst-case events in terms of:

- hazard distances;
- over-pressures;
- radiant heat levels;
- potential for missile generation.

The emphasis should be on the effects of ‘worst-case’ incident scenarios, as these identify the most vulnerable emergency equipment and resources. However, dutyholders should consider specific issues that may arise from lesser incidents, eg different types of foam concentrate, critical emergency equipment located near relatively low-hazard operational areas etc.

55 **Step 2** Identify critical emergency response equipment and resources vulnerable to the worst-case scenarios. Start by reviewing the list to identify critical equipment and resources that may be vulnerable in a major incident. Detailed site plans with significant hazard ranges marked on them may be used as an aid.

56 The templates in part 3 of this appendix provide a detailed list of emergency response equipment and resources, drawn from industry guidance, codes, reports of the BSTG and the MIIIB. Relevant issues in *Buncefield: Hertfordshire Fire and Rescue Service's Review of the Fire Response*¹³¹ have also been included. The list should not be seen as exhaustive. Dutyholders should also consider unique features of their own sites and emergency response arrangements.

57 **Step 3** In reviewing critical equipment and resources consider all necessary measures to manage the incident, ie drainage, firewater management, power supply, control centres, communications etc. Consider the requirements to deal with the more likely scenarios, not just the high impact-low probability events. Assess what the likely level of damage would be to vulnerable equipment and resources, in terms of Table 19:

Table 19 Reviewing critical equipment and resources

Functionality (Can the system still meet its intended role or function?)	Availability (Is the system still available when it might be needed?)	Reliability (Can the system still work as intended when called upon?)
<ul style="list-style-type: none"> – Total loss (eg loss of foam supplies) – Partial loss (eg water spray system pipework may be damaged so that it cannot give adequate coverage to all vessels exposed to radiant heat and/or flames?) – No significant loss (the system can still function as intended) 	<ul style="list-style-type: none"> – Total loss (eg fire pumps destroyed by blast) – Partial loss (eg emergency access may be obstructed from certain directions) – No significant loss (the system is still available for use) 	<ul style="list-style-type: none"> – Total loss (eg severe bund wall) – Partial loss (eg damage to cabling may mean remote operation of valves is lost/unreliable, but manual operation may still be possible) – No significant loss (the system can still function when called upon)

58 **Step 4** Where there are gaps against current good practice, as an alternative to upgrading the on-site facilities, dutyholders may consider other contingency arrangements, for example, relocating mobile equipment and resources. Where further measures are necessary to provide an alternative to fixed equipment, it may be more appropriate to identify what external assistance may be available to provide sufficient contingency (eg local emergency services, mutual aid schemes). Emergency plans should be revised to take into account any possible loss of critical equipment and resources.

59 Additional measures to consider include:

- reducing the risk of the incident at source;
- increased redundancy, eg alternative fire pumps in different locations;
- increasing supplies;
- relocating resources;
- splitting supplies into different locations;
- manual back up for automated systems;
- resources that can be brought in by the emergency services;
- mutual aid schemes;
- contracts/agreements with specialist companies who can provide additional resources within a reasonable time period;
- duplicate copies of emergency information (hazard data, site plans, etc). Information kept in different locations (on and off site) and different formats (hard copy and electronic);
- alternative emergency control centre off site;
- alternative emergency response tactics (eg consideration of controlled burn if firewater supplies are lost);
- revision of emergency plans, tactics and strategies;
- exercises to test the adequacy of contingency arrangements.

60 Should the dutyholder rely on off-site fire and rescue services, the on site plan should clearly demonstrate that there are adequate arrangements in place between the parties.

61 The following guidance is aimed at sites whose current arrangements rely on the Fire and Rescue Service or other off-site responders to fulfil functions as part of their on-site emergency plan. These arrangements should also include off-site Fire and Rescue Service response required to prevent/deal with a MATTE.

62 Part 3 of this appendix provides a template for auditing the test of an off-site emergency plan. It can also be used as a basis for identifying those parts of an on-site emergency plan that rely on off-site responders. The following are examples of areas where this is likely:

- reliable relations between dutyholders, the emergency services and other responders (eg the Environment Agency/HPA) are critical in the successful management of major emergencies and there should be scheduled liaison meetings held;
- if the external Fire and Rescue Service supplements on-site fire teams, the level of training and compatibility of breathing apparatus and firefighting equipment must be established; and
- where a fire plan has been produced by the Fire and Rescue Service for specific COMAH sites including rendezvous points and alternative access to the site.

The effectiveness of these arrangements should be exercised and evaluated.

63 When all instances of reliance on off-site responders have been identified, the adequacy of the joint arrangements should be demonstrated. Part 3 of this appendix can be used to audit a test of the emergency plan. Assumptions should be validated and emergency plans reviewed and updated as appropriate.

64 Part 1 of this appendix clearly defines the arrangements between the dutyholder and the Fire and Rescue Service. These include but are not limited to:

- raising an alert and initial information;
- access points, suitable hard-standings for vehicles and rendezvous points;
- site information (water supplies, foam stocks, equipment details, drainage information, containment capability, evacuation arrangements, etc);
- pre-fire plans clearly indicating firefighting capability, resources available and firewater management arrangements.

65 Dutyholders should review their arrangements to communicate with people and establishments likely to be affected by a major accident to ensure that this information takes account of any additional major accident scenarios resulting from, for example, a large flammable vapour cloud.

66 Guidance on provision of information to the public is given in L111 and HSG191 Examples of communications plans and information letters are provided in Part 3 of this appendix.

Part 3 Example templates supporting the guidance for Recommendations 11 and 12

Template for completion of the on-site plan for COMAH sites

1 By using this template the operator should comply with the requirements of the COMAH Regulations, as detailed in HSG190, HSG191 and L111. A summary of the requirements detailed in these documents can be found in the Route map. These documents should be used as guidance when completing this template.

2 The operator must consult with off-site agencies, and it is advised that the plan is formulated in consultation with the agencies (local authority emergency planners, Fire and Rescue Service, environment agencies, HSE, police and ambulance) as appropriate during the preparation of the plan. It is advised that consultation starts at an early stage to allow for full involvement with the off-site agencies.

Table 20 Overview of emergency arrangements

Name of facility	
Full postal address	
Name or position of the person responsible for compiling this on-site plan and for liaison with the local authority for preparing the off-site plan	
Overview of the activities carried out on site	
This should include number of employees at different times of day and a sample of the potential hazardous scenarios from the site's activities from a high level; more detail will be provided in Appendix 6, Part 3, Table 22	
List of agencies consulted in the preparation of this plan	
Include name and address of contacts	
Fire and Rescue Service	
Police service	
Health authority	
Environment Agency/SEPA	
HSE	
Local authority	
Employees	
Objectives of the on-site plan (see paragraph 19, HSG191)	
Contain and control incident so as to minimise effects and to limit damage to persons, the environment and property. Implement the measures necessary to protect persons and the environment from the effects of a major accident. Communicate the necessary information to the public and to the emergency services and authorities concerned in the area. Ensure the safe and legal removal and disposal of any waste generated, and where environmental measures have failed, provide for the restoration and clean up of the environment.	
Names or positions of persons authorised to set the emergency procedures in motion and the person in charge of and co-ordinating the on-site mitigatory action	
Note: Fire and Rescue Service may at their discretion initiate these measures Identify the criteria for contacting internal/external emergency services.	
Safety of persons on site	
Arrangements to limit the risk to on-site persons. Include how warnings are to be given and the actions persons are expected to take on receipt of warnings Detail the site's means of collating a record of persons on site, identifying casualties and their locations.	
Safety of persons off site	
Arrangements to inform residents located in the Public Information Zone of the site's activities. Include how warnings are to be given and the actions persons are expected to take on receipt of warnings	

<p>Arrangements for providing:</p> <ul style="list-style-type: none"> – early warning of the incident to local authority (usually Fire and Rescue Service) and the Environment Agency/SEPA; – for initiating the off-site emergency plans; – the type of information that should be contained in the initial warning; and – the arrangements for the provision of more detailed information as it becomes available 	
<p>Arrangements for training staff in the duties that they will be expected to perform, including where necessary co-ordination with emergency services Also identify key competencies for these staff and identify methods of testing the plan</p>	
<p>Arrangements for assisting with the off-site effects of the incident Include specialist equipment, personnel, media, gas testing, plume modelling, water testing, decontamination facilities.</p>	
<p>Location of the Site Emergency Control Room (SECC) and the facilities and equipment contained in the SECC, including communications, record keeping and plans and maps of the site</p>	
<p>Identify resources (people) required to manage the response to the incident, identify resources available to ensure 24/7 cover and identify specialists who can provide information to the emergency services</p>	
<p>Identify the key roles, actions and communication flows of the Site Controller and the Site Incident Controller to ensure that these are consistent and effective</p>	
<p>Detail how on-site emergency responders will be made readily identifiable to off-site responders</p>	
<p>Identify suitable locations and mandates for the all the control centres used to mitigate the incident</p>	
Forward control point	
Site Emergency Control Centre (SECC)	
Silver Command	
Gold Command	
Health Advisory Team	

<p>Identify key contact numbers for the establishment, eg SECC, alternative SECC, site main controller, operations control room, medical centre, operations control rooms</p>
<p>Identify environmental consequences of hazard scenarios described in this document. Identify the environment pathways: eg air, permeable ground, drainage systems and receptors at risk, eg local populations, rivers, groundwaters and land</p>
<p>Identify resources available for the restoration and clean up of the environment following a major accident. COMAH specifically requires limitation of consequences and consideration of off-site mitigatory measures including appropriate restoration and clean up, eg pre-arranged contractor callout, removal and disposal of waste, provision of sampling and analytical resource to facilitate determination of disposal of polluted firewater. Identify key steps and actions during the restoration stage for the identified hazard scenarios and the procedures and resources available to:</p> <ul style="list-style-type: none"> – provide for clean up containment systems/plant areas if firewater/pollution is confined to the site; – clean up and restore the off-site environment if containment systems prove inadequate or fail. <p>See Environment Agency web page www.environment-agency.gov.uk/ for further information see Pollution Prevention Guides, eg PPG18, PPG21 and PPG28.</p>

Table 21 Hazardous events: A sample of major accident scenarios

Potential events and consequences	For example: Petroleum products Mogas Catastrophic failure of mogas tank containing 10 000 litres, with the potential to over-top the bund and ignite
Other plant areas with similar (lower) potential	Tank 1, Tank 2, Tank 3
Process and emergency response	Remote valve isolation of the tanks and transfer pumps. Evacuate site using on-site siren. Call emergency services. Apply foam on to pool of mogas.
On-plant equipment/facilities (excluding emergency response equipment)	Tank deluge and foam systems. Firewater storage 70 000 litres, pumps 3000 litres, min, pressure 10 bar.
Distances effect	If fire developed personnel within 150 m of the fire, would be unlikely to escape injury. LFL would extend 230 m.
Human health consequences	Prolonged exposure to petroleum products vapour can result in narcotic effects leading to unconsciousness. Will also cause breathing difficulties, which could be fatal. On ignition, burns could result to persons within 150 m of the fire without protection.
Environmental consequences	Volatile components will evaporate. Less volatile components will persist in the aqueous environment. Components will biodegrade with time. It is likely the contents will enter the river (if it is likely then addition containment must be provided). Firewater run off and FP foam would enter the drainage system and should be contained on site, eg shut Penstock to divert to firewater containment system.

Table 22 Information needs of the emergency services

Fire and Rescue Service

Provide information on the site layout including any other associated risks, including transformers, substations and water treatment facilities. Identify designated rendezvous points	
Identify the location of on-site fire service (if applicable) and emergency medical or first-aid facilities	
Identify systems that enable the operator to provide information during an incident, including inventory levels of notifiable hazardous substances and their physical state	
Provide information on how technical data will be provided during an incident. The data must provide general information on the properties and physical nature of the substances	
Provide information on fixed fire protection installations (eg roof vents, sprinklers, drenchers, fire shutters), with technical detail of their operation	
Identify all loading and unloading installations with technical detail of their operation	
Identify watercourses, separators and plant drainage systems with the aim of minimising environmental pollution. Include areas where firewater run off can be contained. Identify equipment required to assist in this, eg drain sealing equipment, booms and fire service New dimensions pumping equipment. Consideration should be made of the resources held by Fire and Rescue Service (FRS) and how on-site resources will be used by FRS personnel. See Environment Agency section below for more detail	
Identify water supplies available on site	
Stored water on site (litres)	
Top up facilities	
Firewater pumps, pumping capacity and pressures, activation	
Availability of systems to protect specific plant	

Alternative water supplies	
Identify alternative water resources (bore holes, rivers, canals etc) and the distance from the site	
Identify alternative water supplies to supplement on-site storage	
Identify how many <i>New dimensions</i> high-volume pumping equipment is available within your area	
Confirm quantities available from alternative supplies – consider seasonal changes	
Pre-planned strategy to estimate the maximum quantities of firewater run off and to identify lagoon and catchment areas and size	
Identify the on-site communications that can be used by the Fire and Rescue Service and identify any areas for intrinsically safe radios	
Identify any plans that allow for a controlled burn	
Identify foam supplies held on site or are available to the site via mutual aid, or other agreements	
Foam on site (litres)	
Type of foam and percentage ratios	
Storage containment methods (eg drums, IBC, bulk)	
Location of foam stock	
Method of transporting around site	
Fire and Rescue Services foam stock and type (litres)	
Location of foam	
Method of transport	
Third party/mutual aid/ suppliers foam stock and type	
Location of the foam	
Method of transport	
Identify hose on site	
Size, quantities, pressure ratings, couplings (Note: if Storz-type couplings are fitted, detail lug spacing)	
Identify type and location of hose adaptors on site	
Identify hose provided by Fire and Rescue Services, mutual aid and third parties	
Size, quantities, pressure ratings, couplings (Note: if Storz-type couplings are fitted, detail lug spacing)	
Identify type and location of hose adaptors carried	

Site staff and visitors

Details of the actions they should take to protect themselves from the effects of the accident

Police service

For scenarios identified in Appendix 6, Part 3, Table 21, identify potential numbers of off-site casualties
Detail how the site operates its media management so that its response can be dovetailed into emergency services arrangements and allow the police to co-ordinate the media response in the event of an incident
Identify major roads on the site perimeter

Ambulance Service

For scenarios identified in Appendix 6, Part 3, Table 21, identify potential numbers of off-site casualties, including likely injuries (ie burns)
Information regarding an on-site medical facilities and types of treatment that could be provided

Health

For scenarios identified in Appendix 6, Part 3, Table 21, identify potential numbers of off-site casualties, including likely injuries
Details of hazardous substances and their acute and long-term human health effects
Identification numbers of hazardous substances

Local authority

Details of on-site personnel and how they will interface with the emergency services, eg the roles of the Site Main Controller and Site Incident Controller
Details of the on and off-site resources that can be mobilised
For scenarios identified in Table 18, provide details of the impact on people and the environment not already documented, eg effect on local schools, communities, shopping centres

Environment Agency

<p>For scenarios identified in Table 18, identify environmental consequences and environmental protection measures to prevent/mitigate them, including:</p> <ul style="list-style-type: none">– Identify vulnerable surface and groundwaters and pathways to them, eg site drainage systems that need to be protected.– Details of on-site environmental protection measures, eg separators and areas where firewater run off can be contained.– A copy of the planned environmental protection strategy, eg use of controlled burn, how firewater will be contained, environmental monitoring/sampling– Details of equipment available to assist in this action, eg drain sealing mats, pipe blockers, booms, gully suckers and addition equipment held on site and/or on FRS environmental protection units.– Provide a full inventory of all products stored on site and their environmental properties. Include firefighting foams to be used.– Identify arrangements for the removal of waste and clean up of the environment, eg arrangements with licensed waste contractors.– Details of on-site personnel with responsibilities for environmental protection and how they will interface with the emergency services and Environment Agency.

Table 23 Assessment of vulnerable emergency response equipment and resources

Site:							
Major incident scenario:				Results of consequence analysis (hazard ranges):			
1 Identify vulnerable critical emergency response equipment and resources			2 Assess the potential damage and consequences (consider potential loss of functionality, availability and reliability)	3 Identify existing contingency arrangements	4 Are existing arrangements adequate?	5 Consider additional measures and take necessary action	
Critical emergency response equipment and resources	Applicable?	Vulnerable				Additional measures	Comments/ actions (including amendments to emergency plan/exercises to test adequacy of contingency arrangements)
On-site equipment							
Fire pumps/ pumphouse							
Firewater tanks/ pipework							
Fixed deluge/ spray systems							
Firewater hoses							
Ancillary equipment (adaptors, fittings, etc)							
Mobile pumps							
Mobile water/ foam cannons							
On site emergency vehicles							
Specialist equipment (mobile detectors etc)							
Personal/ respiratory protective equipment (PPE/RPE)							
Spill response equipment							
Emergency shutdown systems							
Automated systems							
Other (specify):							

Site:							
Major incident scenario:				Results of consequence analysis (hazard ranges):			
1 Identify vulnerable critical emergency response equipment and resources			2 Assess the potential damage and consequences (consider potential loss of functionality, availability and reliability)	3 Identify existing contingency arrangements	4 Are existing arrangements adequate?	5 Consider additional measures and take necessary action	
Critical emergency response equipment and resources	Applicable?	Vulnerable				Additional measures	Comments/ actions (including amendments to emergency plan/exercises to test adequacy of contingency arrangements)
On-site supplies							
Water supplies							
Foam supplies							
Other (specify):							
Infrastructure							
Emergency control centres							
Access for external emergency services							
Rendezvous points/ parking areas for external emergency services							
Access/ hardstanding for mobile pumps and specialist equipment							
Off-site holding areas for large numbers of responders							
Other (specify):							

Site:							
Major incident scenario:				Results of consequence analysis (hazard ranges):			
1 Identify vulnerable critical emergency response equipment and resources			2 Assess the potential damage and consequences (consider potential loss of functionality, availability and reliability)	3 Identify existing contingency arrangements	4 Are existing arrangements adequate?	5 Consider additional measures and take necessary action	
Critical emergency response equipment and resources	Applicable?	Vulnerable				Additional measures	Comments/ actions (including amendments to emergency plan/exercises to test adequacy of contingency arrangements)
Human, welfare and information equipment and resources							
Critical personnel/ functions							
On-site fire team							
On site incident controllers/ responders							
Operational							
Management							
Technical/ engineering							
SHE							
HR (next of kin contact)							
PR/media liaison							
Other specialists							
Welfare facilities							
Toilets							
Washing							
Rest areas							
Mess/eating areas							
Critical information							
Emergency plans							
Site drawings							
Drainage drawings							
Engineering drawings							
Product hazard data							
IT systems							
Other (specify)							

Table 24 COMAH off-site plan exercising/auditing record

Company:

Site:

	Elements of plan	Exercise date	Audit date	Operator	Competent Authority	Comments Action required
1	Administration					
1.1	Plan written, reviewed and updated					
1.2	Plan readily available to emergency services					
1.3	Maps and plans reviewed and updated					
1.4	Maps and plans readily available to emergency services					
1.5	Public informed as required (COMAH reg 14)					
1.6	Staff emergency plan training records reviewed and updated					
2	Pre-incident fire planning					
2.1	Plan considers worst case scenario					
2.2	Fire water capability proven					
2.3	Controlled burn strategy documented					
2.4	Foam capability recorded					
2.5	Firefighting equipment capability proven					
2.6	Fire water demand established					
2.7	Foam demand established					
2.8	Mutual aid/fire services foam requirements established					
2.9	Foam delivery to site agreed and tested					
2.10	Firefighting equipment demand established					
2.11	Mutual aid firefighting equipment requirements established					
2.12	Delivery of equipment agreed and tested					
2.13	Fire water run-off demand established					
2.14	Fire water run-off plans in place					
2.15	Site staff trained to carry out actions in plan and records available					

	Elements of plan	Exercise date	Audit date	Operator	Competent Authority	Comments Action required
2.16	Fire services trained to carry out actions in plan and records available					
2.17	Written agreement in place of what the fire services will provide					
3	Actions by company should an incident occur					
3.1	Initiation of off-site plan timely and adequate					
3.2	Notification to neighbours timely and adequate					
3.3	Notification to emergency services timely and adequate					
3.4	Any PPE requirements clearly communicated to the emergency services					
3.5	Setting up of Major Emergency Control Centre (MECC)					
3.6	Alerting and calling out of staff not on site, systems in place. Tested and recorded					
3.7	Provision of 'fall-back' MECC tested.					
3.8	Key staff in MECC					
3.9	Off-site communications identified and tested					
3.10	Notification to CA					
3.11	Dynamic risk assessment of off-site or potential off-site consequences					
3.12	Management of any evacuation from site tested and recorded					
3.13	Emergency services liaison, including meeting at site entrance, directions to scene of incident etc.					
3.14	Company representative with adequate knowledge available					
4	Major emergency control centre					
4.1	Communication system between MECC bronze and silver command adequate					
4.2	Briefing procedures/ 'time outs' managed well					
4.3	Adequate availability/ accuracy of site plans/ maps					

	Elements of plan	Exercise date	Audit date	Operator	Competent Authority	Comments Action required
4.4	Adequate technical information supplied to silver command by company representative					
4.5	Effective sharing and dissemination of information					
4.6	Company response adequate					
4.7	Incident log updated accurately with key events					
4.8	Effective links with forward control					
4.9	Adequate mapping to assist mitigation action(s) and reduce off-site consequences /impact on off-site arrangements					
4.10	Mitigatory action(s) to reduce any adverse effects to the environment					
5	On-site forward control					
5.1	Communication links between agencies adequate and effective					
5.2	Adequate provision of up to date and relevant information to MECC/ emergency services					
5.3	Adequate technical information supplied to MECC/emergency services					
5.4	Effective liaison with emergency services					
6	Off-site response					
6.1	Rendezvous points identified clearly, communicated to the emergency services and used correctly					
6.2	Safe routes identified and used					
6.3	Road closures/traffic management initiated by silver command					
6.4	Access to site adequately controlled by site gate staff					
6.5	Site gate staff notified of any mutual aid deliveries					

Communications

Table 25 Example communications plan

Message: emergency instructions/tests

Audience	Method	Frequency	Requirements	Partners	Feedback
Residents	Direct mailing	Annual	Letter, card, envelope Addresses Lingual translation Large print/Braille	Local authority and LRF	X calls to confirm advice
Residents	Residents forum – evening	Annual	Date, time and location Advertisement Include in annual letter Invites Agenda Speakers	Local authority emergency planners, the emergency services, Health Protection Agency, Environment Agency, local leaders	Changes to be made to card for 09/10
Businesses	Direct mailing	Annual	Letter, card, envelope Addresses Lingual translation Large print/Braille	Local authority – business continuity and emergency planning advice LRF – emergency planning	Local authority received X queries about business continuity
Businesses	Local business forum – breakfast	Annual	Date, time and location Advertisement Include in annual letter Invites Agenda Speakers	Local authority – business continuity and emergency planning advice Emergency services, Health Protection Agency, Environment Agency, local leaders	
Schools	Visit	Annual		Local authority – emergency planning	
Shops	Direct mailing	Annual		Local authority – business continuity and emergency planning advice	
Wider community	Press release	Annual			

Example letter to local householders

COMPANY

SITE NAME

ADDRESS

Dear Occupier

SAFETY INFORMATION FOR AREA X RESIDENTS

COMPANY at *SITE* regularly issues information on safety to local householders. I am pleased to enclose your copy of the Emergency Instructions Card/calendar.

This document is important for your safety. Please read it carefully and keep the Emergency Instructions Card in a safe place where you can quickly and easily refer to it should the need arise.

Please make sure that everyone in this building is aware of the emergency alarm and what actions they need to take. Think about what you would have to do and how you would do it in an emergency.

Safety at *SITE*

Safety is the number one priority for the *COMPANY* at *SITE* and we take all reasonable steps to prevent accidents of any type. We have emergency plans in place to minimise the effects of any incident. If necessary, our on-site resources would be supplemented by the emergency services and special provisions made by X County Council. More information on the response to emergencies can be found at www.ukresilience.gov.uk/response.aspx.

Further information

Call *XXXXX XXXXX* free to hear a recording of the emergency instructions and the alarm sound. You can also leave a message to request a large print version of this leaflet. *CONTACT DETAILS FOR TRANSLATION INTO OTHER LANGUAGES*. Please contact us by phone/post/e-mail, if you have any questions or concerns.

Yours sincerely

NAME

POSITION

CONTACT DETAILS incl. E-MAIL ADDRESS

TIME AVAILABLE FOR CALLS

WEBSITE FOR FURTHER INFORMATION

ON THE REVERSE:

include the details required under COMAH Schedule 6, covering points 3, 4, 5 and 6.

Example letter to local businesses

COMPANY

SITE NAME

ADDRESS

Dear Business

SAFETY INFORMATION FOR AREA X RESIDENTS

COMPANY at *SITE* regularly issues information on safety to local businesses. I am pleased to enclose your copy of the Emergency Instructions Card.

This document is important for your safety. Please read it carefully and keep the Emergency Instructions Card in a safe place where you can quickly and easily refer to it should the need arise.

As a business you have a responsibility for your staff and customers on sites. You must ensure that all are aware of the emergency alarm and what actions they need to take. In the event of an emergency, access to your premises maybe restricted so it is important that you consider what impact an emergency will have on your business and how it can be minimised through business continuity planning. *NAME, POSTION, LOCAL AUTHORITY* will advise you on how to develop your business continuity plan. Please call/e-mail *NAME* on *CONTACT DETAILS*. For further information on business continuity, visit www.preparingforemergencies.gov.uk/bcadvice/.

Safety at *SITE*

Safety is the number one priority for *COMPANY* at *SITE* and we take all reasonable steps to prevent accidents of any type. We have emergency plans in place to minimise the effects of any incident. X LOCAL AUTHORITY has an emergency plan which covers the response to an emergency by the emergency services, local authority and other organisations to help minimise the effect of an emergency and to keep you informed of what is happening and what to do.

Further information

Call *XXXXX XXXXX* free to hear a recording of the emergency instructions and the alarm sound. You can also leave a message to request a large print version of this leaflet. *CONTACT DETAILS FOR TRANSLATION INTO OTHER LANGUAGES*. Please contact us by phone/post/e-mail, if you have any questions or concerns.

Yours sincerely

NAME

POSITION

CONTACT DETAILS incl. E-MAIL ADDRESS

TIME AVAILABLE FOR CALLS

WEBSITE FOR FURTHER INFORMATION

ON THE REVERSE:

include the details required under COMAH Schedule 6, covering points 3, 4, 5 and 6.

Example of message on outside of envelope for mailings

COMPANY NAME(S) AND SITE

To the Occupier

**This envelope contains safety information
and your Emergency Instructions Card**

Keep this in a safe place
where you can easily refer to it

Updated: **MONTH YEAR**

Example emergency instructions card – preferably in form of a laminated A5 leaflet

COMPANY NAME

SITE NAME

Please read this card carefully

If a major accident happens at **SITE**, you will hear the emergency alarm.

The **alarm** will be a two-tone warble.
The **all clear** will be a single tone.

Make sure everyone in this property know and understand these instructions.

Keep this card in an accessible place and pass onto subsequent occupiers.

Display this card in a prominent place in business/community premises.

Test

The alarm is tested annually on the first Tuesday in October at 2.30 pm and again at 7.00 pm.

This card is produced in accordance with the Control of Major Accident Hazards Regulations (COMAH) to advise you what to do in the unlikely event of a major accident on our premises that could affect you and people near you.

Additional copies may be obtained from:

COMPANY

ADDRESS

CONTACT DETAILS

EMERGENCY INSTRUCTIONS FOR YOUR SAFETY

SITE NAME

GO IN, STAY IN, TUNE IN

- 1 On hearing the alarm, go inside immediately with everyone and pets.
- 2 Shut all outside doors and windows.
- 3 Pull curtains/blinds across windows facing the SITE.
- 4 Turn off any ventilation system or air conditioning unit that draws in air from the outside.
- 5 Stay in a room that does not face the SITE.
- 6 Tune in to ***BBC Radio XXX (FREQUENCY)***, which will broadcast information and instructions.
- 7 Remain indoors until you hear the 'all clear' or until you receive instructions from the Police.
- 8 If children are at school – do not collect them – they will be looked after until it is safe to go outside.
- 9 Please co-operate with the emergency services and follow their instructions.
- 10 An 'all clear' will be given when it is safe to go outside.

For your safety, access to the area will be restricted during a major accident.

If you hear the emergency alarm, call *XXXXX XXXXX*** to hear a tape recording of these instructions and to confirm the sound of the alarm is not a test.**

Appendix 7 Principles of process safety leadership



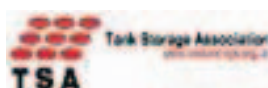
PSLG Principles of Process Safety Leadership

Process Safety Leadership Group (PSLG) is committed to improving process safety in the industries we represent. We believe that to achieve this, industry leaders have a critical role to play and must commit to establishing the following principles of process safety management in each business:

Principles:

- Clear and positive process safety leadership is at the core of managing a major hazard business and is vital to ensure that risks are effectively managed;
- Process safety leadership requires board level involvement and competence. For companies with boards located outside the UK then the responsibility to show this leadership rests with the most senior UK managers;
- Good process safety management does not happen by chance and requires constant active engagement;
- Board level visibility and promotion of process safety leadership is essential to set a positive safety culture throughout the organisation;
- Engagement of the workforce is needed in the promotion and achievement of good process safety management;
- Monitoring process safety performance based on both leading and lagging indicators is central to ensuring business risks are being effectively managed;
- Publication of process safety performance information provides important public assurance about the management of risks by an organisation; and
- Sharing best practice across industry sectors, and learning and implementing lessons from relevant incidents in other organisations, are important to maintain the currency of corporate knowledge and competence.





The PSLG regards these principles as fundamental to the successful management of a major hazard industry. We will work with all stakeholders to establish them as foundations to effective management of risks in our businesses via the following arrangements:

Organisation and resources:

- Process safety accountabilities should be defined and championed at board level. Board members, senior executives and managers should be held accountable for process safety leadership and performance;
- At least one board member should be fully conversant in process safety management in order to advise the board of the status of process safety risk management within the organisation and of the process safety implications of board decisions;
- Appropriate resources should be made available to ensure a high standard of process safety management throughout the organisation and staff with process safety management responsibilities should have or develop an appropriate level of competence;
- Organisations should develop a programme for the promotion of process safety by active senior management engagement with the workforce, both direct and contract staff, to underline the importance of process safety leadership and to support the maintenance of a positive process safety culture within the organisation;
- Systems and arrangements should be in place to ensure the active involvement of the workforce in the design of process safety controls and in the review of process safety performance;
- Business risks relating to process safety should be assessed and reviewed regularly using an appropriate business risk analysis methodology;
- Leading and lagging process safety indicators should be set for the organisation and periodically reviewed to ensure they remain appropriate for the needs of the business. Information on process safety performance should be routinely reviewed at board level and performance in the management of process safety risk is published in annual reports;
- Companies should actively engage with others within their sector and elsewhere to share good practice and information on process safety incidents that may benefit others. Companies should have mechanisms and arrangements in place to incorporate learning from others within their process safety management programmes;
- Systems and arrangements should be in place to ensure the retention of corporate knowledge relating to process safety management. Such arrangements should include information on the basis of safety design concept of the plant and processes, plant and process changes, and any past incidents that impacted on process safety integrity and the improvements adopted to prevent a recurrence.





PSLG commitment

Implementation of the above process safety leadership principles and arrangements may vary in both detail and time in different organisations. However in recognition of the essential role these principles and arrangements play in the management and sustainability of our major hazard businesses, as members of PSLG we commit to working to establish them in the industries and businesses we represent as foundations to effective process safety management and the prevention of major accidents.

Signed:

Tony Traynor
Chair
Process Safety Leadership Group

Peter Davis
UK Onshore Pipeline Operators' Association

Chris Hunt
Director General
UK Petroleum Industry Association

Martin Bigg
Head of Industry Regulation
Environment Agency

Steve Elliott
Chief Executive
Chemical Industries Association

Allan Reid
Head of National Environmental Protection and
Improvement
Scottish Environment Protection Agency

Martyn Lyons
Chairman
Tank Storage Association

Peter Baker
Head of Chemical Industries Division
Hazardous Installations Directorate
Health and Safety Executive

Bud Hudspith
Unite National H&S Adviser
(on behalf of the Trades Union Congress)



Appendix 8 Process Safety Forum: Governance and terms of reference

Background

1 The United Kingdom Petroleum Industry Association (UKPIA), Oil & Gas UK, Nuclear Industry Association (NIA), the Chemical Industries Association (CIA) and the Tank Storage Association (TSA) have various initiatives in place to progress process safety in their industry sectors. OGUK has 'Step Change to Safety', CIA 'Responsible Care' and NIA, UKPIA and TSA are well advanced in their programmes to make process safety commitments a reality. In addition, UKPIA, CIA and TSA are members of the Process Safety Leadership Group Steering Committee, which was established to succeed the Buncefield Standards Task Group originally formed in the aftermath of the Buncefield incident.

2 The Baker Report on the Texas City incident and its criticisms of the lack of leadership in process safety, echoed by the MIIB reports into the Buncefield events, has acted as a wake up call to the high hazard sector in its approach to the subject. Following the HSE-sponsored 'Leading from the Top' conference in April 2008, PSLG held a practitioners workshop in October and CEO workshop in November. All involved challenged the industry and its trade associations to put in place measures to ensure the sharing of best practice and learning from incidents across sectors as well as within sectors. Hence, CIA, OGUK, UKPIA NIA and TSA have established the Process Safety Forum to bring together the trade association experts to facilitate that sharing and learning.

Aims of the Forum

3 The Process Safety Forum (PSF) has been set up to provide a platform whereby initiatives, best practice, lessons from incidents and process safety strategy can be distilled and shared across sectors; to influence our stakeholders (including the Regulator); and to drive the process safety management performance agenda. The Forum may, from time to time, make recommendations to industry via the trade associations on directions of travel that would likely benefit all sectors.

4 Outcomes:

- a shared understanding of the current initiatives in place and immediate future plans in all sectors on process safety;
- identification of barriers to sharing of best practice and incident learnings in sectors and facilitating the development of recommendations for improvement;
- identification of initiatives to enhance process safety leadership across sectors;
- a shared understanding of effective process safety performance indicators;
- stakeholders (including the Regulator) are informed and engaged. Messages are collective where appropriate and individual where necessary.

5 Governance, roles and responsibilities:

- PSF will report progress to the trade associations on a quarterly basis;
- PSF will be chaired by Paul Thomas;
- each trade association in turn will host the meetings;
- secretariat support will be provided jointly by UKPIA, CIA, NIA, TSA and OGUK as and when required by request from PSF chair;
- the chair is responsible for leadership of the PSF and ensuring that it delivers its objectives successfully, resolving any disagreements between PSF members

6 Members of the Task Group include representatives from:

- the UK Petroleum Industry Association;
- Oil & Gas UK;
- the Nuclear Industries Association;
- the Chemical Industries Association; and
- the Tank Storage Association.

7 Members will:

- contribute data and information wherever possible to support the aims of the Forum;
- communicate openly within the Forum and respect information provided by others in confidence;
- observe constraints imposed on the exchange of commercially sensitive information by competition law;
- provide feedback to their trade association.

Appendix 9 BSTG report cross reference

1 Table 26 provides a cross reference with the original BSTG report. Paragraphs have either been:

- superseded – the guidance in the BSTG report has been replaced by new guidance in the PSLG report;
- updated – the guidance in the BSTG report has been revised for inclusion in the PSLG report;
- deleted – the guidance in the BSTG report is no longer required; or
- copied – the guidance in the BSTG report has been copied into the PSLG report.

Table 26 Cross-reference with BSTG report

BSTG paragraph reference	Status	PSLG report reference
Foreword	Updated	Foreword
Introduction (1–6)	Updated	Introduction
Scope (7–9)	Updated	Scope
10–15 (including tables)	Updated	Summary of actions required – Implementation timescales
16–17	Updated	Part 1 Systematic assessment of safety integrity levels – Introduction
18–19	Superseded	Appendix 2 Guidance on the application of Layer of Protection Analysis (LOPA) to the overflow of an atmospheric storage tank
20–21	Superseded	Recommendation 1 – Incorporating the findings of SIL assessments into COMAH safety reports
22	Updated	Part 2 Protecting against loss of primary containment using high integrity systems – Introduction
23–25	Superseded	Appendix 4 Guidance on automatic overfill protection systems for bulk gasoline storage tanks
26–29	Superseded	Recommendation 3, 4, 5 – Tank overfill defining tank capacity
30–31	Superseded	Recommendation 3, 4, 5 – Fire safe shut off valves
32–35	Superseded	Recommendation 3, 4, 5 – Remotely operated shut-off valves (ROSOVs)
36–37	Superseded	Appendix 4 Guidance on automatic overfill protection systems for bulk gasoline storage tanks
38–39	Superseded	Appendix 5 Guidance for the management of operations and human factors
40	Deleted	Not required in final PSLG report
41	Updated	Part 4 Engineering against loss of secondary and tertiary containment – Introduction
42	Superseded	Recommendation 17, 18 – Bund integrity (leak tightness)
43	Superseded	Recommendation 17, 18 – Fire resistant bund joints

BSTG paragraph reference	Status	PSLG report reference
44	Superseded	Recommendation 17, 18 – Bund capacity
45	Superseded	Recommendation 17, 18 – Tertiary containment
46	Superseded	Recommendation 17, 18 – Firewater management and control measures
47	Updated	Part 5 Operating with high reliability organisations – Introduction
48–57	Superseded	Appendix 5 Guidance for the management of operations and human factors
58	Superseded	Recommendation 11, 12 – Emergency response arrangements
59	Superseded	Recommendation 11, 12 – Principles
60	Superseded	Recommendation 11, 12 – On site emergency plan
61	Superseded	Recommendation 11, 12 – Firefighting planning and preparation
62–63	Deleted	Not required in final PSLG report
64–70	Copied	Recommendation 1 – Systematic assessment of safety integrity levels
71–72	Updated	Recommendation 1 – Systematic assessment of safety integrity levels
73–75	Superseded	Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage tank
76–77	Copied	Recommendation 1 – Incorporating the findings of SIL assessments into COMAH safety reports
78–80	Updated	Part 2 Protecting against loss of primary containment using high integrity systems – Introduction
81	Superseded	Appendix 5 Guidance for the management of operations and human factors
82–119	Copied	Recommendations 3, 4 and 5 – Tank overfill prevention: Defining tank capacity
120–157	Updated	Appendix 5 Guidance for the management of operations and human factors
158	Updated	Part 4 Engineering against loss of secondary and tertiary containment – Introduction
159–160	Updated	Recommendations 17, 18 – Bund Integrity (leak tightness)
161–173	Updated	Recommendations 17, 18 – Fire resistant bund joints
174	Updated	Not required in final PSLG report
175–181	Updated	Recommendations 17, 18 – Fire resistant bund joints
182	Updated	Recommendations 17, 18 – Bund capacity
183	Updated	Recommendations 17, 18 – Firewater management and control measures
184–200	Updated	Recommendations 17 and 18 – Tertiary containment
201	Updated	Part 5 Operating with high reliability organisations – Introduction
202	Updated	Recommendation 19
203–217	Updated	Appendix 5 Guidance for the management of operations and human factors
218–230	Updated	Appendix 5 Guidance for the management of operations and human factors

BSTG paragraph reference	Status	PSLG report reference
231–237	Updated	Appendix 5 Guidance for the management of operations and human factors
238–248	Updated	Appendix 5 Guidance for the management of operations and human factors
249–281	Updated	Appendix 5 Guidance for the management of operations and human factors
282–315	Updated	Appendix 6, paragraphs 1–34
316–317	Deleted	Not required in final PSLG report
318–320	Superseded	Recommendation 9
321–325	Superseded	
326–329	Superseded	Appendix 5 Guidance for the management of operations and human factors
330–335	Superseded	Part 6 Delivering high performance through culture and leadership
336–370	Updated	Appendix 5 Guidance for the management of operations and human factors
Part 4	Deleted	Not required in final PSLG report
Appendix 1	Superseded	Appendix 2 Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage tank
Appendix 2	Copied	Appendix 3 Guidance on defining tank capacity
Appendix 3	Updated	Appendix 5 Guidance for the management of operations and human factors
Appendix 4	Updated	Appendix 5 Guidance for the management of operations and human factors
Appendix 5	Copied	Appendix 5 Guidance for the management of operations and human factors, Annex 1 Process safety performance indicators

Appendix 10 Acknowledgements

PSLG would like to thank the following people for their work in compiling this report:

Steering Group

Tony Traynor (Chairperson)	INEOS
Ian Travers	Health and Safety Executive
Martyn Lyons	Simon Storage, Tank Storage Association representative
Peter Davis	BPA, United Kingdom Onshore Pipeline Operators' Association (UKOPA)
Chris Hunt	United Kingdom Petroleum Industry Association
Steve Elliott	Chemical Industry Association
Richard Clarke	Environment Agency
John Burns	Scottish Environment Protection Agency
Bud Hudspith	UNITE the Union
Jane Lassey	Health and Safety Executive
Alexander Tsavalos	Health and Safety Executive
Colette Fitzpatrick	Health and Safety Executive
Peter Davidson	United Kingdom Petroleum Industry Association

Working Group 1 – Human factors

Joanna Woolf (Chairperson PSLG)	Cogent
Stuart Robinson (Chairperson BSTG)	Health and Safety Executive
Mark Scanlon	Energy Institute
Peter Davis	BPA, United Kingdom Onshore Pipeline Operators' Association (UKOPA)
Alan Findlay	INEOS
Rob Turner	ABB Engineering Services
Bill Gall Kingsley	Management Limited
James Coull	Total
John Wilkinson	Health and Safety Executive
Kevin Smith	Murco
Matt Maudsley	Murco
Peter Jefferies	ConocoPhillips
Walter Williamson	Cogent
Mike Wood	SABIC
Ron Wood	Shell
Steve Walmsley	Shell
Steve Maddocks	Shell
Stephen Clarke	BP
Daryn Smith	BP
James Newey	BP
Tom Dutton	Rhodia
David Kelly	Petroplus

Paul Jobling
Allen Ormond
Craig Garbutt
Kevin Shephard
Glen Knight
Jon Evans
Mike Brown
Linda Dixon
Paul Evans
Fiona Brindley
Peter Mullins
Ron McLeod
John Gilbert
Bud Hudspith

Simon Storage
ABB Engineering Services
Vopak
Vopak
ExxonMobil
ExxonMobil
ExxonMobil
Chevron
Chevron
Health and Safety Executive
Health and Safety Executive
Shell
Kaneb
UNITE the union

Working Group 2 – Scope

Stuart Barlow (Chairperson)
James Fairburn
John Galbraith
Doug Leach
Neil MacNaughton
Kevin Shephard
Ian Wilkinson
Stephen Brown

Health and Safety Executive
Petroplus
SABIC
Chemical Business Association
INEOS
Vopak
Total
BP

Working Group 3 – Control and instrumentation

Jeff Pearson (Chairperson)
Chris Newstead
Dave Ransome
Ian Neve
John Donald
Joulian Douse
Malcolm Tennant
Mark Broom
Martyn Hewitson Griffiths
Neil MacNaughton
Neil Waller
Peter Edwards
Richard Gowland
Richard Tinkler
Rob Ayton
Robert Nicol
Stuart Williamson
Terry Lewis
Colin Chambers
David Carter
Alan King
Paul Baker

Health and Safety Executive
Simon Storage
P & I Design Ltd
Total
Total
Petroplus
MHT Technology
Environment Agency
MHT Technology
INEOS
INEOS
ConocoPhillips
EPSC
ConocoPhillips
Petroplus
Shell
Petroplus
Total
Health and Safety Laboratory
Health and Safety Executive
ABB
ConocoPhillips

Working Group 4 – Secondary and tertiary containment

Mark Maleham (Chairperson)	Environment Agency
Alan Trevelyan	Environment Agency
Felix Nelson	Shell
Rob Walker	Vopak
Danny Carter	Kaneb
Chris Newstead	Simon Storage
Michael Dale	Total
Chris Weston	Health and Safety Executive
Peter Coles	BP
Bruce Mcglashan	Environment Agency
Doug Leech	Chemical Business Association
Graham Neil	Exxon Mobil
Mike Cook	Simon Storage
Jackie Coates	Chemical Industries Association
John Wormald	Total
Helen Fowler	BP
James Fairburn	Petroplus
Ian Goldsworthy	Chevron
Steve Bygrave	INEOS

Working Group 5 – Emergency arrangements

David Pascoe (Chairperson)	Health and Safety Executive
Faye Wingfield	Health and Safety Executive
Bruce McGlashan	Environment Agency
Stuart Warburton	Shell
Sandy Todd	INEOS
Alan Dixon	Simon Storage
Paul MacKay	Kaneb
Stephen Alderson	Vopak
Arnie Arnold	Petroplus
Chris Walkington	ConocoPhillips
David Johnson	Essex Fire and Rescue Service
Mark Samuels	Essex Fire and Rescue Service
Eddie Watts	Chevron
Carl Lamb	Total
Neil Leyshon	BP
Jim Rowsell	Exxon Mobil
Kevin Westwood	BP
Doug Leech	Chemical Business Association
Norman Powell	Cheshire Local Authority
Mike Rogers	SABIC
Steve Richardson	Countrywide Energy
Jeff Watson	United Kingdom Liquefied Petroleum Gas

Working Group 6 – Mechanical integrity

Pauline Hughes (Chairperson)	Health and Safety Executive
David Wilkins	Exxon Mobil, EEMUA representative
Mike Cook	Simon Storage, TSA representative
George Reeves	NuStar Eastham Ltd
Stephen Dray	Chevron Ltd
Nick Wells	SABIC UK Petrochemicals
Robert Baird	BP Oil UK
Mike Nicholas	Environment Agency
Jim Fairbairn	INEOS Manufacturing, Scotland
Brian Hewlett	Vopak
Alan Andrew	Total
Steve Taylor	Total
Norman Woodward	Vopak
Andy McKinnell	Petroplus

Working Group 7 – Coordination

Jane Lassey (Chairperson)	Health and Safety Executive
Alexander Tsavalos	Health and Safety Executive
Colette Fitzpatrick	Health and Safety Executive
Hugh Bray	Tank Storage Association
Ian McPherson	United Kingdom Petroleum Industry Association
Peter Davidson	United Kingdom Petroleum Industry Association
Phil Scott	Chemical Industry Association
Mark Maleham	Environment Agency

Note: Affiliations refer to the time of participation.

References

- 1 *COMAH Competent Authority policy on containment of bulk hazardous liquids at COMAH establishments* HSE/Environment Agency/SEPA 2008 www.environment-agency.gov.uk/static/documents/Business/containmentpolicy_1961223.pdf
- 2 *Recommendations on the design and operation of fuel storage sites* Report HSE 2007 www.buncefieldinvestigation.gov.uk
- 3 *BS 2654:2005 Specification for manufacture of vertical steel welded non-refrigerated storage tanks with butt-welded shells for the petroleum industry* British Standards Institution
- 4 *BS EN 14015:2004 Specification for the design and manufacture of site built, vertical, cylindrical, flat-bottomed, above ground, welded, steel tanks for the storage of liquids at ambient temperature and above* British Standards Institution
- 5 *Design and construction of large, welded, low-pressure storage tanks* API STD 620 (Eleventh edition) American Petroleum Institute 2009
- 6 *Welded tanks for oil storage* API STD 650 (Eleventh Edition) American Petroleum Institute 2008
- 7 *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries* HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0
- 8 *Dangerous substances and explosive atmospheres. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L138 HSE Books 2003 ISBN 978 0 7176 2203 0
- 9 *Reducing error and influencing behaviour* HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2
- 10 *The Buncefield Investigation: Third progress report* Report HSE 2006 www.buncefieldinvestigation.gov.uk
- 11 *BS EN 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems* British Standards Institution
- 12 *Users' Guide to the inspection, maintenance and repair of aboveground vertical cylindrical steel storage tanks* Publication 159 (Third edition) Volumes 1 and 2 Engineering Equipment Materials Users' Association 2003 ISBN 978 0 85931 131 1
- 13 *Overfill protection for storage tanks in petroleum facilities* API RP 2350 (Third edition) American Petroleum Institute 2005
- 14 *BS 6755-2:1987 Testing of valves. Specification for fire type-testing requirements* British Standards Institution

- 15 BS EN ISO 10497:2004 *Testing of valves. Fire type testing requirements* British Standards Institution
- 16 *Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice* HSG244 HSE Books 2004 ISBN 978 0 7176 2803 2
- 17 *International safety guide for oil tankers and terminals* (Fifth Edition) International Chamber of Shipping 2006 ISBN 978 1 85609 292 0
- 18 *Area classification code for installations handling flammable fluids: IP Model Code of Safe Practice Part 15* EI 15 (Third edition) Energy Institute 2005 ISBN 978 0 85293 418 0
www.energyinstpubs.org.uk
- 19 *Dangerous substances and explosive atmospheres. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L138 HSE Books 2003 ISBN 978 0 7176 2203 0
- 20 *Unloading petrol from road tankers. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L133 HSE Books 2003 ISBN 978 0 7176 2197 2
- 21 *Design of plant, equipment and workplaces. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L134 HSE Books 2003 ISBN 978 0 7176 2199 6
- 22 *Storage of dangerous substances. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L135 HSE Books 2003 ISBN 978 0 7176 2200 9
- 23 *Control and mitigation measures. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L136 HSE Books 2003 ISBN 978 0 7176 2201 6
- 24 *Safe maintenance, repair and cleaning procedures. Dangerous Substances and Explosive Atmospheres Regulations 2002. Approved Code of Practice and guidance* L137 HSE Books 2003 ISBN 978 0 7176 2202 3
- 25 *Guide for the prevention of bottom leakage from vertical, cylindrical, steel storage tanks* Publication 183 Engineering Equipment Materials Users' Association 1999 ISBN 978 0 85931 115 1
- 26 *Frangible roof joints for fixed roof storage tanks: Guide for designers and users* Publication 180 Engineering Equipment Materials Users' Association 2007 0 85931 161 9
- 27 *Venting atmospheric and low-pressure storage tanks - Non-refrigerated and refrigerated* API STD 2000 (Fifth edition) American Petroleum Institute 1999
- 28 *Tank inspection, repair, alteration, and reconstruction* API STD 653 (Fourth edition) American Petroleum Institute 2009
- 29 *Integrity of atmospheric storage tanks* SPC/Tech/Gen/35 HSE www.hse.gov.uk/foi/internalops/hid/spc/spctg35.htm
- 30 *Chemical storage tank systems – good practice. Guidance on design, manufacture, installation, operation, inspection and maintenance* C598 CIRIA 2003 ISBN 978 0 86017 598 8
- 31 *Establishing the requirements for internal examination of high hazard process plant* RR729 HSE Books 2009 www.hse.gov.uk/research/rrhtm/index.htm

- 32 *Drainage of floating roof tanks* SPC/Enforcement/163 HSE 2009 www.hse.gov.uk/foi/internalops/hid/spc/spcenf163.htm
- 33 BS 476-10:2009 *Fire tests on building materials and structures. Guide to the principles and application of fire testing* British Standards Institution
- 34 BS 476-20:1987 *Fire tests on building materials and structures. Methods for determination of the fire resistance of elements of construction (general principles)* British Standards Institution
- 35 BS 476-22:1987 *Fire tests on building materials and structures. Methods for determination of the fire resistance of non-loadbearing elements of construction* British Standards Institution
- 36 *The storage of flammable liquids in tanks* HSG176 HSE Books 1998 ISBN 978 0 7176 1470 7
- 37 BS EN 60079-0:2009 *Explosive atmospheres. Equipment. General requirements* British Standards Institution
- 38 *Liquid release prevention and detection measures for aboveground storage tanks* API PUBL 340 American Petroleum Institute 1997
- 39 *A survey of diked-area liner use at aboveground storage tank facilities* API PUBL 341 American Petroleum Institute 1998
- 40 *An experimental investigation of bund wall overtopping and dynamic pressures on the bund wall following catastrophic failure of a storage vessel* RR333 HSE Books 2005 ISBN 0 7176 2988 0
- 41 *Model Code of Safe Practice Part 19: Fire precautions at petroleum refineries and bulk storage installations* Energy Institute 2007 ISBN 978 0 85293 437 1
- 42 *Guidance on the interpretation of major accident to the environment for the purposes of the COMAH Regulations 1999* Defra 1999 ISBN 0 11 753501 X www.defra.gov.uk
- 43 *Design of containment systems for the prevention of water pollution from industrial incidents* R164 CIRIA 1997 ISBN 978 0 86017 476 9
- 44 *Managing fire water and major spillages* Pollution Prevention Guidelines PPG18 Environment Agency www.environment-agency.gov.uk
- 45 *Environmental risk assessment of bulk liquid storage facilities: A screening tool* Energy Institute 2009 ISBN 978 0 85293 393 0 <http://www.energyinstpubs.org.uk/tfiles/1258451689/1310.pdf>
- 46 *Guidance on the environmental risk assessment aspects of COMAH safety reports* www.environment-agency.gov.uk/static/documents/Research/comah_environmental_risk_assessment.pdf
- 47 *The Buncefield Investigation: Second progress report* Report HSE 2006 www.buncefieldinvestigation.gov.uk
- 48 *Environmental guidelines for petroleum distribution installations (Second edition)* Energy Institute 2007 ISBN 978 0 85293 440 1
- 49 *Validity study results for jobs relevant to the petroleum refining industry* API 754 American Petroleum Institute 1972
- 50 'Process safety leading and lagging metrics' Center for Chemical Process Safety 2009 www.aiche.org/ccps

- 51 Maremonti M, Russo G, Slazano E and V Tufano 'Post-accident analysis of vapour cloud explosions in fuel storage areas' *Trans IChemE* 1999 **77** 360-365
- 52 Yuill, J *A discussion on losses in process industries and lessons learned* 51st Canadian Chemical Engineering Conference 2001 <http://psm.chemeng.ca>
- 53 Chang JI and Cheng-Chung L 'A study of storage tank incident' *Journal of loss prevention in the process industries* 2006 19 51-59
- 54 Bai CX, Rusche H and Gosman AD 2002 'Modelling of gasoline spray impingement' *Atomisation and sprays* 12 1-27
- 55 *Recommendations requiring immediate action: Buncefield Standards Task Group (BSTG) Initial report* Report HSE 2006 <http://www.hse.gov.uk/comah/buncefield/bstg1.htm>
- 56 *Safety and environmental standards for fuel storage sites: Buncefield Standards Task Group (BSTG) Final report* Report HSE 2007 <http://www.hse.gov.uk/comah/buncefield/final.htm>
- 57 *Layer of protection analysis: Simplified process risk assessment* Center for Chemical Process Safety 2001 ISBN 978 0 8169 0811 0
- 58 *Reducing risks, protecting people: HSE's decision-making process* HSE Books 2001 ISBN 978 0 7176 2151 4 www.hse.gov.uk/risk/theory/r2p2.htm
- 59 *Buncefield explosion mechanism Phase 1: Volumes 1 and 2* RR718 HSE 2009 www.hse.gov.uk/research/rrhtm/index.htm
- 60 *The precautionary principle: Policy and application* Interdepartmental Liaison Group on Risk Assessment 2002 www.hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm
- 61 *Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)* SPC/Permissioning/12 HSE www.hse.gov.uk/comah/circular/perm12.htm
- 62 *A guide to the Control of Major Accident Hazards Regulations 1999 (as amended)*. Guidance on Regulations L111 HSE Books 2006 ISBN 978 0 7176 6175 6
- 63 *Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal* IPPC H1 Version 6 July 2003
- 64 *COMAH safety reports: Technical policy lines to take for predictive assessors* SPC/Permissioning/11 HID Semi Permanent Circular HSE 2007 www.hse.gov.uk/foi/internalops/hid/spc/spcperm11.pdf
- 65 *The implications of dispersion in low wind speed conditions for quantified risk assessment* CRR133 HSE Books 1997 ISBN 978 0 7176 1359 5
- 66 *Lees' loss prevention in the process industries: Hazard identification, assessment and control* (Third Edition) Elsevier 2005 ISBN 978 0 7506 7555 0
- 67 *Ignition probability review, model development and look-up correlations* Research Report Energy Institute 2006 ISBN 978 0 85293 454 8 www.energyinstpubs.org.uk
- 68 *A risk-based approach to hazardous area classification* Energy Institute 1998 ISBN 0 85293 238 3 www.energyinstpubs.org.uk

- 69 *Decompression risk factors in compressed air tunnelling: Options for health risk reduction* CRR203 HSE Books 1998 ISBN 978 0 7176 1650 3
- 70 *A review of layers of protection analysis (LOPA) analyses of overfill of fuel storage tanks* RR716 HSE Books 2009 www.hse.gov.uk/research/rrhtm/index.htm
- 71 *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* NUREG/CR-1278 August 1983
- 72 *Alarm Systems: A guide to design, management and procurement* EEMUA 191 (Second edition) Engineering Equipment Materials User's Association 2007 ISBN 978 0 85931 155 7
- 73 *Principles for proof testing of safety instrumented systems in the chemical industry* CRR428 HSE Books 2002 ISBN 978 0 7176 2346 4
- 74 *The Report of the BP US Refineries Independent Safety Review Panel* January 2007 (The Baker Panel Report)
- 75 Weick KE and Sutcliffe KM *Managing the unexpected: Assuring high performance in an age of complexity* John Wiley and Sons Ltd 2001 ISBN 978 0 7879 5627 1
- 76 *Investigation report: Refinery explosion and fire* Report No 2005-04-I-TX U.S. Chemical Safety and Hazard Investigation Board 2007 www.csb.gov/assets/document/CSBFinalReportBP.pdf
- 77 *Safety Culture* Human Factors Briefing Note No 7 www.hse.gov.uk/humanfactors/briefingnotes.htm
- 78 *Leadership for the major hazard industries* Leaflet INDG277(rev1) HSE Books 2004 (single copy free or priced packs of 15 ISBN 978 0 7176 2905 3) www.hse.gov.uk/pubns/indg277.pdf
- 79 *A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit* RR367 HSE Books 2005 ISBN 978 0 7176 6144 2
- 80 *Involving employees in health and safety: Forming partnerships in the chemical industry* HSG217 HSE Books 2001 ISBN 978 0 7176 2053 1
- 81 Center for Chemical Process Safety *Guidelines for risk based process safety* WileyBlackwell 2007 ISBN 978 0 470 16569 0
- 82 *Process safety management systems SPC/TECH/OSD/13* HSE| <http://www.hse.gov.uk/foi/internalops/hid/spc/spctosd13.htm>
- 83 *Safety report assessment guide: Highly flammable liquids – Criteria* HSE www.hse.gov.uk/comah/sraghfl/index.htm
- 84 *The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board Volume 1* Report HSE Books 2008 ISBN 978 0 7176 6270 8 www.buncefieldinvestigation.gov.uk
- 85 *Competence assessment for the hazardous industries* RR086 HSE Books 2003 ISBN 0 7176 2167 5 www.hse.gov.uk/research/rrhtm/index.htm
- 86 Hopkins A *Lessons from Longford: The Esso gas plant explosion* CCH Australia Ltd 2000 ISBN 978 1 86468 422 3
- 87 *Training and competence* Human Factors Briefing Note No 7 Energy Institute 2003 www.energyinst.org.uk/humanfactors/bn

- 88 *Process plant control desks utilising human-computer interfaces: A guide to design, operational and human interface issues* EEMUA 201 (Second edition) Engineering Equipment Materials User's Association 2009 ISBN 978 0 85931 167 0
- 89 *Successful health and safety management* HSG65 (Second edition) HSE Books 1997 ISBN 978 0 7176 1276 5
- 90 *Competence* Human Factors Briefing Note No 2 HSE 2005
www.hse.gov.uk/humanfactors/briefingnotes.htm
- 91 *Competence assurance* Core Topic 1 HSE 2005
www.hse.gov.uk/humanfactors/topics/core1.pdf
- 92 *Developing and maintaining staff competence* Railway Safety Publication 1 (Second edition) Office of Rail Regulation 2007 www.rail-reg.gov.uk/upload/pdf/sf-dev-staff.pdf
- 93 *Assessing the safety of staffing arrangements for process operations in the chemical and allied industries* CRR348 HSE Books 2001 ISBN 978 0 7176 2044 9
- 94 *Managing shift work: Health and safety guidance* HSG256 HSE Books 2006 ISBN 978 0 7176 6197 8
- 95 *Investigation Report: Refinery explosion and fire, BP Texas City* Report 2005-04-1-TX US Chemical Safety and Hazard Investigation Board 2007
<http://www.csb.gov/assets/document/CSBFinalReportBP.pdf>
- 96 Horne JA and Reyner LA 'Vehicle accidents related to sleep: A review' *Occupational and Environmental Medicine* 1999 56 (5) 289–294
- 97 *Safe Staffing Arrangements – User guide for CRR348/2001 Methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated plant and/or equipment* Energy Institute 2004 ISBN 0 85293 411 4
www.energyinst.org.uk/humanfactors/staffing
- 98 *Managing Fatigue Risks* HSE Human Factors Toolkit: Specific Topic 2
www.hse.gov.uk/humanfactors/comah/specific2.pdf (unavailable)
- 99 *Managing fatigue in the workplace: A guide for oil and gas industry supervisors and occupational health practitioners* OGP Report 392 OGP/IIPECA 2007 www.ogp.org.uk/pubs/392.pdf
- 100 *The development of a fatigue/risk index for shiftworkers* RR446 HSE Books 2006
www.hse.gov.uk/research/rrhtm/index.htm
- 101 *Improving alertness through effective fatigue management* Energy Institute 2006 ISBN 978 0 85293 460 9 www.energyinst.org.uk/humanfactors/fatigue
- 102 *Human factors: Safety critical communications* HSE
www.hse.gov.uk/humanfactors/topics/communications.htm
- 103 *Organisational change and major accident hazards* Chemical Information Sheet CHIS7 HSE Books 2003 www.hse.gov.uk/pubns/comahind.htm
- 104 *Licensee use of contractors and 'intelligent customer capability* Technical Assessment Guide T/AST/049 Issue 3 HSE 2009
http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast049.htm

- 105 *Contractorisation Technical Assessment Guide T/AST/052* HSE 2002
www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast052.pdf
- 106 *Managing contractors: A guide for employers. An open learning booklet* HSG159
HSE Books 1997 ISBN 978 0 7176 1196 6
- 107 *The use of contractors in the maintenance of the mainline railway infrastructure: A report by the Health and Safety Commission May 2002* Report HSC 2002
www.rail-reg.gov.uk/upload/pdf/contrail.pdf
- 108 *Health and safety management systems interfacing* Step Change in Safety 2003
<http://stepchangeinsafety.net/stepchange/>
- 109 *Management of Change* UKPIA Ltd Self Assessment Module 1 and Appendix 1
www.ukpia.com
- 110 *Initial report to the Health and Safety Commission and the Environment Agency of the investigation into the explosions and fires at the Buncefield oil storage and transfer depot, Hemel Hempstead, on 11 December 2005: Buncefield Major Incident Investigation Board* HSE 2006
www.buncefieldinvestigation.gov.uk
- 111 *Revitalising procedures* HSE www.hse.gov.uk/humanfactors/topics/procinfo.pdf
- 112 BS EN ISO 11064: Parts 1-7 *Ergonomic design of control centres* British Standards Institution
- 113 *Alarm handling* Human Factors Briefing Note No 2 Energy Institute 2003
www.energyinst.org.uk/humanfactors/bn
- 114 *Alarm handling* HSE Human Factors Briefing Note No 9 HSE
<http://www.hse.gov.uk/humanfactors/briefingnotes.htm>
- 115 *Better alarm handling in the chemical and allied industries* Chemical Information Sheet CHIS6
HSE Books 2000 www.hse.gov.uk/pubns/comahind.htm
- 116 *Guidance on safety performance indicators: A companion to the OECD guiding principles for chemical accident prevention, preparedness and response* OECD 2003 ISBN 978 9 2640 1910 2
<http://www2.oecd.org/safetyindicators>
- 117 *Human factors in accident investigations* Core topic 2 HSE 2005
www.hse.gov.uk/humanfactors/topics/core2.pdf
- 118 *Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents* Energy Institute May 2008 ISBN 978 0 85293 521 7
www.energyinst.org.uk/humanfactors/incidentandaccident
- 119 Center for Chemical Process Safety *Guidelines for auditing process safety management systems* WileyBlackwell 1993 ISBN 978 0 8169 0556 8
- 120 Center for Chemical Process Safety *Guidelines for technical management of chemical process safety* American Institute of Chemical Engineers 1989 ISBN 978 0 8169 0423 5
- 121 *Preparing safety reports: Control of Major Accident Hazards Regulations 1999 (COMAH)* HSG190 HSE Books 1999 ISBN 978 0 7176 1687 9
- 122 *Major accident prevention policies for lower-tier COMAH establishments* Chemical Information Sheet CHIS3 HSE Books 1999 www.hse.gov.uk/pubns/comahind.htm

- 123 *Emergency response and recovery: Non statutory guidance accompanying The Civil Contingencies Act 2004* (Second edition) The Cabinet Office 2009
<http://www.cabinetoffice.gov.uk/ukresilience/response.aspx>
- 124 *Dealing with disasters together* Guidance The Scottish Government 2003
- 125 *Health and Safety at Work etc Act 1974* (c.37) The Stationery Office 1974
ISBN 978 0 10 543774 1
- 126 *Management of health and safety at work. Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and guidance L21* (Second edition) HSE Books 2000 ISBN 978 0 7176 2488 1
- 127 *HID CI/SI inspection manual. Assessing risk control systems. Guidance: On-site emergency emergency response inspection* RCS8 para 41 HSE 2001
<http://www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf>
- 128 *Model Code of Safe Practice Part 19: Fire precautions at petroleum refineries and bulk storage installations* (Second edition) Energy Institute 2007 ISBN 978 0 85293 437 1
www.energyinstpubs.org.uk duplicate @ref 41
- 129 *Controlled burn* Pollution Prevention Guidelines PPG28 Environment Agency 2007
www.environment-agency.gov.uk
- 130 *Communities and Local Government Fire and Rescue Manual Volume 2: Environmental Protection* The Stationery Office 2008 ISBN 978 0 11 341316 4
- 131 *Hertfordshire Fire and Rescue Service Buncefield: Hertfordshire Fire and Rescue Service's review of the fire response* The Stationery Office 2006 ISBN 978 0 11 703716 8

Abbreviations

ACOP	Approved Code of Practice
ALARP	As low as reasonably practicable
AIChE	American Institution of Chemical Engineers
AMN	All measures necessary
API	American Petroleum Institute
APJ	Absolute probability judgment
ARAMIS	European Commission on Accidental Risk Assessment Methodology for Industries
ASM	Abnormal situation management
ATG	Automatic tank gauging
BAT	Best available technology
BPCS	Basic process control system
BPCF	Basic process control function
BSTG	Buncefield Standards Task Group
CA	Competent Authority
CAP-EPLG	Chemical and pipelines emergency planning liaison group
CCPS	(US) Center for Chemical Process Safety
CIA	Chemical Industries Association
CIRIA	Construction Industry Research and Information Association
CM	Conditional modifier
CMS	Competence management system
COMAH	Control of Major Accident Hazards Regulations
CSB	(US) Chemical Safety Board
DCS	Distributed control system
DETR	Department of the Environment, Transport and the Regions
DRA	Dynamic risk assessment
DSEAR	Dangerous Substances and Explosive Atmospheres Regulations 2002
ECC	Emergency control centre
EEMUA	Engineering Equipment Materials Users' Association
EPC	Error Producing Condition
EPRR	Emergency preparedness and response report
ERP	Emergency response plan
FMEA	Failure modes and effects analysis
FMP	Fatigue management plan
FRS	Fire and Rescue Service
HAZID	Hazard identification
HAZOP	Hazard and operability study
HCI	Human-computer interface
HEART	Human error assessment and reduction technique
HEP	Human error probability
HFL	Highly flammable liquids

HSC	Health and Safety Commission
HSE	Health and Safety Executive
HSI	Human-system interface
HSL	Health and Safety Laboratory
ICT	Incident control team
IPL	Independent protection layers
ISGOTT	International Safety Guide for Oil Tankers and Terminals
LAH	Level alarm high
LAHH	Level alarm high-high
LOPA	Layer of protection analysis
MAPP	Major accident prevention policy
MATTE	Major accident to the environment
MIIB	Buncefield Major Incident Investigation Board
MIMAH	Methodology for identification of major accident hazards
MOC	Management of change
MTTR	Mean time to repair
NIA	Nuclear Industry Association
NOS	National Occupational Standard
NVQ	National Vocational Qualification
OECD	Organisation for Economic Co-operation and Development
ORR	Office of Rail Regulation
PFD	Probability of failure on demand
PHA	Process hazard analysis
PPE	Personal protective equipment
PSA	Process safety analysis
PSF	Performance shaping factor
PSLG	Process Safety Leadership Group
PSMS	Process safety management system
QRA	Quantitative risk analysis
RBI	Risk-based inspection
RCS	Risk control system
ROSOV	Remotely operated shut-off valve
ROV	Remotely operated valve
RVP	Reed vapour pressure
SCADA	Supervisory control and data acquisition
SEPA	Scottish Environment Protection Agency
SG	Specific gravity
SIC	Site incident controller
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SMC	Site main controller
SMS	Safety management system
SRAG	Safety report assessment guide
SRS	Safety requirement specification
SVQ	Scottish Vocational Qualification

THERP	Technique for human error rate prediction
TRC	Tank rated capacity
TSA	Tank Storage Association
TWI	The Welding Institute
UKOPA	United Kingdom Onshore Pipeline Operators' Association
UKPIA	United Kingdom Petroleum Industry Association
VCE	Vapour cloud explosion

Further information

HSE priced and free publications can be viewed online or ordered from www.hse.gov.uk or contact HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 Fax: 01787 313995. HSE priced publications are also available from bookshops.

For information about health and safety ring HSE's Infoline Tel: 0845 345 0055 Fax: 0845 408 9566 Textphone: 0845 408 9577 e-mail: hse.infoline@natbrit.com or write to HSE Information Services, Caerphilly Business Park, Caerphilly CF83 3GG.

British Standards can be obtained in PDF or hard copy formats from BSI: <http://shop.bsigroup.com> or by contacting BSI Customer Services for hard copies only Tel: 020 8996 9001 e-mail: cservices@bsigroup.com.

The Stationery Office publications are available from The Stationery Office, PO Box 29, Norwich NR3 1GN Tel: 0870 600 5522 Fax: 0870 600 5533 e-mail: customer.services@tso.co.uk Website: www.tso.co.uk (They are also available from bookshops.) Statutory Instruments can be viewed free of charge at www.opsi.gov.uk.

Safety and environmental standards for fuel storage sites

Process Safety Leadership Group
Final report

£11.95

ISBN 978-0-7176-6386-6



9 780717 663866

CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Process Safety Leadership Group – Other
Products in Scope

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members a guideline and screening methodology for assessing the risk from other products within the scope of the Process Safety Leadership group (PSLG) final report.

It is not the intention of this document to specify the risk assessment process, nor replace any existing corporate policies or processes. The intent is to provide a reference for those organisations storing the products defined within the scope of appendix 1 of the final PSLG report, and provide the means by which effective and efficient risk assessment can be performed.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to the risk assessment of other products defined within the scope of the PSLG final report.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – PSLG Other Products in Scope".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

This guidance is not intended to be an authoritative interpretation of the law; however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for the risk assessment of other products within the scope of the final PSLG report, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

FOREWORD	2
CONTENTS.....	3
1 EXECUTIVE SUMMARY	4
2 SCOPE	5
3 REFERENCE DOCUMENTS AND KEY GUIDANCE	6
3.1 PSLG final report	6
3.2 Health and Safety Laboratory (HSL) Research Report ‘RR908 Vapour cloud formation: Experiments and modelling’	6
3.3 Explosion mechanism phase 2	6
3.4 Containment Policy (CP).....	6
3.5 CA agreement on the nature and architectures of overfill prevention systems.....	6
3.6 Chemical and Downstream Oil Industry Forum (CDOIF).....	7
4 SCREENING METHODOLOGY	8
5 GENERIC PARAMETERS AND DATA.....	9
5.1 Threat lines	9
5.2 Misalignment.....	10
5.3 Failure to terminate	11
5.4 Ullage	12
5.5 Mechanical failures	13
5.6 Barriers and probability of failure on demand (PFD).....	15
5.6.1 Operating Procedures used as Barriers	16
ABBREVIATIONS.....	18
ACKNOWLEDGEMENTS.....	19
REVISION HISTORY.....	20
APPENDIX 1 – VAPOUR CLOUD FORMATION CALCULATION	21

1 Executive summary

The final report of the Process Safety Leadership Groups (PSLG) safety and environmental standards for fuel storage sites was published in December 2009.

Since publication, duty holders have been completing detailed risk quantification against the guidance provided in Appendix 2 of the report, for the scenario of over topping a finished gasoline tank which has the same or similar characteristics as tank 912 at Buncefield (as defined in paragraph 24 of the PSLG report):

- those storing gasoline (petrol) as defined in Directive 94/63/EC European Parliament and Council Directive 94/63/EC of 20 December 1994 on the control of volatile organic compound emissions resulting from the storage of petrol and its distribution from terminals to service stations;
- vertical, cylindrical, non-refrigerated, above-ground storage tanks typically designed to standards BS 2654,3 BS EN 14015,4 API 620,5 API 6506 (or equivalent codes at the time of construction);
- with side walls greater than 5 m in height; and
- filled at rates greater than 100 m³/hour (this is approximately 75 tonnes/hour of gasoline).

The Competent Authority (CA) has reviewed the risk assessments, and in the vast majority of cases these have been agreed, Safety Integrity Levels (SIL) identified, and implementation plans submitted. In many instances the overfill protection systems have already been installed.

The purpose of this guidance is to draw on the experience of both the CA and Duty Holders in completing risk assessments for finished gasoline storage tanks, and propose a screening methodology that can be adopted to simplify and expedite the assessment of other products (as defined in appendix 1 of the final PSLG report) which may give rise to the formation of a flammable vapour cloud.

It is not the intention of this document to replace the guidance provided in the final PSLG report, but instead provide a methodology for simplifying the risk assessment process for 'other products' based on the knowledge and feedback from the assessment of finished gasoline. The CA and Duty Holder should continue to reference the guidance provided by the final PSLG report when determining what measures may be required to reduce the risk of an overfill from other product tanks.

This guidance also takes into account the research report published by the Health and Safety Laboratory (HSL) 'RR908 Vapour cloud formation: Experiments and modelling', which has the potential to influence the other products in scope, and the parameters considered when performing a risk assessment.

2 Scope

This document provides guidance and a screening methodology to assist duty holders and the CA in the risk assessment of other products in scope of the final PSLG report.

Other products are identified as follows:

Substances considered likely to form a large vapour cloud
Acetone
Benzene
Crude Oils ¹
Raw Gasoline
Methyl ethyl ketone
Naphthas
Reformate (worse case – light)
Natural gas liquids (condensate)
Methyl tert-butyl ether
Iso Pentane
Special boiling point solvent 2
Toluene

All tanks storing the products identified above are subject to the scope criteria as defined in paragraph 24 of the final PSLG report.

Note¹ – the crude oils considered in scope are subject to paragraph 6 of the PSLG final report appendix 1

Note: Some of these products may be screened out of scope, following an assessment using the Health and Safety Laboratory (HSL) research report RR908, 'Vapour cloud formation: Experiments and modelling'. Refer to section 3.2 and Appendix 1 for further information.

3 Reference documents and key guidance

3.1 PSLG final report

In the first instance, reference should be made to the PSLG final report appendix 2 for guidance on completing risk assessments for the scenario of overfilling a PSLG in-scope tank.

3.2 Health and Safety Laboratory (HSL) Research Report 'RR908 Vapour cloud formation: Experiments and modelling'

This research report focuses mainly on what happens at the base of a tank during a cascade, the predictive methods that can be adopted for calculating evaporation of the material, and recommending dilution factors that can be applied.

In support of the research report, a simple calculation methodology has been developed to help to determine the range and nature of a flammable vapour cloud over time. This has an influencing factor over the risk assessments that need to be performed; some products may no longer be in scope (for example Toluene and some grades of crude oil).

Reference should be made to Appendix 1 for a simple evaluation tool to help in determining the properties of vapour cloud formation for in-scope products.

3.3 Explosion mechanism phase 2

There is an on-going project which is looking at the explosion mechanism from Buncefield. Those completing risk assessments should pay close attention to the results of this work as it may influence any assessments that are performed, specifically:

- The actual explosion mechanism, for example whether this is from flame acceleration through trees and undergrowth, or acceleration due to leaf and other debris at the front of the flame
- The distances that should be considered when performing a risk assessment (PSLG states two zones at a radius of 250m and 400m from the base of the tank)

3.4 Containment Policy (CP)

Those products within scope of the PSLG are defined in Appendix 1 of the final report. The scope of the Containment Policy is defined in part 2 of the policy. These may not include the same products, for example crude oil is in scope for PSLG and out of scope for containment policy. Implementation of the PSLG scope does not bring those products into the scope of the containment policy, unless they are already included.

3.5 CA agreement on the nature and architectures of overfill prevention systems

Following completion of the risk assessment, when considering the installation of overfill protection to other products and the architecture and nature of these systems, reference should be made to the alternative measures cited in the report, particularly in relation to the use of operators:

‘Those that include an operator(s) as part of the overfill prevention system must demonstrate that the reliability and availability of that operator(s) can be adequately supported to undertake the necessary control actions to prevent an overfill without compromising the ALARP outcome. Operator involvement should be properly managed, monitored, audited and reviewed on an on-going basis. The CA is unlikely to accept that an operator can be included in a system rated above Safety Integrity Level (SIL) 1 within BS EN 61511-1’

UKPIA has published guidance and an assessment methodology to help duty holders in reviewing the requirements and minimum standards for the use of operators as part of a SIL1 Safety Instrumented System (SIS). More information can be found here: <http://www.ukpia.com/process-safety/tools/self-assessment-tools.aspx> in the section “Understand Hazards and Risks”.

3.6 Chemical and Downstream Oil Industry Forum (CDOIF)

There are three projects that are currently under consideration by CDOIF which may influence the outcome of the risk assessments, or design of overfill prevention systems. These are:

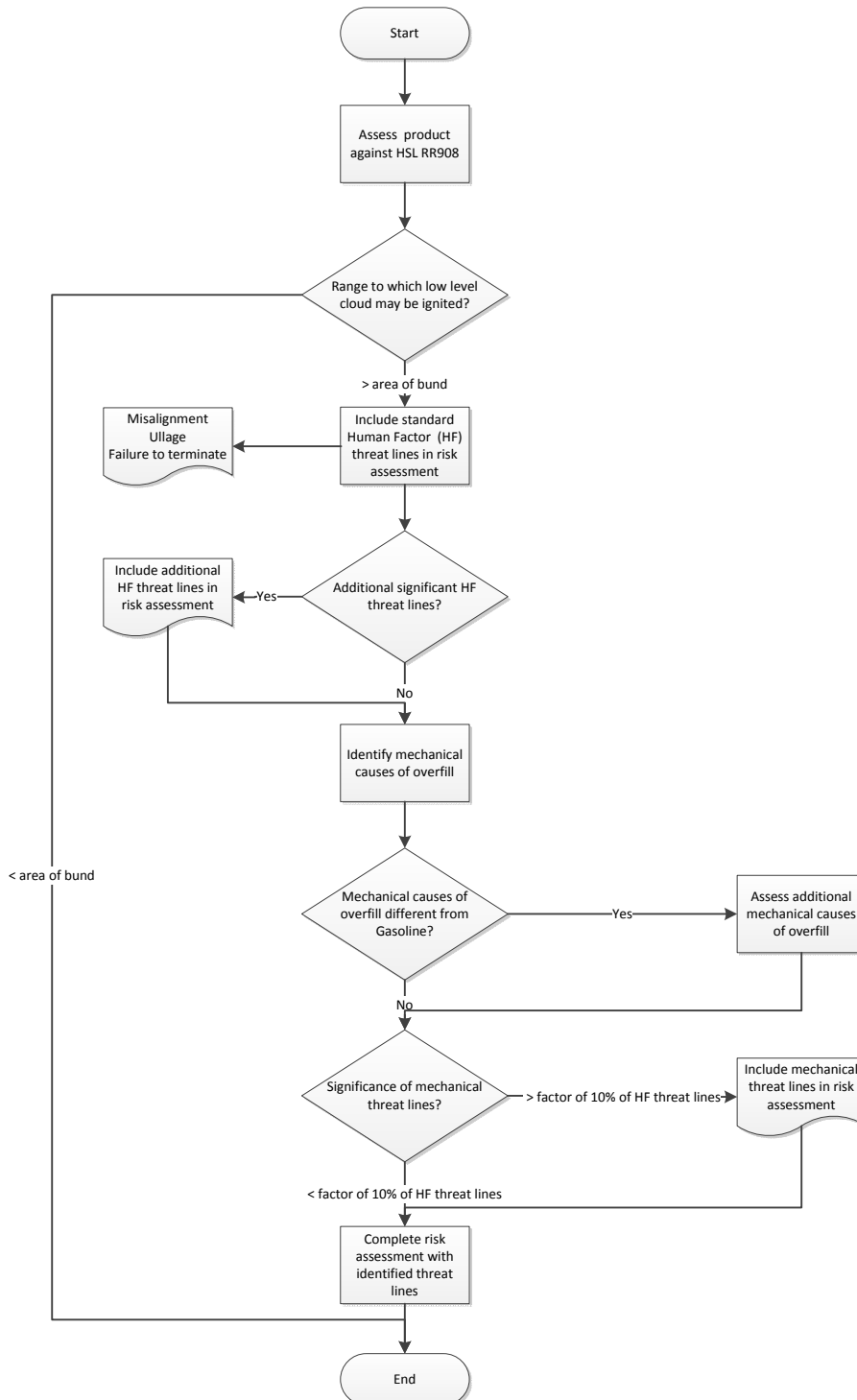
- Environmental Risk Assessment
- Leak Detection
- Prior Use – suitability of existing equipment to form part of the Safety Instrumented Function

The output of the environmental risk assessment working group may influence the need for, and target SIL levels of overfill protection systems. The leak detection work group may provide alternative means (or mitigation layer) that could be employed to reduce the risk of a vapour cloud explosion to a tolerable level, thus also influencing the need for, and target SIL levels of overfill protection systems.

Where the need for a SIL rated overfill protection system has been identified, the Prior Use guidance can be adopted when determining the suitability of existing equipment to form part of the Safety Instrumented Function.

4 Screening methodology

The following flowchart provides a simple screening methodology to assist in the development of risk assessments for other products within the scope of the final PSLG report. Reference should be made to section 5 of this guidance where additional information is provided on the selection of generic data which may be applied to relevant threat lines and barriers.



5 Generic parameters and data

5.1 Threat lines

To justify the Human Error Probabilities (HEP)'s for operators performing critical tasks during the transfer of other in scope substances as described in this guidance, it is expected that good practice be implemented. Good practice with regard to sites that come under the scope of this guidance is described in the PSLG report, 'Safety and environmental standards for fuel storage sites'. Specific guidance on incorporating human error in initiating events is given in appendix 2; annex 7 of the PSLG report.

For those processes that are similar to those for finished gasoline (for example the same operators carrying out the same type of basic activities, who are suitably trained and have the necessary operational experience and are familiar with the process) then the error probabilities suggested in the following sections may be used, as task analysis has already been completed for finished gasoline. Where different HEPs are used, these should be justified.

For those processes that are not similar to finished gasoline, it is suggested that the following risk controls contribute towards good practice and should be in place as a minimum before the human error probabilities suggested in the following sections can be applied.

- Perform a task analysis of all relevant critical tasks relating to an overflow event.
- Perform human error analysis to identify what could go wrong with each critical task and how to detect and deal with this.
- Have sufficiently detailed procedures covering all relevant aspects of the transfer of other in-scope substances.
- Perform training in the task(s) to be performed, including refresher training.
- Demonstrate, periodically, operator competence in the tasks to be performed.
- Determine that the operator has no other demands on their time that could limit their ability to safely perform the required tasks.
- Perform periodic operational audit (functional test) for critical tasks.
- Monitor critical operator tasks over time (trending).
- Provide an audit trail / records for all of the above.

Note: When completing risk assessments, consideration can be given to operational cross-checks of the tank levels which may provide an additional layer of protection thus further reducing the risk of an overfill. See PSLG final report, appendix 2, annex 6 for further guidance on cross-checks.

5.2 Misalignment

Misalignment refers to the threat that an operator has incorrectly lined up the receiving tank with the discharging tank – the wrong tank will be filled.

Alignment of sending and receiving tanks can be carried out by either a control room operator via the control system, or by a local operator via local control panel or manual valve(s).

The following logic can be used when selecting the number of failures of tank alignments (or critical step).

IF	The control room or local operator carries out the operation (or critical step) on a routine basis (it is a regular task), and the operator can be demonstrated to be competent in carrying out that task OR The task (or critical step) is not routine, but there is a detailed procedure in place (requiring confirmation of steps completed), and the operator can be demonstrated to be competent in carrying out the task
THEN	Assume a failure of 1/1000 tank alignment operations
OTHERWISE	Assume a failure of 1/100 tank alignments operations ¹

Note¹ – further detailed analysis of the critical step may be required where tasks are not routine, and where there are specific and unusual site requirements for carrying out the task.

5.3 Failure to terminate

Failure to terminate refers to the threat that an operator fails to terminate a transfer of product, resulting in overfill.

This threat line applies to any tank (containing product within the scope of the PSLG final report) which goes through a fill and empty cycle. It may not apply to tanks which are continuously fed (for example run-down tanks).

The following logic can be used when selecting the number of failures to terminate a transfer (or critical step)¹.

IF	The control room or local operator carries out the operation (or critical step) on a routine basis (it is a regular task), and the operator can be demonstrated to be competent in carrying out that task OR The task (or critical step) is not routine, but there is a detailed procedure in place (requiring confirmation of steps completed), and the operator can be demonstrated to be competent in carrying out the task
THEN	Assume a failure to terminate the transfer of 1/1000 tank fill cycles
OTHERWISE	Assume a failure to terminate the transfer of 1/100 tank fill cycles ²

Note¹ – Consideration should be given to ship-fed transfers, which may require more than one action to terminate the transfer.

Note² – further detailed analysis of the critical step may be required where tasks are not routine, and where there are specific and unusual site requirements for carrying out the task.

5.4 Ullage

Ullage refers to the threat that an operator incorrectly specifies the flow rate or 'fill' time of the transfer, or the operator incorrectly determines the Ullage, resulting in the potential over-filling of the receiving tank.

Note: this threat line may not be relevant where Ullage calculations are performed in conjunction with other departments, such as planning, accounts.

Ullage calculations can be performed for either batch transfers of product, or where a continuous flow of product is required to maintain the level in a receiving tank.

The following logic can be used when selecting the number of failures to correctly enter either a flow rate or 'fill' time as part of a transfer (or critical step)¹.

IF	The control room or local operator carries out the operation (or critical step) on a routine basis (it is a regular task), and the operator can be demonstrated to be competent in carrying out that task OR The task (or critical step) is not routine, but there is a detailed procedure in place (requiring confirmation of steps completed), and the operator can be demonstrated to be competent in carrying out the task
THEN	Assume a failure to correctly enter flow rate or 'fill' time of 1/1000 tank fill cycles
OTHERWISE	Assume a failure to correctly enter flow rate or 'fill' time of 1/100 tank fill cycles ²

Note¹ – Where the receiving tank level is maintained under service, particular attention should be drawn to the integrity of the level gauge (which can highlight unexpected variations in level). Further additional analysis may be required based on the fill rate, for example identification of what could cause overflow, and over what duration this could occur.

Note² – further detailed analysis of the critical step may be required where tasks are not routine, and where there are specific and unusual site requirements for carrying out the task.

5.5 Mechanical failures

Mechanical failures can occur to such equipment as Automatic Tank Gauging (ATG) systems, flow-meters, pumps or Remotely Operated Solenoid Valves (ROSV's).

With reference to the screening methodology in section 4, where this equipment is considered to contribute significantly to the threat of overfill (greater than a factor 10% of the human factors related initiating event frequency, which was not the case for any of the PSLG LOPAs on Finished Gasoline which were filled via a batch process),

OR

Where the mechanical failures of equipment is considered to be different to that assessed for finished gasoline (for example, the equipment, architecture or service is significantly different), then any additional mechanical causes of overfill should be assessed, in accordance with the guidance provided by the final PSLG report.

For equipment that is not considered to contribute significantly to the threat of overfill (less than a factor 10% of the human factors related initiating event frequency), and where the equipment is not significantly different from that used for finished gasoline, no further detailed assessment should be required.

When considering the failure rate data for the equipment installed, this should be obtained from appropriate sources.

The best and most appropriate information comes from the operational experience of the end user.

Where an end user has no operational experience of a new item of equipment, there are other sources of failure data that might be considered. These may include:

- Manufacturers failure rate data
- Generic failure rate data, from sources such as EEMUA, FARADIP, OREDA etc.

However, great care should be taken when using either of these alternative sources to gain failure rate information for *existing* equipment. Firstly, manufacturers will almost certainly have no direct experience of the use of the items under conditions similar to those of the end user. Furthermore, the data provided by manufacturers is often simply a synthesised prediction of performance that they are hoping for from the product.

Secondly, with the generic failure rates to be found in databases, there is no guarantee that the component that the end user is considering will be similar in performance to the database figure. Any use of generic data should have appropriate justification for its appropriateness and should be regarded as a provisional figure until real experience is available to support or reject the figure.

Preferentially end users own failure data should be used to calculate failure rates. Further information can be found in Appendix 1 of the CDOIF guideline 'Demonstrating prior use'.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Note that for new installations of equipment, it is likely that manufacturer's failure rate data will be used; this should be analysed as part of the design process, to ensure that required risk reduction (for the layer of protection in question) has been achieved.

5.6 Barriers and probability of failure on demand (PFD)

Based on the risk assessments completed and accepted by the CA for finished gasoline, the following typical data may be adopted when completing risk assessments for other products within the scope of the PSLG final report.

Parameter	Value	Comments
CM1	-	Probability of ignition, based on site (and off-site where relevant) specific data
CM2	1	Probability of explosion after ignition, however this will be influenced by the HSL research report RR908 which may screen out some products, and the work of the Phase 2 explosion mechanism (refer to section 3.3).
CM3	-	Weather conditions, based on site specific data, but may be re-used from the calculations performed for finished gasoline
CM4	-	Probability that a person(s) in the explosion zone, based on site specific data
CM5	1	Probability of fatality in the explosion zone
IPL1 – Operator Cross-checks	0.1	Operational cross-checks of the tank levels, see below for definition.
IPL2 – Alarm & Operator Response	0.1	The barrier is “Alarm and Operator Response”, i.e. an alarm in a manned location and an operator responding to the alarm. See below regarding assurance required for the operator to have a PFD of 0.07. The PFD of the rest of the system (i.e. field instrument, data processing and transfer and the audible/visual alarm) is assumed to be less than 0.03 provided that good management control and maintenance of the system can be demonstrated
IPL3 - IHHA	0.1	Independent Protection Layer (IPL) provided by an independent high high alarm system. If a Safety Related SIL 1 system is used as this IPL using an operator, then the system should conform to the UKPIA SIL1 Human Factors criteria.

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Parameter	Value	Comments
IML1	-	Consideration may be given to an additional Independent Mitigation Layer (IML) such as leak detection. Further reference should be made to the CDOIF guideline 'Leak detection'

5.6.1 Operating Procedures used as Barriers

The "Operational Cross-Check" procedure involves the expected level being manually calculated on a regular basis using the feed rate and/or monitoring the level in another tank going down. This calculated value is cross-checked against the level indication of the tank being filled. If the anticipated change in level is not in line with the level indication of the tank that is filling then predefined and specific actions shall be undertaken (e.g. checking the level indication by measurements in the field or redirecting the rundown to an alternative tank with sufficient ullage). This system allows for both a faulty instrument and for errors in the original line-up to be detected. The checks of the level indication with the calculated level need to be performed at regular intervals (e.g. an hour after the start of the tank filling and every 3-4 hours thereafter).

The "**Alarm and Operator Response**" barrier involves a well defined response to a maintained tank level alarm (i.e. a high level alarm).

To ensure these operational barriers are effective, there should be in place tank operating procedures which include the following elements (or similar):

- a. Be clearly written, kept current and required to be used by the operator.
- b. Set requirements for periodic maintenance and validation to confirm correct tank gauge operation.
- c. Require a start of shift orientation (which may be part of the shift handover) where the tank levels are assessed and a search for abnormal tank levels, fill rates or line-ups is made. This should include re-evaluating each filling tank's "time to fill" and predicted "time at full."
- d. Require periodic verbal interaction or supervision of the operator to sustain their continuous vigilance.
- e. Provide a step-by-step tank management procedures that include:
 - i. Tank valve line up instructions with check off provisions for each different tank transfer configuration.
 - ii. Standard form (i.e. a manual calculation carried out by competent personnel), software program, or DCS based tank inventory management system that can be used to estimate the fill rate and ultimate level in the tank during the transfer.

- iii. Proactive monitoring of the tank level as the transfer occurs such as a standard transfer form or software program that requires the operator to log initial tank level from the tank gauging system, direction of level change (increasing or decreasing) and periodic tank levels throughout the transfer.

In addition to these specific elements the duty holder should also conform to the guidance provided in Section 5.1 Threat Lines, i.e. training, competence, demands on operator time, audits, etc. See PSLG final report, appendix 2; annex 6 for further guidance on cross-checks.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations

Abbreviation	Description
ALARP	As Low as is Reasonably Practicable
ATG	Automatic Tank Gauging
BPCS	Basic Process Control System
CA	Competent Authority
CDOIF	Chemical and Downstream Oil Industry Forum
CM	Conditional Modifier
CP	Containment Policy
HEP	Human Error Probability
HF	Human Factors
IHHA	Independent High High Alarm
HSE	Health and Safety Executive
HSL	Health and Safety Laboratory
IML	Independent Mitigation Layer
IPL	Independent Protection Layer
PFD	Probability of Failure on Demand
PSLG	Process Safety Leadership Group
ROSOV	Remotely Operated Solenoid Valve

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Mark Manton (Chair)	Essar
Peter Davidson	UK Petroleum Industry Association
Neil Macnaughton	BP
Julian Douse	Petroplus
Mike Boothman	Phillips 66
Raman Sridhar	BP
Paul Jobling	Simon Storage
Kathy Whileman	Exxon
Craig Pugh	Exxon
Paul Birkmyre	INEOS
Ed Fergus	Health and Safety Executive
Dylan Peters	Murco

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	14-May-2012	Peter Davidson
1	All	Updated to include working group comments	19-June-2012	Peter Davidson
2	All	Updated to include further working group comments	02-Aug-2012	Peter Davidson
3	All	Updated to include CA comments	12-Nov-2012	Peter Davidson, Mark Manton, Neil Macnaughton
4	All	Updated to include final comments from CA and CDOIF Working Group	15-Nov-2012	Peter Davidson
5	All	Updated to include final UKPIA comments	03-Dec-2012	Peter Davidson

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 1 – Vapour cloud formation calculation

CDOIF

Chemical and Downstream Oil Industry Forum

Guideline

Automatic Overfill Prevention Systems for
Terminal Loading Racks

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members a guideline on automatic overfill prevention systems for terminal loading racks.

It is not the intention of this document to specify the detailed design of overfill prevention systems, nor replace any existing corporate policies or design standards. The intent is to provide a reference for those organisations developing or wishing to review their existing terminal loading rack overfill prevention architectures.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to overfill prevention systems at terminal loading racks.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Automatic Overfill Prevention Systems for Terminal Loading Racks".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

This guidance is not intended to be an authoritative interpretation of the law, however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holders compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for overfill prevention, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action. If the duty holder does follow the guidance they will normally be doing enough to comply with the law. Health and Safety inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Contents

FOREWORD	2
CONTENTS.....	3
1. EXECUTIVE SUMMARY.....	4
2. SCOPE	5
3. OVERVIEW.....	6
3.1 Causes of Overfills.....	6
3.2 Overfill Prevention System Goal.....	7
4. RISK ASSESSMENT	8
4.1 Assessing the Suitability of Road Tanker Loading System Architectures	8
4.1.1 Specification of Valves	8
4.1.2 Automated Shutdown Valves	9
4.1.3 Initiation of Automated Shutdown Valves	9
4.1.4 Effectiveness of Emergency Shutdown Valves.....	11
4.1.5 Testing of Valves	11
4.1.6 Maintenance of Valves	12
4.1.7 Management of Risk	12
5. SYSTEM DESIGN AND OPERATION	13
5.1 Overfill Prevention System Equipment	13
5.2 Overfill Prevention System Control Philosophy	15
ABBREVIATIONS.....	17
GLOSSARY OF TERMS	17
OTHER RELEVANT PUBLICATIONS	18
ACKNOWLEDGEMENTS.....	19
REVISION HISTORY.....	20
APPENDIX 1 – EXAMPLES OF FACTORS THAT MAY INFLUENCE RESPONSE TIMES.....	21

1. Executive Summary

A number of overfilling incidents have occurred during the loading of gasoline into road tankers. Overfilling has occurred due to the failure of people and equipment, resulting in an uncontrolled flow and significant quantities of gasoline being lost from containment¹. In each case there were unrecognised deficiencies in the architecture of the loading system which were exposed by a single failure. The deficiencies in the loading system have included the inability of the emergency shutdown system to stop gasoline flow. The majority of these occurrences were due to failure of the flow control valve.

Personnel have been exposed to risks of serious injury during overfilling incidents due to their presence in the spill area. In some cases personnel have purposely entered the spill area during attempts to diagnose faults and to stop the flow of gasoline.

The target Audience for this document is primarily operators of fuel distribution terminals, including terminal managers, engineering managers, HSE/SHE managers, C&I and risk control engineers. Suppliers of equipment/packages and system integrators may also find the guidance provided in this document informative.

A working group was commissioned under CDOIF to develop a guideline for overfill prevention systems at terminal loading racks. This guideline is not intended to be prescriptive in defining the detailed design criteria for these systems, but aims to raise awareness within industry of existing good design practice, and highlight where appropriate key areas against which duty holders may review their existing systems.

A second working group was commissioned to look into hazard awareness of tanker drivers and terminal personnel during filling operations, the guidance for which can be found in the CDOIF publication entitled 'CDOIF Guideline – Terminal Loading Operations Hazard Awareness'.

Note 1

Each tank compartment's overfill prevention sensor is set to provide ullage of not less than 150 litres between the point of it being tripped and overfilling. This is to ensure that all the product passed by the gantry flow control valve from the triggering of the overfill prevention sensor until flow is ceased will be contained within the compartment (even if the event is triggered at the maximum flow rate)

Note that the overfill prevention system plays no part in ensuring that the tanker is not overloaded nor in ensuring that the maximum degree of filling (ADR 4.3.2.2) has not been exceeded

2. Scope

This document provides guidance on the architecture of loading systems for delivering gasoline into bottom loaded road tankers.

This guideline does not cover toxic hazards, fuels that are below their flash point at normal loading temperatures and atmospheric pressures, non ignition risks. This document does not comment on the safety integrity level (SIL) of any measure or system used to prevent the overfilling of road tankers, or the measures necessary to control risk during any recovery operation following an overfill. The need for, and definition of, any additional layers of protection should be completed as part of an operator's standard design processes for hazard identification, risk assessment and SIL determination, where necessary.

For the purposes of this guidance overfilling means filling a compartment to the point that gasoline flows out of that compartment, for example into a vapour recovery system or through a pressure relief valve.

3. Overview

Overfilling can occur for a variety of reasons, including:

- filling a compartment that already contains gasoline that the driver is unaware of or does not take account of,
- filling the wrong compartment,
- failure of equipment intended to automatically stop gasoline flow.

Where a flow control (or metering) valve fails there is often very little time from the onset of the failure before the compartment overflows. This is because compartments have a limited ullage of about 5% (for transport), and because high flow rates can continue even if the pump has been turned off. The high flow may continue under flow control valve failure conditions because of the momentum of the flow in the pipe work, and the large liquid head arising from the tall supply tanks at many installations.

An example of an automated road tanker loading system can be seen in figure 1 below.

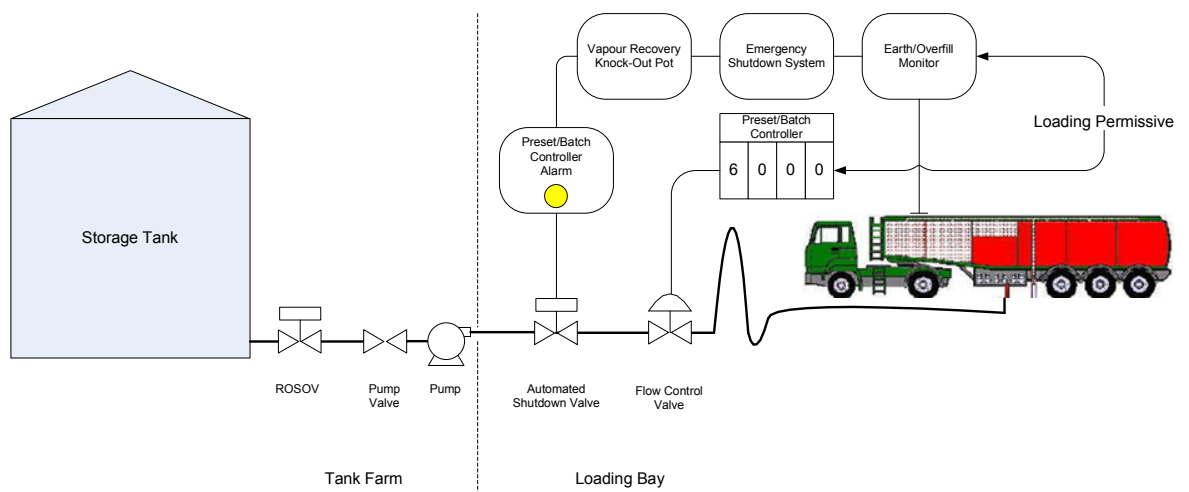


Figure 1 – Example road tanker loading system

3.1 Causes of Overfills

Flow control valves are generally considered to be reliable. However, flow control valves have failed to close when expected either because the flow control valve itself has failed, or because a pilot valve has failed. Valves have failed due to damage to elastomer materials as a result of changes in gasoline blends, due to the ingress of foreign material preventing closure, or due to physical wear. In each case the failure has been sudden; there were few clear signs of performance deterioration.

Many incidents have occurred because there is no automated shutdown valve. In these cases, a failure of the flow control valve has led to an uncontrolled flow of gasoline that can only be stopped by the closure of a manual isolation valve. This requires a fast response. Experience has showed that it is not realistic to expect overfilling to be prevented by a person closing a manual valve (see table 2 on the response times required).

A number of incidents have occurred even where there is an automated emergency shutdown valve that can close in the event of the failure of the flow control valve. This has been because the emergency shutdown valve was not triggered to close by the overfill event, the automated emergency shutdown valve closed too slowly, or the emergency shutdown valve was triggered too late to prevent an overfill.

Failure to trigger the emergency shutdown valve has been caused by a reliance on an overfill signal that may not occur in certain circumstances, such as a high liquid level in the vapour recovery line knock out pot.

A rule of thumb applied to valve closure speeds is that it takes approximately one second per inch diameter for a valve to close, but some valves may close more slowly than this. A limitation of the speed of closure is the 'hammer' effect caused by the momentum of the fuel which can increase pipe pressure to dangerous levels if the flow rate is slowed too quickly.

The emergency shutdown valve may be triggered too late for a number of reasons including where human action is relied on to quickly identify the developing overfill and respond.

3.2 Overfill Prevention System Goal

The goal of an overfill prevention system is self-evidently to prevent the overfilling of a road tanker or any of its compartments. In this context overfilling means exceeding the capacity of a compartment to the point that gasoline flows out of that compartment (including into the vapour recovery system). The extent to which overfill prevention measures are implemented is subject to formal risk assessment as described in section 4.

4. Risk Assessment

It is essential that the risks arising from all road tanker loading operations are assessed, and measures put in place to ensure these risks are, 'as low as reasonably practicable'. This includes any risks that may arise from potential component failures or design inadequacies in the engineering architecture. Risks may include risks to people, risks to installations, and risks to the environment.

4.1 Assessing the Suitability of Road Tanker Loading System Architectures

The adequacy of the measures used to control risks during filling operations should be assessed. This can be achieved by asking a number of questions regarding the architecture of a loading system.

1. Is the flow control valve, and any associated pilot valves, correctly specified for the function it is expected to perform? (refer to 4.1.1)
2. In the event of a failure of the flow control valve, is there an automated shutdown valve to stop gasoline flow? (refer to 4.1.2)
3. Is an automated shutdown valve triggered in response to identified faults or failures (refer to 4.1.3)
4. Is an emergency shutdown automated valve able to prevent or mitigate against overfilling of a road tanker, taking into account realistic scenarios? (refer to 4.1.4)
5. Are automated shutdown valves tested at a suitable frequency, according to specific criteria? (refer to 4.1.5)?
6. Are automated shutdown valves maintained according to appropriate instructions? (refer to 4.1.6)?
7. Are indications of failures recorded and assessed, and actions to address these taken? (refer to 4.1.7)

Any dependencies between risk control measures should be identified, and eliminated if possible. It is good practice to be able to detect the failure of a measure as soon as possible after it occurs, preferably by automated means, so that adequate risk control is maintained.

4.1.1 Specification of Valves

Site operators should document the design requirements for the different valves in the loading system, and should ensure suitable valves are installed. Design requirements should include compatibility with the gasoline being loaded and number of operations.

Valve failures have occurred due to;

- Excessive number of operations. Manufacturers produce specifications regarding the maximum number of cycles a valve should be expected to perform, depending upon the conditions the valve is operating under. For example, it is common for pilot valves to operate many times during each loading operation,

and, if rate adjustment valves are not correctly set, for excessive pilot valve cycling to occur. Consideration should be given to the use of any extended diagnostic functionality that may be available.

- Product incompatibility. Valve failures have occurred because of incompatibility between gasoline and seal elastomers, so it is important that valves are suitable for the gasoline to which they are exposed (especially gasoline/ethanol blends with ethanol content, even as low as 5%). Further investigation on compatibility of materials used in handling ethanol and gasoline/ethanol blends has been undertaken by the Energy Institute, reference to the latest manufacturer's guidance on material compatibility should also be sought. Any significant change in gasoline formulation should trigger an assessment to verify valves continue to be suitable, and any remedial action required. This should be part of a suitable Management of Change process.
- Incorrect selection. Valves have failed because they have been incorrectly selected for use based on sales literature that was incomplete, not more detailed technical specifications. Personnel responsible for device selection should have a design requirement specification for each device, and the competence to assess the potential impact of any deviation.
- Incorrect pressure specifications. Whilst working pressures in many loading systems are relatively low, large pressure spikes may be experienced as a result of fast changing flow rates, such as those experienced towards the end of a filling operation.

Valve specifications should be archived so that they can be used by competent staff to select a new valve in the event of a replacement being required at some time in the future.

Spare valves in stock should be clearly labelled to ensure the correct replacement valve can be selected.

4.1.2 Automated Shutdown Valves

Correct specification, operation, and maintenance will reduce the risk of a flow control valve failure. However, the range of challenges to a particular flow control valve means this risk cannot be eliminated. An automated shutdown valve when triggered prevents uncontrolled flow of gasoline in the event of a failure of the flow control valve. Use of an automated shutdown valve has been shown to be a reasonably practicable way of managing this risk. A manually operated secondary valve has been shown to be ineffective in preventing overfill and loss of containment.

A means of regularly testing the required functions of the automated shutdown valve should be incorporated into the design, including the ability of the valve to actually stop liquid flow. Information on this is given in section 4.1.3.

4.1.3 Initiation of Automated Shutdown Valves

Automated shutdown valve closure should be initiated as soon as possible after a loss of control. Detection may be via a number of means, and a combination of means may be

necessary to adequately control risk. Closure of automated shutdown valves may be initiated by several, or all, of the following;

- An alarm resulting from the preset/batch controller detecting a flow rate outside that programmed for the phase of loading
- An alarm resulting from the preset/batch controller detecting an overrun beyond the programmed amount
- A detection of high level in the road tanker
- An emergency shut-down button being pressed
- Gasoline detection in the vapour recovery system
- Action being taken from a remote location such as a control room

Other initiators may be available from a variety of engineered systems and human sources.

The initiator at the top of the list above is likely to provide the fastest response to a loss of flow control, and the initiator at the bottom of the list is likely to provide the slowest response. The overfill prevention system should be designed so the automated shutdown valve closure is initiated as soon as possible after the loss of flow control. This reduces the chance that gasoline will be lost from containment.

The initiators listed above depend upon a range of mechanical, electrical, electronic and programmable electronic systems. These should be effective for a range of different failure scenarios such as failure of the preset/batch controller electronics (that may have caused the loss of control in the first place), and variations in the mechanical arrangement of the vapour recovery system. Some measures, such as human responses, and desktop computers should not be expected to provide significant amounts of risk control.

The effectiveness of each initiator for automated shutdown valves should be tested on a regular basis using tests that confirm the correct operation of as much of the system as possible. More frequent partial checks may be appropriate where more complete tests are intrusive.

Effective management processes should be in place to ensure the operability and continued maintenance of the high level probe in each road tanker compartment which is connected to the earth/overfill monitor. Management processes may include participation in a scheme which aims to control the hazards associated with road tankers when they are loaded at distribution terminals such as the Safe Loading Pass Scheme, or other similar initiatives.

4.1.4 Effectiveness of Emergency Shutdown Valves

Emergency shutdown valves should be effective in preventing a loss of containment when triggered by an engineered system such as the high level detection system in the road tanker. This should take into account the time between the loss of flow control, to the flow reaching zero. An example of timings is shown in figure 2.

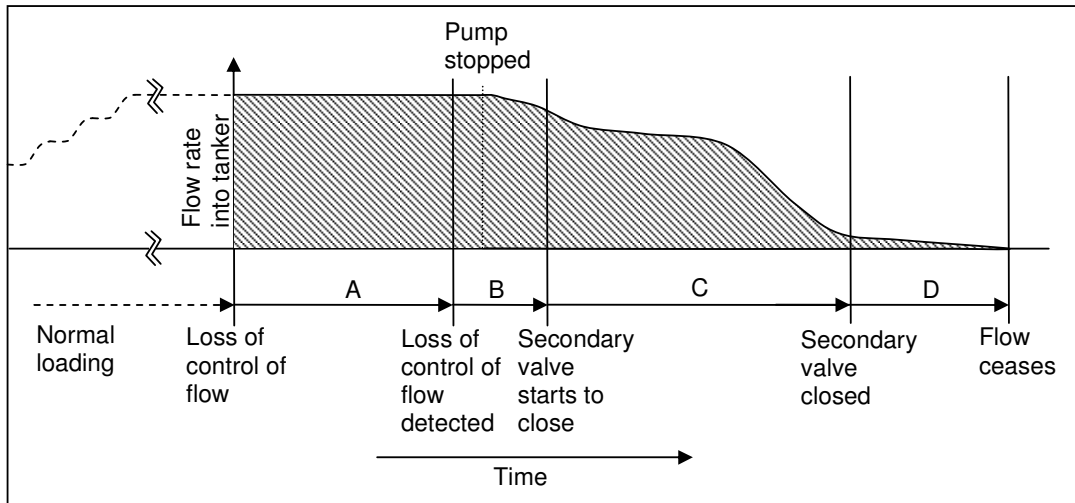


Figure 2 – Time to stop flow on loss of flow control

Definition of times:

- A. Time between loss of control and detection of the loss of control.
- B. Time between the detection of the loss of control and closure initiation of the automated shutdown valve. This includes any delays caused by logic.
- C. Time that the automated shutdown valve takes to close. A rule of thumb is one second per inch diameter of the valve, but certain automated valve types may take longer.
- D. Time between the emergency shutdown valve becoming fully closed, and cessation of all flow.

The total time to stop flow using the automated shutdown valve after a loss of flow control is $A+B+C+D$. The exact timing of each of the components A, B, C, and D will depend upon the configuration of the loading system, and what has led to the loss of flow control. Refer to appendix 1 for examples of factors that may influence response times.

4.1.5 Testing of Valves

Valves should be tested at a frequency that is appropriate, according to the extent that the valve is being relied upon for risk control. Test frequencies should be set so that there is little chance of valves failing between two tests.

Valve tests should cover as much of the functionality of the valves as possible. This may include speed of response and the actual ability of the valve to shut against an upstream pressure.

Some valve functions may be automatically tested during their cycling in normal operation through a control system. This may significantly improve confidence that the valve will continue to perform correctly, and a failure may trigger a very early response that may minimise risk.

Where there are indications of deterioration of a valve, action to correct the fault should be taken. The frequency of tests should be managed, and may need to be changed in response to a significant number of test failures.

Valve test records should be kept as part of the maintenance process providing evidence of the tests conducted, results of the test and any remedial actions carried out.

4.1.6 Maintenance of Valves

Valves should be maintained according to the specification from the manufacturer. In addition, certain aspects of maintenance may be specified locally, in order to manage risks. Locally originated maintenance should be specified by a person who is competent, who may need to liaise with the valve manufacturer regarding the particular valve usage.

Valves have failed because:

- Maintenance has not been carried out
- Maintenance has as not been carried out correctly
- Faults have been identified but not remedied

Personnel who maintain valves should be competent to do so, and should know when to refer difficulties to other personnel with the appropriate knowledge and skills for correction. Senior staff should be competent to direct others such that the risk is adequately managed.

4.1.7 Management of Risk

Risks must be managed using appropriate means, and should be regularly re-assessed. It may be necessary for indications of failures to be recorded and assessed, so changes can be made to prevent failures that could lead to overfills.

5. System Design and Operation

The following sections provide a high level overview of the equipment that may form part of an overfill prevention system for a terminal loading rack, and the interactions between those components as part of an overall control philosophy.

Note that this represents one design philosophy; it should not be considered as the only or the preferred solution. This will be dependent on the individual site requirements, and in consideration of the risks and appropriate measures discussed in section 4.

5.1 Overfill Prevention System Equipment

Typical equipment that may be incorporated into a loading rack control and overfill prevention system is provided below. Reference should be made to figure 1, Example road tanker loading system contained in section 3.

1. **Loading Rack Control System** – the loading rack control system is the PLC/SCADA system which provides control operation for the terminal or the loading rack, or both. In some instances, interlocks and permissives may be hardwired via relays, and not via the loading rack control system. Where risk assessment has determined that the overfill prevention system requires a further layer of protection, this functionality may be provided by an independent safety related logic solver.
2. **Electronic preset/batch controller** – the system which controls loading operations. The electronic preset/batch controller accepts earth and overfill interlocks (hardwired from relays or via the loading rack control system), which provides a permissive for pump demands, flow control and controls flow rates. The electronic preset/batch controller should prevent or stop loading on loss of interlocks or on detection of abnormal conditions (such as high or low flow, batch quantity overrun)
3. **Earth/overfill monitor** – the system monitors tanker earth integrity and tanker overfill detectors. Outputs from the monitor should be hardwired via relays or via the loading rack control system, providing the interlock signal to the electronic preset/batch controller, and allowing automatic closure of the automated shutdown valve(s). Faults detected on the monitor should allow unit to fail safe.
4. **Flowmeter** – connected to the electronic preset/batch controller to provide flow signal. Typically the flowmeter type will be positive displacement or turbine.
5. **Flow control valve** – connected to the electronic preset/batch controller, controls flow rates and stops/starts the batch flow.
6. **Vapour knockout pot high level detector** – monitors fluid level at lowest point in vapour system as close as possible to the tanker vapour hose/arm. The signal should be hardwired from relays or via the loading rack control system providing the interlock signal to the electronic preset/batch controller, and allowing automatic closure of the automated shutdown valve(s).
7. **Emergency shutdown pushbutton** - hardwired via relays or via the loading rack control system, providing the interlock signal to the electronic preset/batch

controller, and allowing automatic closure of the automated shutdown valve(s). Faults detected on the pushbutton, or loss of power should allow unit to fail safe.

8. **Automated shutdown valve(s)** – the automated shutdown valve should automatically close on detection of fault conditions, either through hard wired relays or from the loading rack control system. The automated shutdown valve should ideally be located at ground level on loading bay. There may be one valve per arm, or one valve per grade depending upon the individual site requirements. The automated shutdown valve may be either motor, hydraulic or gas operated and should be fail safe closed under fault/loss of power condition.

5.2 Overfill Prevention System Control Philosophy

Reference should be made to the simplified cause and effect diagram provided in figure 3 as an example control philosophy for overfill prevention.

Note: automated shutdown valve may be per bay or per grade

	Close FCV - Bay A	Close FCV - Bay B	Close FCV - Bay C	Close S/D Valve - Bay A	Close S/D Valve - Bay B	Close S/D Valve - Bay C
Meter Overrun - Bay A	X					
Meter Overrun - Bay B		X				
Meter Overrun - Bay C			X			
Earth/Overfill Monitor - Bay A						
Loss of Earth Signal	X					
High Level Detected	X			X		
Earth/Overfill Monitor - Bay B						
Loss of Earth Signal		X				
High Level Detected		X			X	
Earth/Overfill Monitor - Bay C						
Loss of Earth Signal			X			
High Level Detected			X			X
Vapour K-O Pot High Level - Bay A	X			X		
Vapour K-O Pot High Level - Bay B		X			X	
Vapour K-O Pot High Level - Bay C			X			X
Site ESD Initiated	X	X	X	X	X	X

Figure 3 - Simplified cause and effect diagram

Note that pumps have been excluded from the cause and effect diagram in figure 3. Determining what action to take for pumps should form part of the risk assessment and design process.

1. **Electronic Preset/Batch controller** – a healthy earth/overspill interlock from the earth/overfill monitor provides a healthy permissive signal allowing pump demand

and flow control valve outputs. Loss of the interlock removes the permissive and stops flow by closing the flow control valve. Depending on the preset/batch controller type, various internal parameters (for example high/low flow, additive high/low flow, loss of flowmeter pulses) can be configured to operate an internal alarm relay, which may be used to indicate “preset/batch controller overrun” and remove the permissive stopping flow by closing the flow control valve and/or closing the automated shutdown valve.

2. Earth/overflow monitor –

- a) Loss of the earth signal should remove the earth/overspill input from the preset/batch controller, hence removing the permissive signal and stopping flow by closing the flow control valve.
- b) Loss or activation of overflow signal should remove the earth/overspill input from the preset/batch controller, hence removing the permissive signal and stopping flow by closing the flow control valve. Additionally the overspill signal should close the automated shutdown valve(s) on the loading bay the overflow signal was generated on; all other loading bays can remain operational.

3. Flow control valve – the preset/batch controller will close the flow control valve on loss of earth/overspill signal, activation of preset/batch controller alarm relay (where available to indicate preset/batch controller overrun) or end of batch.

4. Vapour knockout pot high level detector – the vapour knockout pot high level should be part of the electronic preset/batch controller permissive. Activation of the high level detector should remove the permissive, thereby closing the flow control valve on that loading bay. Additionally the automated shutdown valve(s) on the loading bay that the knockout pot high level signal was detected on should close. All other loading bays can remain operational.

5. Emergency shutdown pushbutton – activation of any of the tanker loading bay emergency shutdown pushbuttons should remove the permissive for all electronic preset/batch controllers thereby closing the flow control valves and automated shutdown valves.

6. Automated shutdown valve(s) – automated shutdown valve(s) should close on activation of the road tanker overflow signal via the earth/overflow monitor, vapour knockout pot high level signal associated with that loading bay or activation of any terminal ESD pushbutton.

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations

Abbreviation	Description
CA	Competent Authority
C&I	Control and Instrumentation
CDOIF	Chemical and Downstream Oil Industry Forum
ESD	Emergency Shut Down
FCV	Flow Control Valve
HSE	Health, Safety and Environment; Health and Safety Executive
K-O	Knock Out
PLC	Programmable Logic Controller
ROSOV	Remotely Operated Solenoid Valve
S/D	Shutdown (Automated Shutdown Valve)
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SHE	Safety, Health and Environment

Glossary of Terms

Loading	Loading is synonymous with the ADR related term 'filling'
Flow control valve	The valve used to accurately meter gasoline into road tankers, sometimes referred to as a metering valve.
Automated Shutdown valve	The valve used to shutdown the flow of gasoline on detection of fault or overfill conditions
Gasoline	low flashpoint liquid fuel, also known as petroleum spirit or petrol, including where blended with ethanol, where there is a significant probability of flammable vapour present at normal loading temperatures and pressures.
Metering valve	See flow control valve.
Overfilling	For the purposes of this guidance overfilling is considered to be filling a compartment to the point that gasoline flows out of that compartment, for example into a vapour recovery line or through a pressure relief valve .
Overflow	The point at which a compartment is overfilled to the extent that the addition of more liquid will result in liquid beginning to flow out of the compartment.

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Other Relevant Publications

Further information relating to road tanker installations can be found in the following publications.

- 1) HSG 176 [1998]
- 2) EI Model Code of Safe Practice - Marketing safety code [1978 – revised in 1998, and again in 2005.
- 3) EI Model Code of Safe Practice – Design, construction and operation of petroleum distribution installations [September 2005]
- 4) API RP 1004 [Eighth Edition, January 2003].

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Mark Jolliffe (Chair)	Total
Darren Peck	Nustar Energy
Andrew Dodd	Nustar Energy
Clive Dennis	Health and Safety Executive
Andrew White	Health and Safety Executive
Eddie Watts	Chevron
Ian Goldsworthy	Chevron
Kevin Shepherd	Vopak
Peter Lloyd	Vopak
Rex May	BP
Robert Harris	Amber Engineering Consulting Ltd.
Peter Davidson	UK Petroleum Industry Association

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	05-Jan-2011	PSD
1	All	Update following working group comments	04-Feb-2011	PSD
2	4.1.1	Update following CDOIF comments	06-May-2011	PSD

Appendix 1 – Examples of factors that may influence response times

Examples of factors that may influence the times;

- A.
- Where the loss of flow control has been caused by a failure of the flow control valve and is detected in the preset/batch controller, and this detection feature has been correctly configured, time A may be short.
 - Where the loss of control is detected by a high level detection in the road tanker, time A will be longer.
- B.
- The time between the detection of the loss of control of flow and the initiation of the closure of the automated shutdown valve will normally be short. This time could be longer or may vary where there is significant electronic processing prior to the close signal being given, or where the initiation is delayed by, for example, the dumping of pneumatic pressure.
 - The rate of flow will generally reduce after the pump is stopped. However, where a centrifugal pump (or other non positive displacement pump) is used, then any upstream pressure, such as that caused by fluid head in the storage tank, will continue to drive the gasoline at a constant flow rate. The flow rate will depend upon the upstream pressure and the diameter and configuration of pipe work and any orifices.
 - Some preset/batch controller systems are designed to delay the stopping of the pump until the flow control valve has closed. Depending upon the exact arrangement, this may delay the stopping of the pump so this occurs later than shown on the diagram.
- C.
- The speed of closure of the automated shutdown valve will depend upon its design and configuration. Larger valves generally take longer to close than smaller valves. Closing a valve too quickly can cause high pressures to be developed upstream of the valve, with the subsequent risk of damage that could lead to leakage.
 - The momentum of the gasoline will tend to continue driving the gasoline out of the pipe work due to the initially high linear speeds of the gasoline at maximum loading rates.
- D.
- This time between the complete closure of the emergency shutdown valve and the cessation of all flow will depend on the physical arrangement of the loading system and the road tanker. For example, fuel may enter the vapour recovery pipe work from the tanker vapour recovery manifold. A table of example pipe work capacities for pipe diameters and lengths is given in table 1.

The amount of gasoline stored in pipe work can be estimated using the following formula:

$$\text{Volume (litres)} = (\text{Pipe diameter (inches)} / 2 * 2.54)^2 * 3.14 * \text{pipe length (metres)} / 10$$

Example volumes of pipe work are given in table 1

CDOIF

Chemical and Downstream Oil Industry Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Pipe length (metres)	Pipe diameter (inches)						
	3	4	6	8	10	12	14
	Volume (litres)						
10	45.604	81.073	182.41	324.29	506.71	729.66	993.15
20	91.207	162.15	364.83	648.59	1013.4	1459.3	1986.3
30	136.81	243.22	547.24	972.88	1520.1	2189	2979.4
50	228.02	405.37	912.07	1621.5	2533.5	3648.3	4965.7

Table 1 – Liquid volume of pipe work (litres)

The total amount of gasoline that will flow into the road tanker, for the various detection routes, will be the area under the graph in figure 2, which will be unique for each loading arrangement. Whether the road tanker becomes overfilled, or gasoline is lost from containment depends on how much empty volume there is in the tanker compartment when the control of flow is lost, and whether gasoline flows into other unfilled compartments and the vapour recovery system. Experience has shown that whilst gasoline from an overfilled compartment does flow into other unfilled compartments, and into the vapour recovery line, it preferentially flows out of containment. Consequently, when estimating whether a configuration will be able to prevent a loss of containment, no claim should be made that gasoline can flow into other compartments or the vapour recovery system.

The time between the high level detection in a tanker compartment and overflow occurring depends on the size of the compartment, and the flow rate. Table 2 shows example times based on a range of flow rates and compartment sizes.

Flow rate after failure (litres/min)	Compartment size (litres)						
	7600	7000	6000	5000	4000	3000	2500
	Approximate remaining volume in compartment at high level detection point (litres) @ 95% full						
	380	350	300	250	200	150	150*
Time to loss of containment after high level detection (seconds)							
2500	9.1	8.4	7.2	6.0	4.8	3.6	3.6
2200	10.4	9.5	8.2	6.8	5.5	4.1	4.1
1900	12.0	11.1	9.5	7.9	6.3	4.7	4.7
1700	13.4	12.4	10.6	8.8	7.1	5.3	5.3
1500	15.2	14.0	12.0	10.0	8.0	6.0	6.0
1200	19.0	17.5	15.0	12.5	10.0	7.5	7.5
1000	22.8	21.0	18.0	15.0	12.0	9.0	9.0
800	28.5	26.3	22.5	18.8	15.0	11.3	11.3
500	45.6	42.0	36.0	30.0	24.0	18.0	18.0
300	76.0	70.0	60.0	50.0	40.0	30.0	30.0

Table 2 – Time before overflow of a tanker compartment

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

* The minimum remaining ullage volume at the high level detection point is normally 150 litres.

Additional measures may have to be taken to prevent risks arising from gasoline entering the vapour recovery system. This document does not comment on these

Case study: Warwickshire Oil Storage Ltd (WOSL)

Introducing a competency management system



Introduction

This case study explains how WOSL managed the introduction of a competency management system (CMS) with the support of Environmental Resources Management Ltd (ERM).

Who is WOSL and what does it do?

Kingsbury Oil complex, in the Midlands, is the largest inland oil storage depot in the United Kingdom and storage operators on site include BP, Valero and WOSL (Shell and the British Pipelines Agency also have facilities on site). Together with BP and Valero, WOSL stores petroleum products (eg petrol, diesel and heavy oil) for distribution around the UK and the site is classified as hazardous under the COMAH Regulations 1999.

Why did WOSL look at CMS?

Three key reasons why WOSL looked at developing a CMS were:

- The General Manager of WOSL recognises the importance of competency and competency management in reducing accidents, which is particularly important in the high-risk industry that he and his colleagues work. As a member of the working group of the sector skills council for chemicals, pharmaceuticals, nuclear, oil and gas, petroleum and polymer industries (COGENT) Downstream Advisory Council (which was formed to develop guidelines for competency management systems for downstream and petroleum site), he is aware of the positive impact a well thought-out and effective CMS can have in reducing incidents. This initiative is also seen as being good for business, with any costs attached to ensuring safety fading into insignificance against the risk of a major accident. Prevention of a large-scale incident by spending time on improving the knowledge, skills and abilities of WOSL staff, was considered a small price to pay.
- The General Manager welcomed the HSE's intention to increase their focus on ensuring competency at COMAH sites as this fitted well with plans already underway at WOSL.
- Due to organisational changes, WOSL had greater autonomy from their parent companies and, with this came new responsibilities, including establishing health and safety initiatives such as developing an effective CMS.

How is the CMS being developed?

WOSL and ERM recognise that competency is important to individuals; with intrinsic and extrinsic job feedback providing a feeling of success and 'self efficacy'. This feedback supports workers' sense of being competent and their awareness of how their actions are impacting on safe site operations. It also identifies practice gaps that help people to perform better.

Guidelines for Competency Management Systems for Downstream and Petroleum Sites (COGENT (2011)) is based on six principles that are contained within the CMS cycle (see Figure 1).

Figure 1 The six principles of competence assurance



15

Delivering sustainable solutions in a more competitive world



This cycle is underpinned by the management principles of 'POPMAR' (HSG65) and is similar to the CMS cycle published by HSE in 2002 and by the Office of Rail Regulation in 2007.

WOSL and ERM began by defining the scope of the CMS in line with COGENT guidance (2011). As part of this process, and based on experience and industry wide statistics, a team of subject matter experts decided on the safety critical tasks at WOSL. Over 20 safety critical tasks were identified (eg permit to work), together with related sub-tasks (eg completion and checking of work permits).

Major accident hazard scenarios were identified and plotted on a hazard identification and risk assessment matrix (ie based on the severity and likelihood of the scenario). The aim of this exercise was to prioritise the scenarios. Each scenario was presented as a bow tie diagram (ie a diagrammatic representation of hazardous events including threats, barriers and consequences). This helped to visualise the possible threats leading to the scenario, determine the subsequent consequences of the scenario and the potential barriers (eg control measures and mitigation factors).

In order to systematically consider the types of human failure that may occur when performing the safety critical tasks, ERM and WOSL carried out a human error analysis for each task, whereby each step of each task was assessed to determine the potential human failure and/or the opportunity to recover from this failure. In line with HSE's Human Factors Roadmap, the human error analysis also formed

the basis of the standard operating procedures (SOPs), with the understanding of why errors occur and the different factors that make them worse, helping WOSL to develop and improve their procedures.

ERM and WOSL ensured a high level of worker engagement, where operators and supervisors were actively involved in the updating of the safety critical procedures, using human factors professionals to apply design usability principles, like consistency, clarity and navigability. This noticeably improved the usability of critical operating procedures.

All this information makes a valuable addition to WOSL's COMAH safety report, helping to demonstrate how the competency of staff, particularly in relation to safety critical tasks, is assured on site. The linking of the CMS with the COMAH safety report is outlined in the COGENT guidance (2011).

To facilitate the mapping of competency to the safety report, ERM ran workshops with WOSL employees to identify on which of the safety critical tasks they have an impact. Figure 2 is a photograph taken at the workshop, and shows WOSL staff and management all involved in the mapping exercise. This was found to be beneficial to all those involved, as it highlighted that everyone had a role to play in reducing accidents. In addition, individuals reported that this task had highlighted the impact that they have on safety and accident prevention.

Figure 2 Everyone at WOSL gets involved with the mapping exercise



Feeding the results of the workshop into the safety report highlights how the safety report is a living document, the importance of which in reducing accidents is recognised by all WOSL employees. The active participation of the workforce in the workshop demonstrates how WOSL senior managers together with front line operators own the safety report, with all employees now being even clearer on their role in accident prevention.

How is the CMS being implemented?

In order to implement the CMS, all WOSL staff who carry out safety critical tasks are assessed against the competency standards for the job role. The existing standards have been in place since 2010 and there are plans to carry out a job analysis to systematically review the job description competency matrix to integrate it into the newly established CMS, in line with COGENT guidance (2011).

One method of assessment is through appraisal systems and the first stage of the WOSL appraisal system is for jobholders to assess themselves on the criteria laid out on the competency matrix. This is followed by a discussion with their line manager to seek agreement on their performance against the criteria. This process identifies where the individual's knowledge, skills and experience gaps are. Having established where the gaps are the line manager and jobholder work together to address these gaps by developing a training plan.

The development and maintenance of competencies is primarily through qualifications, training and supervision. Evidence of individual competency is captured in the CMS records and WOSL have various methods to monitor competence, depending on the activity and skill type, for instance:

- direct observation;
- indirect information gathering (eg systems data);
- emergency exercise simulations;
- written and verbal questions;
- open questions in performance interviews;
- multiple choice question tests;
- post-incident review.

The WOSL team competency matrix provides an overview of the training requirements. It shows the current and required level of training for the team. It provides a framework that enables the business to define minimum competence, together with the flexibility and cover required for the team to function effectively.

The WOSL team competency and training matrix is regularly updated centrally and gives an overview of the team competencies and training requirements. The matrix provides details on the collective set of skills and knowledge to facilitate cover, flexibility and to assure team competence.

By monitoring the competency and training matrix, team leaders are able to measure the team's level of competence against the standards and requirements of the job. The competency and training matrix is used on an annual basis as part of the appraisal conversation and when individuals move to a new role.

Assessing and maintaining the CMS

For the ongoing assessment and maintenance of the CMS, WOSL will be:

- reviewing competence standards in light of critical task analysis and risk assessment;
- conducting safety culture surveys to identify areas for improvement;
- maintaining the competence of CMS managers and assessors;
- assuring 'proof of competence' through the CMS and/or by mapping evidence across from a number of other different management systems;
- continue developing Key Performance Indicators (KPIs) such as the number of competence assessments carried out against plan and the number of task observations with non-compliance;
- undertaking an annual review of the CMS that could include; a) determining whether or not the CMS continues to meet its objectives; and b) identifying the availability of suitable and sufficient resources to run the CMS.

Verifying and auditing

Verifying and auditing the CMS is the final principle in the CMS cycle. Having established an active CMS, WOSL intends to audit the CMS by developing KPIs and measuring the percentage of compliance against each KPI measure. For instance, verification will be directed towards determining compliance with agreed standard operating procedures.

Application of CMS to the contractor workforce

Contractors are also expected to develop a CMS based on the COGENT guidelines (2011), linked in with the WOSL CMS and to be audited by WOSL. In line with this guidance, contractors may be categorised as type 1 contractors or as type 2 contractors, as this helps to identify where responsibility for the application of CMS lies. For example responsibility for maintaining training records lies with either the client company (type 1 contractor) or with the contractor (type 2 contractor).

What next?

WOSL are committed to establishing an effective and practical CMS, and having developed and implemented the CMS described above they are now striving to make informed improvements to the system (eg job and training needs analyses are planned that will form the basis of further development of the job description competency matrix, as well as the team and training competency matrix).

Further information

A Human Factors Roadmap for the Management of Major Accident Hazards
www.hse.gov.uk/humanfactors/resources/hf-roadmap.pdf

Developing and Maintaining Staff Competence (Second edition) Office of Rail Regulation
www.rail-reg.gov.uk/upload/pdf/sf-dev-staff.pdf

Guidelines for Competence Management Systems for Downstream and Petroleum Sites COGENT, UPIA 2011
www.cogent-ssc.com/Publications/CMS_Web_Version.pdf

Competence Human factors briefing note no. 2 HSE
www.hse.gov.uk/humanfactors/topics/02competency.pdf

Successful health and safety management HSG65 (Second edition) HSE Books 1997
ISBN 978 0 7176 1276 5 www.hse.gov.uk/pubns/books/HSG65.htm

This document is available at: www.hse.gov.uk/pubns/casestudy#.pdf

© *Crown copyright* If you wish to reuse this information visit www.hse.gov.uk/copyright.htm for details. First published 11/12.

CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Demonstrating prior use of elements of a
safety instrumented function in support of BS
EN 61511

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members a guideline on demonstrating prior use for elements of a safety instrumented function.

It is not the intention of this document to replace any existing corporate policies or processes. The intent is to determine the process by which a user can review equipment to support a claim of prior use.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of how to demonstrate a prior use claim for sensors and final elements and non-PE logic solvers of a safety instrumented function.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline - Demonstrating prior use of elements of a safety instrumented function in support of BS EN 61511".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

Reference should be made to BS EN 61511, *Functional safety - Safety instrumented systems for the process industry sector*, which provides detailed information relating to the demonstration of Prior Use.

This guidance is not intended to be an authoritative interpretation of the law; however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for demonstrating prior use, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

1.	EXECUTIVE SUMMARY.....	4
2.	INTRODUCTION AND SCOPE.....	5
2.1	Safety Integrity Levels in BS EN 61511	5
2.2	Hardware Fault Tolerance	6
3.	PRIOR USE - DEFINITION	9
4.	DEMONSTRATING PRIOR USE	10
4.1	Manufacturer’s quality, management and configuration management systems	10
4.2	Identification and specification of the components or subsystems	12
4.3	Demonstration of the performance of the components or subsystems in similar operating profiles and physical environments	12
4.4	Volume of the operating experience	13
Appendix A	Failure rate calculations.....	15
A.1	Failure rate	15
A.2	Calculating failure rates	16
A.2.1	Calculation based on Mean Time Between Failures	17
A.2.2	Calculation based on failure data analysis	17
A.3	Assessing the dominant failure mode	19
A.4	Other techniques for calculating failure rates	21
A.5	Systematic capability	21
A.6	Safety manuals.....	21
Appendix B	Worked example.....	23
Appendix C	Abbreviations.....	27
Appendix D	Other relevant publications	28

1. EXECUTIVE SUMMARY

The final report of the Process Safety Leadership Groups (PSLG) safety and environmental standards for fuel storage sites was published in December 2009. Appendix 4 of that report provides guidance on the architecture and design of automatic overfill protection systems for bulk gasoline storage tanks, one of the systems (or layers of protection) necessary to achieve the target Safety Integrity Level (SIL) level identified through the risk assessment.

The PSLG report provides supplementary guidance to the British Standard on the design, operation and maintenance of safety instrumented systems (for example an automatic overfill protection system) BS EN 61511, Functional safety – Safety instrumented systems for the process industry sector.

For a safety instrumented function designed to achieve a specific safety integrity level, BS EN 61511 has architectural requirements for the subsystems that comprise that safety instrumented function (sensors, logic solver and final elements). These architectural requirements are in addition to the failure measure requirements for the intended safety integrity level - BS EN 61511 Clause 11.4. The architectural requirements are expressed in terms of hardware fault tolerance (the number of dangerous failures that a subsystem can tolerate and still perform its function as intended).

If the end user wishes to reduce the hardware fault tolerance requirements for a specific safety instrumented function, the end user can gather evidence to meet the "Prior Use" requirements described in BS EN 61511 Clause 11.5.3. This allows the end user to reduce the hardware fault tolerance requirements by 1 - see BS EN 61511 Clause 11.4.4. The demonstration of "Prior Use" in BS EN 61511 is solely related to allowing a modification of the hardware fault tolerance needed for a specific safety integrity level.

A working group was commissioned under CDOIF to develop this guideline to assist users in preparing a case for demonstration of prior use. This is not intended to be prescriptive in defining the mechanism by which prior use should be demonstrated, but aims to highlight key factors that should be considered.

2. INTRODUCTION AND SCOPE

This document provides guidance to help duty holders prepare a demonstration of prior use for a component of a Safety Instrumented Function (SIF). A simple SIF can be described as having three elements, with each element having a number of components, as follows:

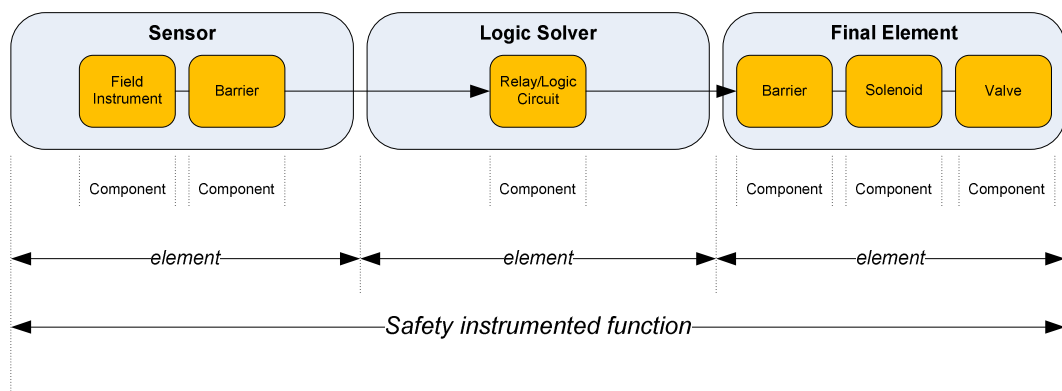


Figure 1 Elements and Components of a Safety Instrumented Function

Sensor: The components of the sensor element of the SIF that are used to detect an event. A component may be, for example, a level/pressure/temperature instrument or a barrier providing isolation.

Logic Solver: The components of the logic solver element of the SIF that are used to determine if an event has occurred. A component may be, for example, a simple relay/logic circuit, or complex safety controller

Final element: The components of the final element of the SIF that are used to maintain the process in a controlled state should an event occur. A component may be, for example, an isolation barrier, solenoid, valve, or pump.

When considering whether a component may be a suitable candidate for a demonstration of prior use, reference can be made to ISA-TR84.00.04 'Guidelines for the Implementation of IEC61511', Annex L1, which provides a work process for the selection of devices.

2.1 Safety Integrity Levels in BS EN 61511

Safety Instrumented Functions meeting the requirements of BS EN 61511 may be assigned one of four Safety Integrity Levels (SIL): SIL 1, SIL 2, SIL 3, or SIL 4.

Within the requirements for SIL 1, SIL 2 and SIL 3 in BS EN 61511, there is a need to achieve a specified degree of hardware fault tolerance (HFT)¹. The hardware fault

¹ See Section 2.2

tolerance requirements for SIL 4 are beyond the scope of BS EN 61511 and the reader of BS EN 61511 is referred to BS EN 61508. This guidance document on prior use will likewise focus only on SIL 1, SIL 2 and SIL 3.

2.2 Hardware Fault Tolerance

Hardware fault tolerance describes the ability of a subsystem or element to continue working successfully in the presence of dangerous faults. Consider a safety instrumented function (SIF) with two sensors configured such that only one of the sensors detecting the hazardous condition is needed to trigger the safety function. The occurrence of a dangerous fault in one sensor does not prevent the safety function from operating successfully. The sensor subsystem can therefore be described as having a hardware fault tolerance of 1. Were the sensor subsystem to have only one sensor, it would have a hardware fault tolerance of zero. A dangerous fault in the single sensor would prevent the safety instrumented function from operating.

For safety instrumented functions, BS EN 61511 sets out the minimum hardware fault tolerance requirements for sensors, logic solvers and final elements². Table 1 below shows minimum hardware fault tolerance requirements set out in BS EN 61511-1 for Sensors and Final Elements and non-Programmable Electronic Logic Solvers:

SIL	Minimum Hardware Fault Tolerance
1	0
2	1
3	2
4	Special requirements apply (refer to BSEN 61508)

Table 1 Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers

The values in Table 1 apply provided that the dominant failure mode is to the safe state or dangerous failures are detected, otherwise the fault tolerance shall be increased by one. However, the standard also indicates that the values in Table 1 may be reduced by one if the devices used comply with all of the following:

- the hardware of the device is selected on the basis of prior use
- the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;
- the adjustment of the process-related parameters of the device is protected, for example, jumper (an electrical connector on a circuit board), password;
- the function has an SIL requirement of less than 4.

² BS EN 61511-1 Clause 11.4

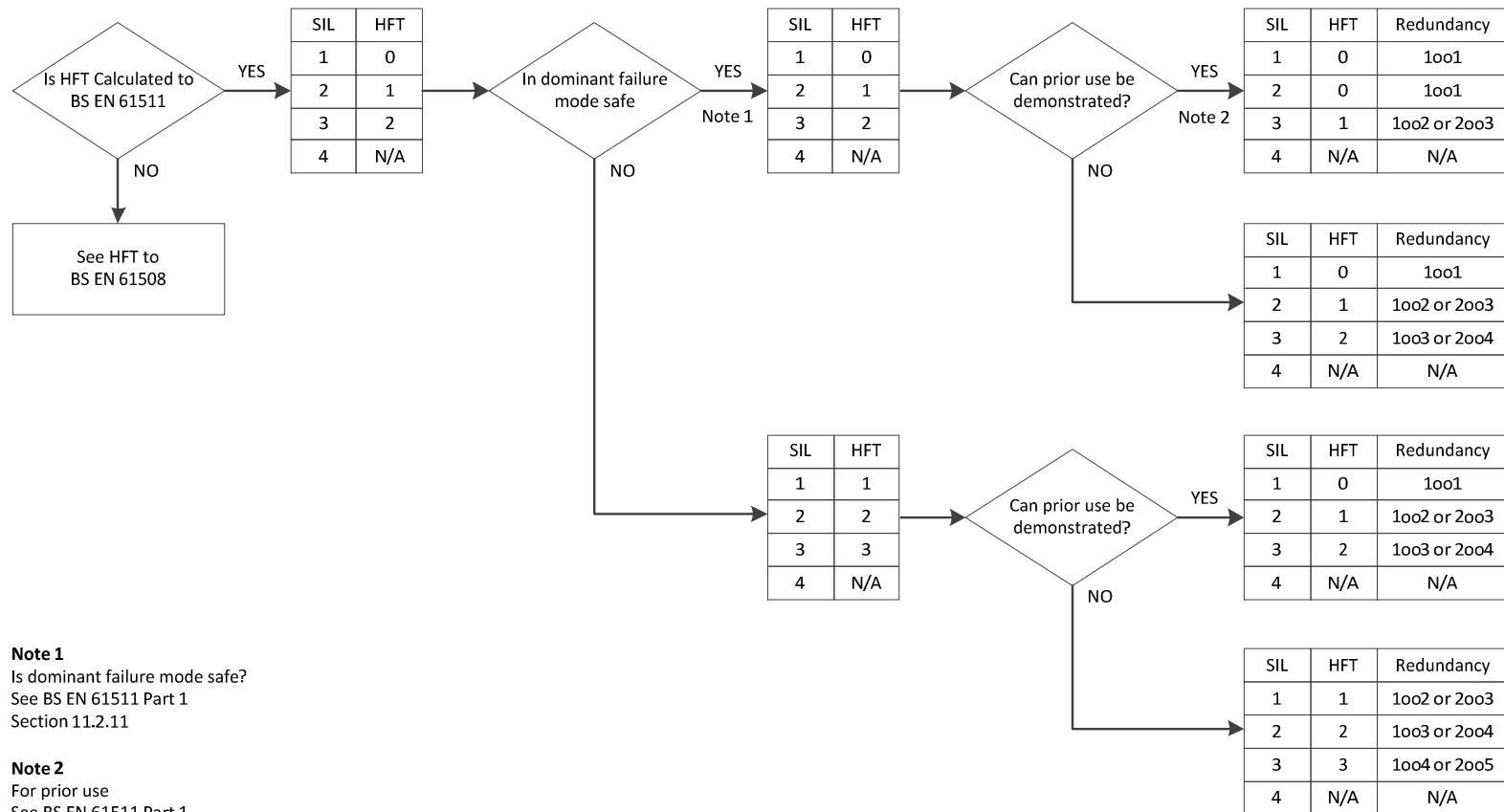
CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

The decision process for the hardware fault tolerance requirements for sensors, non-programmable logic solvers and final elements is illustrated in Figure 2. However, we are still faced with the question, what is meant by “Prior use“?

Figure 2 Hardware Fault Tolerance Flowchart to BS EN 61511 (For Sensors, Final Elements and Non-Programmable Logic Solvers)



3. PRIOR USE - DEFINITION

Prior Use is a term defined in BS EN 61511-1 relating to the selection of components or subsystems. For the claim to be made that the selection of components and subsystems has been made on the basis of prior use, there needs to be appropriate evidence available that the components and subsystems are suitable for use in the safety instrumented system under consideration.

The standard requires that the evidence of suitability is based on the following four aspects:

- Consideration of the manufacturer's quality, management and configuration management systems;
- Adequate identification and specification of the components or subsystems;
- Demonstration of the performance of the components or subsystems in similar operating profiles and physical environments;
- The volume of the operating experience.

4. DEMONSTRATING PRIOR USE

BS EN 61511 prior use requirements are based upon providing evidence that the component has suitability for use in a SIF. In the case of field equipment this is achieved by confirming extensive operating experience in an equivalent (or near equivalent) process related system, which may or may not be safety related.

Non safety related data is comparable to safety related data only where the application is similar in terms or duty and environment on both the wetted and non-wetted parts of the component (for example process fluid characteristics [clean, dirty, viscous], temperature, corrosiveness, indoor or outdoor service).

The level of detail required in the assessment should be in accordance with the complexity of the component and with respect to probability of failure required to achieve the required SIL of the Safety Instrumented Function.

In order to evaluate if a component can be considered for inclusion into a Safety Instrumented Function based on prior use, and to provide the evidence, the following requirements must be met:

- The manufacturer of the component has a recognised quality management system in operation (Refer to section 4.1)
- The component has an identifiable specified functionality required for inclusion in the SIF (Refer to section 4.2)
- The component has been used before in an equivalent (or near equivalent) process operation (which may be either safety or non-safety related) (Refer to section 4.3)
- The component has been used in sufficient volume to gain realistic and reliable operating experience (Refer to section 4.4)

This demonstration of Prior Use suitability is an End User activity with respect to a specific Safety Instrumented Function application.

4.1 **Manufacturer's quality, management and configuration management systems**

In order to assess the suitability of the component it is important that it is manufactured by a manufacturer with a proven quality management system and product history. This is important as any documented justification for the component to be classified as suitable through prior use certain information will be required from or about the manufacturer.

There are potentially three routes by which this aspect can be supported:

1. The Quality Management System¹ for manufacture of the component in question has been independently verified by a third party certification body. This would be supported by a third party certificate verifying compliance with relevant standards such as ISO 9001.

2. The Quality Management System¹ for manufacture of a component similar to the one in question has been independently verified by a third party certification body, and would be supported by a third party certificate verifying compliance with relevant standards such as ISO 9001. In addition, the equipment manufacturer (or third party certification body) has performed a quality assurance gap analysis between the component which is intended to form part of the SIF, and the version which has been assessed to identify any differences which may impact a claim of prior use.
3. Where there has been no third party or retrospective assessment of the component, the following information should be available from the manufacturer in order for the duty holder to make an accurate evaluation of the suitability of the component:
 - The suitability of the quality management system
 - The length of time that the manufacturer has been trading
 - The quantity of components that have been manufactured (which may be required where there is limited confidence in the manufacturers quality management system or the component has been manufactured over a limited period of time)
 - Whether the component is still in production
 - If it is still in production, a history of design modifications where this is available
 - The process of revision control that is in place for modifications to the component
 - Availability of operating and maintenance manuals for the component
 - The procedures in place for returns and equipment failure assessments (note that this refers to the procedures in place to monitor returns of failed equipment, and not to the sole use of this information as part of a prior use demonstration)
 - Evidence of and procedures for dealing with component re-call's or safety modifications
 - Evidence of reliability data for the component where this is available

¹ Most manufacturers will have a quality management system and be accredited to a standard such as ISO 9001. Part of this management system should have a modification process which evaluates the impact of reported failures and modifications in order to improve the quality of the devices being manufactured.

Appropriate evidence of design and manufacture to an industry recognised standard should also be provided where possible. For example, an isolation valve situated in a

potentially flammable atmosphere, an appropriate standard such as BS EN 161 Automatic shutoff valves for gas burners and gas appliances, API 553 Refinery control valves and API 607 (ISO 10497) Testing of valves – Fire-type testing requirements would be considered appropriate.

4.2 Identification and specification of the components or subsystems

The desired functionality of the component should be fully defined (i.e. what is the component required to do, and in what environment), and compared to the capabilities of the component as provided by the equipment manufacturer. This should include but not be limited to:

- The required function it is to perform
- Operating range if applicable
- Relevant process conditions:
 - Temperature
 - Pressure
 - Viscosity
 - Chemical Properties
 - Environmental Conditions (for example vibration, EMC, extremes in temperature)
- Response time

Any assessment between the functionality required and the component capabilities should be made in the context of the requirements of the SIF defined in the Safety Requirement Specification (SRS).

4.3 Demonstration of the performance of the components or subsystems in similar operating profiles and physical environments

It is conceivable that a component is to be included into a SIF because it is already providing that functionality in a satisfactory manner, albeit not SIL rated. The component may have also been extensively used in equivalent (or near equivalent) applications at many other facilities.

Where this is the case, relevant and sufficient data should be available in order to confirm that the component has provided service under the conditions which will be demanded by the SIF and to identify any conditions which may be different to that which the component has previously been exposed. The data that should be available is discussed in section Appendix A.

Note: In the case of field devices (for example, sensors and final elements) fulfilling a given function, this function is usually identical in safety and non-safety applications, which means that the device will be performing in a similar way in both type of

applications. Therefore, consideration of the performance of such devices in non-safety applications may be included in the overall volume of operating experience.

4.4 Volume of the operating experience

It is expected that, if the component is to be utilised as prior use, it will have had significant and reliable service in equivalent (or near equivalent) operations. The following data should be available in order for the end user to make this assessment:

- The end-user needs to confirm that the component is on their list of approved equipment¹
- Component reliability records (refer to the guidance provided in EEMUA 222 and HSE SPC 48 for further information relating to component reliability records)
- The number of years that the component has been used in equivalent (or near equivalent) applications at a facility
- The process and environmental conditions that the component has been used at a facility
- The different applications that the component has been used at a facility, where this is relevant to the prior use assessment
- Whether the component has been used at other of the user's facilities
- Records of any modifications that have been necessary on the component
- Records of any failures²

¹ In order to control which components are used in safety applications, the end user should create an approved or recommended vendor document from which to select components. This document should detail all the different types of components along with the manufacturers and vendors from whom those products may be sourced. If there are any restrictions in terms of operating location or service, then this should also be identified within the document. This document should be updated frequently based upon the successful operating experience of components. Components that have had a history of poor reliability should be removed from the list in preference for more reliable devices

² There should be a reliable system in place to detect and record failures to ensure confidence in the failure records. Failures should be readily categorised in terms of safe/dangerous, revealed/unrevealed, the failure type and cause. All failures should be recorded consistently (refer also to Appendix A).

Note: For field devices³, information relating to operating experience is to be recorded in the user's list of equipment approved for use in their facilities, and based on an extensive history of successful performance in safety and non-safety applications. The list of field devices may be used to support claims of experience in operation, provided that

³ Sensors, valves and other devices that are located on the process.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

- the list is updated and monitored regularly;
- field devices are only added when sufficient operating experience has been obtained;
- field devices are removed when they show a history of not performing in a satisfactory manner;
- the process application is included in the list where relevant

For field devices, failure rate information provided by the Manufacturer should not be included as this does not demonstrate qualitative suitability under the user's operating conditions nor does it support a failure rate that relates to the user's operating conditions.

Appendix A Failure rate calculations

In addition to addressing hardware fault tolerance for a Safety Instrumented Function (SIF), it is necessary to demonstrate that the failure measure for the function falls within the range specified in BS EN 61511 for the Safety Integrity Level required for the function. For low demand mode Safety Instrumented Functions this failure measure is the Average Probability of Failure on Demand (PFDavg).

Calculation of the PFDavg for the safety instrumented function uses the dangerous failure rate (λD) for each of the elements that comprise the safety instrumented function, the proof test interval, and a knowledge of the architecture of the function, including voting arrangements for both input and output channels.

The demonstration of prior use by the end user, as discussed earlier, involves the recording of failure information. This recording of failure information provides the opportunity to determine an appropriate failure rate for the devices or components to be used in safety applications.

A.1 Failure rate

For the calculation of PFDavg the best and most appropriate failure rate information comes from the operational experience of the end user (refer to section 4.4).

Where an end user has no operational experience of a new item of equipment, there are other sources of failure data that might be considered. These may include:

- Manufacturers failure rate data
- Generic failure rate data, from sources such as EEMUA, FARADIP, OREDA etc.

However, great care should be taken when using either of these alternative sources. Firstly, manufacturers will almost certainly have no direct experience of the use of the items under conditions similar to those of the end user. Furthermore, the data provided by manufacturers is often simply a synthesised prediction of performance that they are hoping for from the product.

Secondly, with the generic failure rates to be found databases there is no guarantee that the component that the end user is considering will be similar in performance to the database figure. Any use of generic data should have appropriate justification for its appropriateness and should be regarded as a provisional figure until real experience is available to support or reject the figure.

Preferentially end users own failure data should be used to calculate failure rates. This represents the actual reliability of a given component in a given service and operating environment. One mechanism to gather failure rate data for a component is through analysis of records held within a maintenance management system (or equivalent), which should indicate the number of components in use, the period of time the component has been in use for, and record any failures and failure modes during that time. The end user should have confidence in their maintenance management system to ensure that records are kept correctly, and are up to date. As discussed in Section 4.4, the system should sufficiently reliable to be able to accurately detect and record failures

to ensure confidence in the failure records. Failures should be readily categorised in terms of safe/dangerous, revealed/unrevealed, the failure type and cause.

For field equipment such as sensors and final elements, the function of the device is usually the same whether the device has been used in a safety or non-safety application; therefore reliability data from both applications is acceptable. Non safety related data is comparable to safety related data only where the application is similar in terms or duty and environment on both the wetted and non-wetted parts of the component (for example process fluid characteristics [clean, dirty, viscous], temperature, corrosiveness, indoor or outdoor service).

Where failure rate data has been obtained from a maintenance management system, periodic reviews of the data applicable to the component should be performed after it has been deemed suitable for a prior use claim. This will provide additional evidence of suitability, and also provide a mechanism by which previously unidentified failure modes can be detected.

Where evidence derived from an end user maintenance management system is insufficient or not available, the end user may consult with the equipment manufacturer and with other end users (for example through trade bodies such as EEMUA) to ascertain if reliability data is available from similar applications on other sites. Should failure rate and failure modes still not be available from these other sources, the end user may carry out an alternative more formal assessment of the component to ensure the device will perform as required, refer to Sections A.3 - A.4.

The challenge, where non site-specific failure data is to be used, is to demonstrate that the values selected are appropriate for the site in question. In reality, this means using, say, conservative generic failure data for PFDavg calculations and then planning to record site-specific data followed by a review to determine whether the generic or other data used is sufficiently conservative.

A.2 Calculating failure rates

In order to achieve the risk reduction required for a given safety integrity level, the overall reliability and the failure mode of each component needs to be determined. The reliability of the individual components in terms of their probability of failure on demand (PFD) must be added together to determine the overall PFDavg for the SIF. Further guidance on calculating the reliability of a SIF can be found in the following:

- EEMUA 222, Annex F 'Application of BS EN 61511 to safety instrumented systems'
- HSE SPC 48, Annex A and B 'Proof Testing of Safety Instrumented Systems in the Onshore Chemical/Specialist Industry'

The methodology adopted to calculate failure rates should be based on the rigour required, and the data available to perform the calculation. Reference should be made to BS EN 61508 part 6 for a full definition of the calculation methodologies available.

A.2.1 Calculation based on Mean Time Between Failures

The example provided below may produce distorted results if the sample size is small, or detection of failures that have occurred are not identified and recorded in a timely manner. Further, the accuracy of any failure rate calculation is dependent on failures being revealed, and replaced immediately (failures revealed only after a proof test may also distort the calculated results).

Using the data provided by the maintenance management system⁴, or derived from other sources, the Mean Time Between Failures (MTBF) of the component can be derived as follows:

$$\text{MTBF} = (\text{number of hours of operation}) \div (\text{number of failures})$$

The failure rate can be calculated as follows:

$$\lambda = 1/\text{MTBF}$$

For example, a barrier has been in operation for 10 years (87,600 hours). During that period, 5 failures have been recorded, therefore:

$$\text{MTBF} = (87,600) \div (5) = \underline{17,520 \text{ hours}}$$

This calculation may also be applied where the number of samples is increased (i.e. the number of the same component in the same application and environment) but the sample period is over a shortened period of time. For example, there are 10 barriers that have been in operation for 1 year (8,760 hours), during that period, 5 failures have been recorded, in this instance:

$$\text{MTBF} = (10 \times 8,760) \div (5) = \underline{17,520 \text{ hours}}$$

The failure rate (λ) would be:

$$\lambda = 1/17,520 = 0.000057, \text{ or } \underline{5.7 \times 10^{-5} \text{ failures per hour}}$$

Note: this calculation will not work where the number of failures is zero. In this instance, consideration should be given to an approximation to the Poisson distribution curve.

A.2.2 Calculation based on failure data analysis

Where failure rates are available for the component, a more rigorous calculation can be performed to determine the components PFD and Safe Failure Fraction (SFF).

The types of failure that can be attributed to a component can be described as follows:

- Safe Failure – a failure that when it occurs causes the system to perform the function which puts the system into the safe state, this is performed without a demand from the process and is often referred to a nuisance or spurious trip. Safe failures can further be categorised as either:

⁴ When using maintenance records for prior use evidence, the end user should be able to demonstrate that the records are sufficiently robust and statistically significant

- Safe detected (SD)
- Safe undetected (SU)
- Dangerous Failure - a failure that when it occurs does not cause the system to perform the function which puts the system into the safe state, a failure that occurs when the system fails to operate when the process puts a demand onto it. Dangerous failures can further be categorised as either:
 - Dangerous detected (DD)
 - Dangerous undetected (DU)

Dangerous undetected (DU) failures can only be identified on an actual process demand or by proof testing (providing the proof test is designed to detect the failure).

The four different failure modes are described in reliability modelling as follows:

λ_{SU} , Safe undetected failure

λ_{SD} , Safe detected failure

λ_{DU} , Dangerous undetected failure

λ_{DD} , Dangerous detected failure

Using the failure mode data as defined above allows calculation of the PFD and SFF.

For a 1001 component, the average failure of probability on demand (PFD) can be calculated as follows:

$$PFD_{avg} = [(\lambda_{DU}) + (\lambda_{DD})] t_{ce}$$

Where t_{ce} is the channel equivalent mean down time in hours (this is the combined down time for all of the components in the channel of the sub-system), and can be calculated as follows:

$$t_{ce} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_1}{2} + MTTR \right) + \left(\frac{\lambda_{DD}}{\lambda_D} \times MTTR \right)$$

T_1 = Proof test interval (hours)

$MTTR$ = Mean Time to Restore (hours)

Safe Failure Fraction (SFF) can be calculated as follows:

$$\text{Safe Fail Fraction} = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Reference should be made to appendix B for a worked example.

A.3 Assessing the dominant failure mode

Using the data provided by the maintenance management system, or derived from other sources, the dominant failure mode can be determined by performing a high level analysis of the component (note that this does not imply analysis of individual entities that make up the component, for example resistors, capacitors, semiconductors).

It may be sufficient for the dominant failure mode to be determined based on an analysis of the suitability of the component - if it fails to a safe state on loss of input or motive power (for example, air supply, electricity supply), and if there are no known duty vulnerabilities. Where this cannot be established, a more formal review can be undertaken.

An example of an analysis performed on an interface relay component which provides a shutdown signal to a Motor Control Centre (MCC) is given in Table 2 below. Assuming that the failure rate of failure ID #4 is less than that of ID #1 to #3, it can be seen that the *dominant* failure mode is to the Fail To Safe mode (FTS).

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

ID	Component Description	Function	Failure Mode	Sub-system Effects	Detection Method	Detected	Failure Rate	FTD/FTS	Mitigation
1	Interface relay	Provides shutdown function to MCC	Fail to respond (Coil open Circuit)	Open circuit is the shutdown condition for the MCC	Hardwired logic circuit	Immediate	0.0002	FTS	All connected devices will be driven to safe state. Proof Test shall also identify failed relay.
2	Interface relay	Provides shutdown function to MCC	Fail to respond (Coil Short Circuit)	Coil Short Circuit will de-energise the contacts, which is the shutdown state for the MCC	Hardwired logic circuit	Immediate	0.0002	FTS	All connected devices will be driven to safe state. Proof Test shall also identify failed relay.
3	Interface relay	Provides shutdown function to MCC	Contacts failed open circuit	Open circuit is the shutdown condition for the MCC	Hardwired logic circuit	Immediate	0.00003	FTS	All connected devices will be driven to safe state. Proof Test shall also identify failed relay.
4	Interface relay	Provides shutdown function to MCC	Contacts failed short circuit	None	None	Latent	0.00001	FTD	Proof Test is required to identify failed relay.

Table 2 – Example Failure Modes Analysis

A.4 Other techniques for calculating failure rates

Where no failure rate data is available, either from the end users or equipment manufacturers it may be necessary to perform a detailed analysis of the component using such techniques as Failure Modes, Effects and Diagnostic Analysis (FMEDA). Any such analysis should only be completed by a suitably independent and competent person. Even then, there is no guarantee that any failure rate derived from such an exercise will match eventual experience.

A.5 Systematic capability

Systematic capability is mentioned in BS EN 61511, but is discussed in detail in BS EN 61508⁵. It is particularly relevant in relation to items of equipment containing software. The techniques and measures that have been employed during the development of the software limit the safety integrity level that can be claimed for a safety instrumented function that uses an equipment item containing software. BS EN 61508-2 relating to hardware and BS EN 61508-3 relating to software contain tables of techniques and measures and the safety integrity levels to which they apply.

It should be noted that this topic is not related to Prior Use demonstration.

A.6 Safety manuals

The Safety Manual is mentioned in BS EN 61511, and Part 1 defines Safety Manual as “safety manual: manual which defines how the device, subsystem or system can be safely applied”.

Note: This could be a stand-alone document, an instructional manual, a programming manual, a standard document, or included in the user document(s) defining application limitations.

However, it is a new significantly more prominent requirement in BS EN 61508 Edition 2. BS EN 61508 Edition 2 introduces a new normative requirement in Part 2, Annex D “Safety Manual for Compliant Items”. It defines the purpose of the Safety Manual as, “The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard”.

In BS EN 61508-3 Edition 2, Annex D, there are further normative requirements for the safety manual with respect to software, “Safety manual for compliant items – additional requirements for software elements”. This annex makes it clear that the safety manual may comprise solely the manufacturer’s documentation, if that is sufficient to meet the new normative BS EN 61508 Edition 2 requirements, or it should be created as part of the design of the safety related system.

Thus, the safety manual is documentation that is produced by the supplier or the system integrator.

⁵ BS EN 61508 Edition 2 Published 2010

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

However, it should be noted that the safety manual does not relate to “Prior Use” and BS EN 61508 Edition 2 does not even discuss the term “Prior Use”.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix B Worked example

Basis of Analysis – Example ^{See Footnote 6}

Data Gathering of Failure Data

A ball valve manufactured by the Mucky Valve Company, Model Number MD 12656 has been utilised throughout the Tank Farm area in both process and safety critical applications since 1998 up to and including 2011. Throughout that period there have been no manufacturer design changes and no systematic failures have been uncounted.

Total number of valves in service = 163

Combined operational service: Number of valves multiplied by years of operation per valve = 960 component years

The following table provides an extract of all failures involving all the 163 valves from 1998 to 2011.

Failure data for ball valves (BA) of the same manufacture a)

Tag Number	Failure Record	Date	Duty	Service	Classification	Failure	Reason for Failure	Event	SD	SU	DD	DU	Remarks	Maintenance/Repair	MTTR
XV10098	1998/034	13/04/1998	Tank 98 Import Valve	Diesel	Clean	Packing Leaks Noticed	Insufficient tension on packing	Fail Safe	1				Failure noted at visual inspection. No safety related issues, valve operation unaffected.	Routine Maintenance	<30mins
XV10101	1999/02	16/02/1999	Tank 101 Import Valve	Diesel	Clean	Packing Leaks Noticed	Insufficient tension on packing	Fail Safe	1				Failure noted at visual inspection. No safety related issues, valve operation unaffected.	Routine Maintenance	<30mins
XV10014	1999/09	21/06/1999	Tank 14 Import Valve	Gas Oil	Clean	Long Valve closure time noticed. High friction on shaft	High tension on Packing	Possible Dangerous Failure			1		Failure noted at visual inspection. Safety related issues, valve operation affected.	Routine Maintenance	<1 hour
XV10031	2000/56	18/12/2000	Tank 31 Import Valve	Gasoline	Clean	Valve Shaft Sheared	Torque too high. Valve Seized.	Fail to Danger. However detected on proof test				1	Mechanical Failure noted at proof test under flowing process conditions - Safety Related	Valve Replacement	<8 hours
XV10097	2001/01	03/01/2001	Tank 97 Export Valve	Diesel	Clean	Valve not closed 100%	Build up of material on shaft bearing	Possible Dangerous Failure				1	Failure noted at proof test. Safety related issues, valve operation marginally affected. Consideration given to reorientation of valve from vertical	Valve Replacement and maintenance prior to re-use.	<8 hours
XV10001b	2001/07	12/05/2001	Tank 1 Export Pump Discharge Isolation valve	Additive	Clean	Tight Shut-off not achieved	Solids in the additive causing erosion of the valve and seat	Possible Dangerous Failure				1	Failure noted during operation. Safety related issues, valve operation affected. Valve specification modified for all additive valves.	Valve Replacement	24 hours

Figure 1 – Typical Failure Report

⁶ Please note this example is fictitious and the data used is to illustrate a methodology for compiling and analysing field reliability data. There are alternate methods that can be employed and this paper in no way implies this is the best or only technique.

Calculations

There are many sources and techniques for performing reliability calculations. Various formulae and techniques can be found in BS EN 61508 and BS EN ISO 14224, to name just two. There are also many technical publications on Reliability Assessments which provide further calculations.

For the purpose of this example, two techniques have been demonstrated, the first example utilising a Mean Time between Failure calculation and the second utilising formulae within BS EN 61508 for a 1oo1 system.

Calculation Method 1 - Failure Data MTBF Calculation for 1oo1

Total number of dangerous failures = 1 ^{See Footnote 7}

Thus the MTBF is $\frac{960}{1}$ years = 960 years

Basic Formula for converting MTBF to failure rate

$$\lambda = \frac{1}{MTBF}$$

Converting MTBF to dangerous failure rate (λ_{DU}) = $\frac{1}{MTBF} = \frac{1}{960}$ per year = 1.04×10^{-3} per year

Simplified PFD Calculation ^{See Footnote 8}

Approximate $PFD_{(avg)} = \lambda_{DU} \times \frac{TI}{2}$ (Where TI is the proof test interval in years)

For this case, assuming TI = 1 year then:

$$PFD_{(avg)} = (1.04 \times 10^{-3}) \times \left(\frac{1}{2}\right)$$

$$PFD_{(avg)} = 5.2 \times 10^{-4}$$

Complete PFD Calculation

$$\begin{aligned} PFD_{(avg)} &= 1 - \left(\frac{1}{\lambda_{DU}} \times TI\right) \times (1 - e^{-(\lambda_{DU} \times TI)}) \\ &= 1 - \left(\frac{1}{1.04} \times 10^{-3}\right) \times (1 - e^{-(1.04 \times 10^{-3})}) \\ &= 1 - (961.5 \times (1 - 0.99896)) \end{aligned}$$

$$PFD_{(avg)} = 5.19 \times 10^{-4}$$

⁷ Note – Calculation will not work if there are no dangerous failures recorded and is only valid when repair rate is much greater than failure rate.

⁸ The theory behind the formula is developed in Reliability, Maintainability and risk by David J Smith and based upon algebraic simplifications of Markov models.

Calculation Method 2 – BS EN 61508 1001 Calculation

For the same case (with all failures documented).

Using the basis of 960 component years provides:

Dangerous Undetected 1 in 960 years

$$\lambda_{DU} = \frac{1}{960} = 1.04 \times 10^{-3} \text{ per year} = \frac{1.04 \times 10^{-3}}{8760} = 1.2 \times 10^{-7} \text{ per hour (118 FITS)} \text{ See Footnote 9}$$

Dangerous Detected 3 in 960 years

$$\lambda_{DD} = \frac{3}{960} = 3.10 \times 10^{-3} \text{ per year} = \frac{3.10 \times 10^{-3}}{8760} = 3.6 \times 10^{-7} \text{ per hour (356 FITS)}$$

Safe Detected 2 in 960 years

$$\lambda_{SD} = \frac{2}{960} = 2.08 \times 10^{-3} \text{ per year} = \frac{2.08 \times 10^{-3}}{8760} = 2.4 \times 10^{-7} \text{ per hour (237 FITS)}$$

Safe Undetected = $\lambda_{SU} = 0$

$$\lambda_D = 118 + 356 \text{ FITS } (4.74 \times 10^{-7} \text{ per hour})$$

Assuming perfect testing with all failures repaired to original condition:

Reference: BS EN 61508-2:2010 Annex C

$$\text{Safe Fail Fraction} = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

$$\text{Safe Fail Fraction} = \frac{237 + 0 + 356}{237 + 0 + 356 + 118}$$

$$\text{Safe Fail Fraction} = \frac{593}{711}$$

$$\text{Safe Fail Fraction} = 0.83$$

Reference: BS EN 61508-6:2010 B.3.2.2.1 1001

From the failure data records the following can be quantified:

$$T_1 = \text{Proof Test Interval } 1 \text{ year} = (8760 \text{ hours})$$

$$\text{MTTR} = \text{Mean Time to Restore } \sum \frac{0.5 + 0.5 + 1 + 8 + 8 + 24}{6} = 7 \text{ hours}$$

Using the formula:

$$\text{PFD}_{\text{avg}} = [(\lambda_{DU}) + (\lambda_{DD})] t_{ce}$$

⁹ Failures In Time (FIT) is the number of failures that can be expected in 1×10^{-9} (E-09) failures per hour.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Where:

$$t_{ce} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_1}{2} + \text{MTTR} \right) + \left(\frac{\lambda_{DD}}{\lambda_D} \times \text{MTTR} \right)$$

t_{CE} – Channel equivalent mean down time (hour)

(this is the combined down time for all the components in the channel of the sub-system).

$$t_{ce} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_1}{2} + \text{MTTR} \right) + \left(\frac{\lambda_{DD}}{\lambda_D} \times \text{MTTR} \right)$$

$$t_{ce} = \frac{1.2 \times 10^{-7} \text{ per hour}}{4.74 \times 10^{-7} \text{ per hour}} \times \left(\frac{8760 \text{ hours}}{2} + 7 \text{ hours} \right) + \left(\frac{3.6 \times 10^{-7} \text{ per hour}}{4.74 \times 10^{-7} \text{ per hour}} \times 7 \text{ hours} \right)$$

$$t_{ce} = (0.253 \times 4387) + (0.76 \times 7 \text{ hours})$$

$$t_{ce} = (1110) + (5.3 \text{ hours})$$

$$t_{ce} = 1115 \text{ hours}$$

$$\text{PFD}_{avg} = [(\lambda_{DU}) + (\lambda_{DD})] t_{ce}$$

$$\text{PFD}_{avg} = [1.2 \times 10^{-7} \text{ per hour} + 3.6 \times 10^{-7} \text{ per hour}] \times 1115 \text{ hours}$$

$$\text{PFD}_{avg} = 5.3 \times 10^{-4}$$

As with the result of any calculation, a sanity and sensitivity check should be conducted to ensure that the results are realistic. It is often a practise to provide a statistical analysis of uncertainties.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix C Abbreviations

Abbreviation	Description
BVAA	British Valve and Actuators Association
CA	Competent Authority
CDOIF	Chemical and Downstream Oil Industries Forum
EEMUA	Engineering Equipment and Materials Users Association
EMC	Electromagnetic Capability
FARADIP	Failure Rate Data in Perspective
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FTS	Fail To Safe
HFT	Hardware Fault Tolerance
HSE	Health and Safety Executive
MCC	Motor Control Centre
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
PFD	Probability of Failure on Demand
PSLG	Process Safety Leadership Group
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
UKPIA	United Kingdom Petroleum Industry Association

Appendix D Other relevant publications

Further information relating to prior use can be found in the following publications

- 1) BS EN 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- 2) BS EN 61511, Functional safety - Safety instrumented systems for the process industry sector
- 3) Safety and Environmental Standards for Fuel Storage Sites, Process Safety Leadership Group Final Report
- 4) ISA-TR84.00.04, Guidelines for the Implementation of IEC61511

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Peter Davidson (Chair)	UKPIA
Dave Ransome	P&I Design Ltd.
Alan G King	ABB
Ian Neve	Total
Stuart Williamson	Petroplus
Keith Willett	Petroplus
Mike Cook	Simon Storage
Neil Waller	INEOS
Ed Fergus	Health and Safety Executive
Peter Hirst	Rotork
Peter Churm	British Valve and Actuators Association

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	30-June-2011	Peter Davidson
1	All	Updated following working group review	08-July-2011	Peter Davidson
2	All	Updated following working group second review	15-Nov-2011	Peter Davidson
3	All	Updated following comments received through CDOIF members and Competent Authority stakeholder reviews	20-April-2012	Alan G King, Dave Ransome, Peter Davidson
4	All	Updated following final stakeholder review	13-July-2012	Peter Davidson

CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Leak Detection

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members this guideline on available leak detection techniques for Above-ground Storage Tanks (AST).

The intent of this document is to provide a reference for those organisations wishing to consider the use of leak detection systems to provide mitigation against the loss of product from an AST.

It is not the intention of this document to replace any existing corporate policies or processes. The intent is to provide a reference to users to help in the selection of appropriate leak detection techniques.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to leak detection.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Leak Detection".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

It should be understood that this document does not explore all possible options for leak detection, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

1.	EXECUTIVE SUMMARY.....	4
2.	INTRODUCTION AND SCOPE.....	5
3.	TECHNIQUES FOR LEAK DETECTION.....	6
3.1	Gas detection within the tank bund.....	9
3.2	Tank base perimeter/bund floor point detectors.....	10
3.3	Sump/interceptor point or interface detectors.....	11
3.4	Hydrocarbon detection tapes installed in the bund floor or underneath the tank.....	12
3.5	Under tank membrane with tell-tail leak detection.....	13
3.6	Interspace loss of vacuum detection.....	14
3.7	Tank level gauging with product loss alarm.....	15
3.8	Point or interface detection at floating roof drain valve outlet.....	16
3.9	Point or interface detection at bund drain valve outlet.....	17
3.10	Point or interface detection at tank water draw valve outlet.....	18
4.	RISK REDUCTION CONSIDERATION.....	19
4.1	Defining the mitigation layer.....	20
4.2	Claiming risk reduction.....	21
	Abbreviations.....	22
	Other relevant publications.....	23
	Acknowledgements.....	24
	Revision History.....	25

1. EXECUTIVE SUMMARY

Hazardous substances which are stored in above-ground storage tanks could have the potential to pollute the environment or harm people if the primary containment measure in which they are stored (i.e. the tank) fails.

Leak detection is one method by which hydrocarbons can be detected should primary containment fail. Early indication of the failure may ensure that mitigation measures to prevent escalation of the scenario can be deployed quickly.

The final report of the Process Safety Leadership Groups (PSLG) safety and environmental standards for fuel storage sites was published in December 2009. Part 2 of that report provides limited guidance on the use of gas and liquid detection systems to detect overflows from a bulk storage tanks. A research report commissioned by the Health and Safety Laboratory (HSL), entitled 'A review of leak detection for fuel storage sites, ECM/2008/08' provided further guidance.

As part of its role to deliver improvements in health, safety and the environment, the CDOIF Process Safety Work-stream agreed to examine the types of leak detection that had been successfully implemented in the UK. A working group was commissioned to develop this guideline to assist duty holders in the selection of appropriate techniques and what impact these systems may have in terms of risk reduction.

There are different leak detection methodologies available, which each have their own strengths and weaknesses. Methodologies considered in terms of their benefits, limitations and indicative costs are described in section 3, Techniques for Leak Detection.

Leak detection systems may reduce the risk to people or the environment. They could be considered as a further layer of protection against specific scenarios or be considered a more cost effective risk reduction technique as part of an ALARP (As Low As Reasonably Practicable) demonstration. The possibility of spurious trips will discourage their use in automatic systems, whether in the Basic Process Control System (BPCS) or Safety Instrumented System (SIS). As per other guidance, any claims for risk reduction as an additional mitigation barrier will require justification in terms of clearly defined operating procedures and emergency responses.

2. INTRODUCTION AND SCOPE

Leak detection in the context of this guidance relates to the detection of hydrocarbons following the failure of primary containment. Primary containment inside a bund consists of the tank shell and associated pipe work. Primary containment may fail in any of the following ways:

- The tank is over-filled, resulting in loss of product from the top of the tank, or through roof vents
- Failure of the tank floor
- Failure of the tank wall joints
- Catastrophic tank failure
- Failure of pipe-work associated with the tank
- Failure of pipe-work running through the bund

The risk of these failures occurring can be reduced significantly through measures such as good inspection, maintenance and repair processes, and where appropriate the installation of preventative systems such as overfill protection. Leak detection systems can complement these other measures to reduce the risk further, or they may also provide an alternative means of risk reduction when other systems or processes are disproportionate in terms of the risk reduction achieved versus the cost.

This guidance should not be interpreted as a requirement to install such systems, but instead provide a useful reference to those duty holders who may be considering the installation of leak detection for the reasons stated. Other techniques are available, and cost will be variable depending on the technology adopted and existing site infrastructure. Consideration should also be given to the sensitivities of any installed system to spurious trips during routine operations (such as flushing), and procedures should be updated accordingly.

The following sections provide an overview of typical leak detection systems adopted by the downstream oil industry in the UK – this list is not exhaustive and other techniques may also be available.

3. TECHNIQUES FOR LEAK DETECTION

Leak detection may be considered as one mechanism for the early detection of failure of primary containment. Typical examples of Hydrocarbon detection techniques include:

- Gas detection (point sensors)
- Point detectors placed around the circumference of the tank or in the bund floor
- Interface or level detectors placed in an interceptor or sump
- Hydrocarbon detection 'tapes' installed in the bund floor, or underneath the base of the tank
- Under tank membrane with tell-tail leak detection
- Interspace loss of vacuum detection
- Tank level gauging with product loss alarm (wet-stock reconciliation)
- Point or interface detectors located at the outlet to a floating roof drain valve
- Point or interface detectors located at the outlet to a bund drain valve
- Point or interface detectors located at the outlet to a tank water draw valve

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

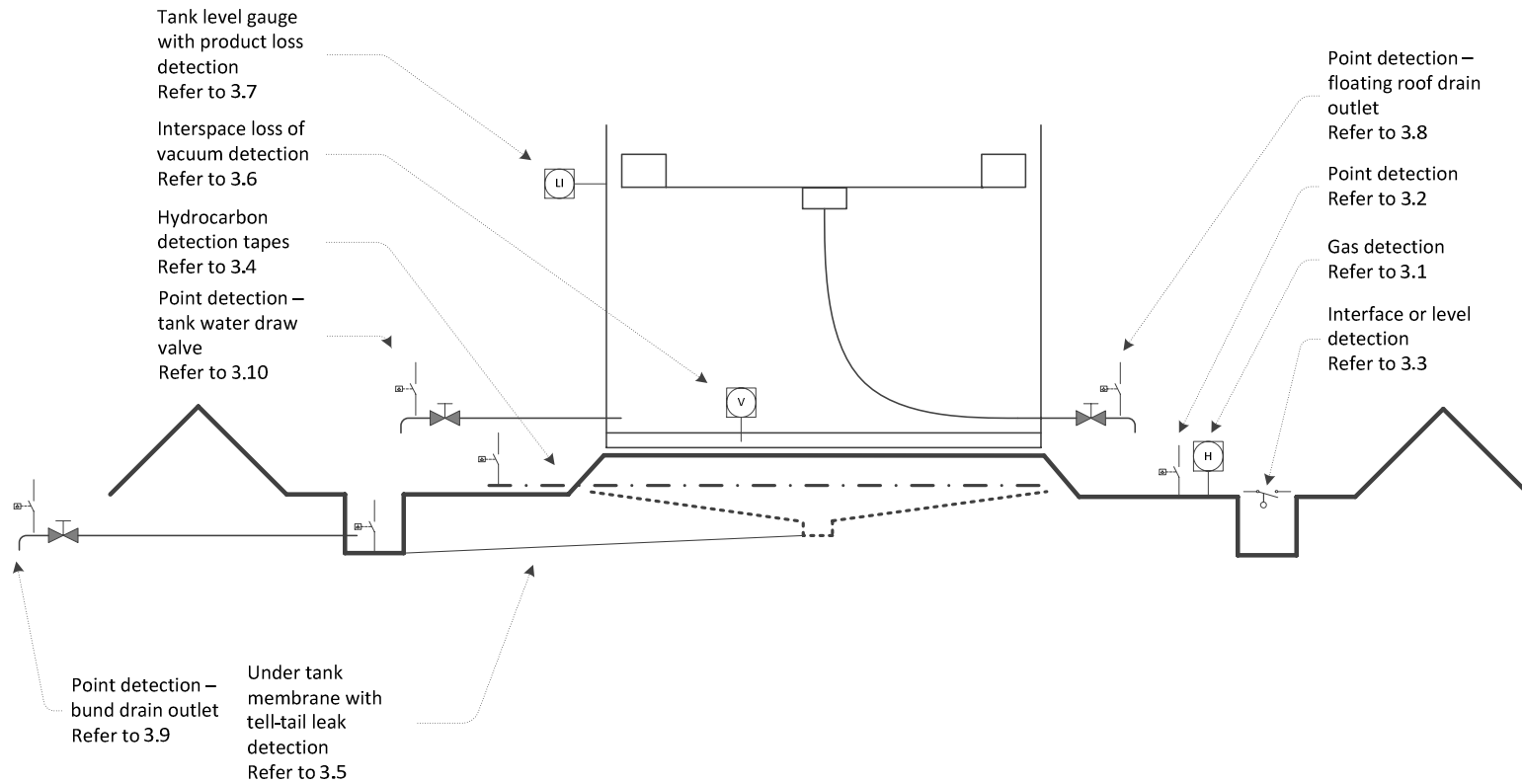


Figure 1 – Examples of Hydrocarbon detection points

When reviewing the applicability of leak detection techniques, it is important to consider the circumstances under which it will be used, and the scenario(s) it is intended to detect, for example:

- Installing liquid or gas detection is unlikely to have an effect on reducing the risk to people or the environment following catastrophic tank failure, or loss of very large volumes of product after the failure of wall joint as the volumes lost would be significant over a very short space of time. However smaller leaks may be a pre-cursor to more significant failures, and therefore leak detection may prove beneficial.
- Leak detection is likely to be beneficial in mitigating the risk arising from tank over-fill, or from other significant tank leaks.
- Gas detection may be effective in detection of vapour formation following over-topping thus limiting the size of a Flammable Vapour Cloud (FVC), but it is unlikely to be effective in detecting a leak from the base of the tank.
- The positioning of gas detectors can be impacted by prevailing weather conditions. Gas detectors will be much less sensitive to leaks down-wind of the detector.

Reference should be made to section 4, Risk Reduction Consideration, for further information on the benefits that could be claimed, and the restrictions that should be applied when considering the chosen leak detection system in a risk assessment.

Installations appropriate to new build tanks may not be appropriate for tanks which are refurbished.

The following sub-sections provide an analysis of typical leak detection techniques, their benefits and limitations and indicative cost.

3.1 Gas detection within the tank bund

Usage	Potential benefits	Considerations	Indicative Cost
<p>Gas detectors positioned within the bund can be used to detect vapour cloud formation caused either from tank over-fill or failure of the tank shell (where these failures are located in such a place as to cause cascade of product likely to form a vapour cloud)</p> <p>Early detection of loss of containment could reduce the size, or prevent the formation of a large flammable vapour cloud which may lead to a Vapour Cloud Explosion (VCE)</p> <p>Early detection of loss of containment could reduce the risk of a pool fire by detecting vapour within the bund before ignition.</p>	<p>Gas detection is a well proven technology, which is generally robust and cost effective where a suitable integrity, reliability or preventative maintenance strategy is applied.</p>	<p>Effective positioning of detectors is important as the spread of a vapour cloud will be directly affected by weather conditions.</p> <p>Suitable technology should be selected depending upon the product and conditions to be detected - technology includes point and open path. Further information can be found here: http://www.hse.gov.uk/pubns/gasdetector.pdf</p> <p>Gas detection would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to periodic testing.</p>	<p>Medium</p>

3.2 Tank base perimeter/bund floor point detectors

Usage	Potential benefits	Considerations	Indicative Cost
<p>Liquid point detectors positioned around the base of the tank, or in the bund floor (typically in the lowest gradients of the bund floor) can be used to detect loss of containment into the bund, either from tank over-fill or failure of the tank shell. In some instances this may also detect loss of containment from the tank floor, though this will be dependent on the topology and geology of the bund underneath the tank</p> <p>Early detection of hydrocarbons in the bund could reduce the size, or prevent the formation of a large flammable vapour cloud which may lead to a VCE</p> <p>Early detection of hydrocarbons in the bund may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund may also provide an early indication of loss of containment, reducing the risk of a Major Accident to the Environment (MATTE)</p>	<p>Liquid point detectors can provide an early indication of hydrocarbons within the bund, reducing the escalation of several scenarios which if undetected could lead to a VCE or a MATTE.</p>	<p>Liquid point detection may be subject to spurious trips due to bund materials which may already be contaminated, or through rain water collecting in the bund.</p> <p>Detection is only effective at the point of measurement, and therefore the positioning and number of detectors require careful consideration</p> <p>Care should be taken when claiming credit for the reduction in size of a flammable vapour cloud, as liquid would only be detected in the bund if the tank was already overflowing – giving time for the vapour cloud to form.</p> <p>Liquid point detection within the bund would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to periodic testing.</p>	<p>Medium</p>

3.3 Sump/interceptor point or interface detectors

Usage	Potential benefits	Considerations	Indicative Cost
<p>Liquid Point Detectors positioned in the bund sump or interceptor can come in two forms:</p> <ol style="list-style-type: none"> 1. Simple level switch (fitted with a displacer for greater accuracy), or 2. Interface level detectors <p>These technologies can be used to detect loss of containment into the bund either from tank over-fill or failure of the tank shell. In some instances this may also detect loss of containment from the tank floor, though this will be dependent on the topology and geology of the bund underneath the tank</p> <p>Early detection of hydrocarbons in the bund sump or interceptor may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund sump or interceptor may also provide an indication of loss of containment, reducing the risk of a MATTE</p>	<p>Bund sump or interceptor liquid/interface detectors can provide an early indication of hydrocarbons within the bund, reducing the escalation of several scenarios which if undetected could lead to a MATTE.</p> <p>Interface level detectors in particular have been shown to be very reliable and easy to maintain.</p>	<p>Simple level switches in particular can be subject to spurious trips due to rain water collecting in the bund.</p> <p>Liquid Point Detection is only effective at the point of measurement, and therefore detection will only occur where product collects in the bund sump/interceptor</p> <p>Bund sump or interceptor liquid/interface detection within the bund would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to period testing.</p> <p>Hydrocarbon detection may be linked with executive action (for example closing an automated valve) if failure is likely to result in hydrocarbon release into the bund</p>	<p>Low</p>

3.4 Hydrocarbon detection tapes installed in the bund floor or underneath the tank

Usage	Potential benefits	Considerations	Indicative Cost
<p>Hydrocarbon tape/cable detectors positioned underneath the tank floor can be used to detect loss of containment from the tank floor.</p> <p>Early detection of hydrocarbons underneath the tank may provide an indication of loss of containment, reducing the risk of a MATTE</p>	<p>Tape/cable detectors are an effective method for detecting leaks from the tank floor, which otherwise may be undetected for some time.</p> <p>Arranged in a lattice format, this method of detection may also provide some accuracy as to the location of the leak within the tank floor.</p> <p>Tape or cable detectors can either be installed underneath the tank base (typically using a boring technique) or between two floors of a double bottomed tank.</p>	<p>Tape/cable detectors can be sacrificial, and would require replacement following detection.</p> <p>There is a risk of premature failure of the system if installation is not carefully planned and executed.</p> <p>Care should be taken in assessing the contamination that may already exist underneath the tank before installation</p> <p>Tape/cable detection underneath the tank would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to period testing.</p>	<p>High</p>

3.5 Under tank membrane with tell-tail leak detection

Usage	Potential benefits	Considerations	Indicative Cost
<p>Liquid point detectors positioned at the outlet of under tank floor/over membrane leak detection pipes can be used to detect loss of containment into the bund from tank floor failure.</p> <p>Early detection of hydrocarbons underneath the tank may provide an indication of loss of containment, reducing the risk of a MATTE</p>	<p>Liquid point detectors can provide an early indication of hydrocarbons within the bund, reducing the escalation of several scenarios which if undetected could lead to a MATTE.</p>	<p>Liquid point detection may be subject to spurious trips due to bund materials which may already be contaminated, or through rain water collecting in the bund.</p> <p>Detection is only effective at the point of measurement, and therefore the positioning and number of detectors require careful consideration</p> <p>Under tank membranes are primarily concerned with detecting tank floor leaks. Other leaks leading to FVC are unlikely to be detected.</p> <p>Liquid point detection within the bund would form part of a mitigatory protection layer – routine operator monitoring or alarm activation would be required to initiate further action and/or emergency response, however the system indicates failure of only one of the containment systems, and therefore immediate response may not be required. Any further activity would be required to be clearly defined and subject to periodic testing</p>	<p>Low/ Medium</p>

3.6 Interspace loss of vacuum detection

Usage	Potential benefits	Considerations	Indicative Cost
<p>Loss of vacuum on vacuum annulus systems installed on tank floors can be used to detect loss of containment from the tank floor.</p> <p>Early detection of hydrocarbons underneath the tank may provide an indication of loss of containment, reducing the risk of a MATTE</p>	<p>Loss of vacuum techniques are an effective method for detecting leaks from the tank floor, which otherwise may be undetected for some time.</p> <p>Loss of vacuum detection systems are installed in the space between an internal epoxy/steel tank floor and the external tank floor.</p>	<p>Loss of vacuum detection systems would form part of a mitigatory protection layer – routine operator monitoring or alarm activation would be required to initiate further action and/or emergency response, however the system indicates failure of only one of the containment systems, and therefore immediate response may not be required. Any further activity would be required to be clearly defined and subject to periodic testing</p>	<p>Medium/ High</p>

3.7 Tank level gauging with product loss alarm

Usage	Potential benefits	Considerations	Indicative Cost
<p>Liquid level monitoring (wet-stock reconciliation) of the product within the tank can be used to detect a loss of containment over a period of time (for example, where product is leaking from the tank).</p> <p>Monitoring of the tank level for loss of containment is only relevant during the period when the product in the tank is stationary (for example when no transfers into or out of the tank are in progress, such as when a terminal is closed overnight).</p> <p>Tank gauging systems can detect comparatively small leaks of product loss</p> <p>Early detection of hydrocarbons in the bund could reduce the size, or prevent the formation of a large flammable vapour cloud which may lead to a VCE</p> <p>Early detection of hydrocarbons in the bund may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund may also provide an early indication of loss of containment, reducing the risk of a Major Accident to the Environment (MATTE)</p>	<p>Liquid level monitoring is a well proven technology with proven reliability and repeatability for accuracy</p>	<p>Monitoring is normally via the tank gauging system</p> <p>The system should be configured with a change in level (discrepancy) alarm that is relayed to relevant personnel who can take appropriate action/. This could either be the central control room or security office.</p>	<p>Low</p>

3.8 Point or interface detection at floating roof drain valve outlet

Usage	Potential benefits	Considerations	Indicative Cost
<p>Leak detection installed on the outflow from a floating roof drain valve can provide indication of a failure of the drain line (hose or flexible joint) or a sunken floating roof.</p> <p>Early detection of hydrocarbons in the bund may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund may also provide an early indication of loss of containment, reducing the risk of a Major Accident to the Environment (MATTE)</p>	<p>Cost effective when installed in drain lines from the outlet of the drain valves</p>	<p>Functionality is only relevant where the policy on the site is to leave the roof drain normally open, in this instance leak detection could be beneficial. The detection will not function if the drain line is closed.</p> <p>Close care and attention is needed during the set-up and commissioning of such systems to prevent spurious alarms and avoid loss of confidence.</p> <p>Detection in the drain line would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to period testing.</p> <p>Hydrocarbon detection may be linked with executive action (for example closing an automated valve) if failure is likely to result in hydrocarbon release into the bund.</p>	<p>Low</p>

3.9 Point or interface detection at bund drain valve outlet

Usage	Potential benefits	Considerations	Indicative Cost
<p>Leak detection installed on the outflow from the bund drain valve can provide indication of over-fill or loss of containment into the bund.</p> <p>Early detection of hydrocarbons in the bund may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund may also provide an early indication of loss of containment, reducing the risk of a Major Accident to the Environment (MATTE)</p>	<p>Cost effective when installed in drain lines from the outlet of the drain valves</p>	<p>Functionality is only relevant where the policy on the site is to leave the bund drain valve normally open, in this instance leak detection could be beneficial. The detection will not function if the drain line is closed.</p> <p>Close care and attention is needed during the set-up and commissioning of such systems to prevent spurious alarms and avoid loss of confidence.</p> <p>Detection in the drain line would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to period testing.</p>	<p>Low</p>

3.10 Point or interface detection at tank water draw valve outlet

Usage	Potential benefits	Considerations	Indicative Cost
<p>Leak detection installed on the outflow from a water drain valve can provide indication of loss of containment into the bund.</p> <p>Early detection of hydrocarbons in the bund may be used to reduce the risk of pool fires.</p> <p>Early detection of hydrocarbons in the bund may also provide an early indication of loss of containment, reducing the risk of a Major Accident to the Environment (MATTE)</p>	<p>Cost effective when installed in drain lines from the outlet of the drain valves</p>	<p>Tank water draw is normally an attended operation, but can take place over long periods of time. In these instances, hydrocarbon detection may be of benefit.</p> <p>Close care and attention is needed during the set-up and commissioning of such systems to prevent spurious alarms and avoid loss of confidence.</p> <p>Detection in the water drain line would form part of a mitigatory protection layer – alarm activation would be required to initiate further action and/or emergency response. This further activity would be required to be clearly defined and subject to period testing.</p> <p>Hydrocarbon detection may be linked with executive action (for example closing an automated valve) if failure is likely to result in hydrocarbon release into the bund</p>	<p>Low</p>

4. RISK REDUCTION CONSIDERATION

Whether or not a leak detection system is installed will be dependent on the benefits that it gives versus the costs of installation and maintenance - this decision should be made by the duty holder when completing a risk assessment for the credible scenarios which could result in loss of containment from an AST. Further guidance relating to risk assessment can be found here:

- For the protection of people, refer to the numerous publications by the Health and Safety Executive (HSE) for COMAH, <http://www.hse.gov.uk/comah/>
- For the protection of the environment, one methodology for environmental risk assessment is provided in the CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments'

The installation of such systems may be appropriate to reduce the risk to people or the environment (or both). They could be considered as a further layer of protection against specific scenarios (for example reducing the risk of the formation of a flammable vapour cloud, or the risk of pollution to an environmental receptor), or be considered a more cost effective risk reduction technique as part of an ALARP (As Low As Reasonably Practicable) demonstration. However as any such system will only indicate the presence of hydrocarbons after they have escaped from the tank, they should only be considered as a mitigation layer.

Whilst leak detection mechanisms could be configured with an automatic action (for example closure of an inlet valve, drain valve or stopping a transfer pump), caution should be taken when considering these systems to be safety related as further mitigatory actions would be required even if the automatic action¹ completed successfully, i.e.:

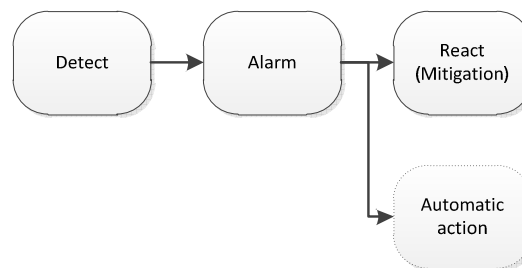


Figure 1 – Leak Detection Actions

These further mitigatory actions (for example emergency response) would themselves be required to have written procedures and be tested in order to claim credit as part of the risk assessment process.

¹ *There is a probability of spurious alarms with some types of leak detection technology used in this application (detection of hydrocarbons in a banded area) therefore due consideration should be given to the robustness of installation before integration with an automated action.*

4.1 Defining the mitigation layer

Before determining the level of risk reduction that can potentially be claimed following the installation of leak detection, it is first important to understand what potential consequences it is intended to mitigate against, and whether it is in support of other systems such as a Basic Process Control System (BPCS) or Safety Instrumented System (SIS).

A risk assessment should determine if further measures are required to reduce the risk to Tolerable if ALARP (TifALARP), and

- Where leak detection is to be considered in support of other systems such as an SIS or BPCS to reduce overall risk (for example its purpose is to mitigate against the formation of a large FVC or the risk to an environmental receptor from over-filling a tank), independence from the BPCS would need to be demonstrated as with other protection/mitigation layers such as independent alarms. Further information on independence can be found in the following publications:
 - Process Safety Leadership Group (PSLG) final report, Appendix 4
 - CDOIF guideline 'Process Safety Leadership Group – Other Products in Scope'
- Where the leak detection system is to be considered to reduce the potential for a MATTE but not in conjunction with other automated systems such as an SIS or BPCS (for example its purpose is to mitigate the risk against a leak from the base of a tank), independence would not need to be demonstrated from the BPCS (or other systems) as the leak detection system is not providing a supporting mitigation layer to others provided by the BPCS. Further information on environmental risk assessments and MATTE definitions can be found in the following publication:
 - CDOIF guideline 'Environmental Risk Tolerability for COMAH Establishments'

When determining the appropriateness of leak detection as a mitigation layer, clear descriptions should be given of the definition of the alarm, where and how it is sounded, who will react to it and how they should react, and how much time is available to react. This review should include consideration of:

- Sounding the alarm in a different location to the Central Control Room, for example security building, to increase independence where necessary from the existing automation systems such as the BPCS and SIS.
- Whether or not there is a need for investigation by local operators should the leak detection system alarm, and how long this would take.
- Standard and Emergency operating procedures which define what needs to be done when the alarm is sounded, for example:
 - Transfer of the substance to another location

- Adding water to the tank (where this is a viable option for the type of substance)
- Shutdown of the process, sub-process or transfer

Note that leak detection introduced as a mitigation layer may reduce the consequence of loss of primary containment, but would not reduce the frequency.

4.2 Claiming risk reduction

The installation of appropriate leak detection, and supporting operational and emergency procedures can contribute to overall risk reduction in any of the following ways:

- Providing a layer of protection (or additional layer of protection) reducing the overall risk to people and the environment to TifALARP
- Providing an additional layer of protection in support of existing systems which may in turn reduce the Safety Integrity Level (SIL) required by a SIS (Note however installation of leak detection does not negate the need for an independent SIS for overfill protection on finished gasoline tanks within the scope of the PSLG)
- Providing the potential for an alternative (subject to ALARP and Cost Benefit Analysis (CBA)) and more cost effective mechanism for reducing the risk of a MATTE as part of an ALARP demonstration

Following existing guidance relating to alarm systems as layers of protection, the claimed risk reduction for leak detection systems can be 0.1 (subject to the requirements laid out in this guideline, and other applicable publications, and appropriate justification). A claim of better than 0.1 would not be credible where an operator response to an alarm/monitoring activity is required, and may be worse depending on the reliability placed on the chosen detection method.

When completing a risk assessment, appropriate conservatism should be applied when determining relevant conditional modifiers and the probability of failure on demand of other independent layers of protection.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations

Abbreviation	Description
ALARP	As Low As is Reasonably Practicable
AST	Above-ground Storage Tank
BPCS	Basic Process Control System
CBA	Cost Benefit Analysis
CDOIF	Chemical and Downstream Oil Industry Forum
COMAH	Control of Major Accident Hazards
EEMUA	Engineering Equipment and Materials Users Association
FVC	Flammable Vapour Cloud
HSE	Health and Safety Executive
HSL	Health and Safety Laboratory
MATTE	Major Accident to the Environment
PSLG	Process Safety Leadership Group
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TifALARP	Tolerable if As Low As is Reasonably Practicable
UK	United Kingdom
UKPIA	United Kingdom Petroleum Industry Association
VCE	Vapour Cloud Explosion

Other relevant publications

Further information relating leak detection techniques can be found in the following publications

- 1) Process Safety Leadership Group, final report – Safety and Environmental Standards for Fuel Storage Sites
- 2) Health and Safety Laboratory – A review of leak detection for fuel storage sites, ECM/2008/08
- 3) EEMUA 159 – User’s guide to the inspection, maintenance and repair of above ground vertical cylindrical steel storage tanks, Third Edition
- 4) EEMUA 183 – Prevention of tank bottom leakage – a guide for the design and repair of foundations and bottoms of vertical, cylindrical, steel storage tanks, Second Edition
- 5) EEMUA 191 - Alarm Systems - A Guide to Design, Management and Procurement
- 6) EEMUA 213 – Emission reduction from oil storage tanks and loading operations, First Edition
- 7) Storage BREF (Best Available Techniques Reference Document), 2006
- 8) Energy Institute Model Code of Safe Practice Part 2
- 9) Energy Institute Environmental Guidelines for Petroleum Distribution Installations

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Peter Davidson (Chair)	UKPIA
Dave Ransome	P&I Design Ltd.
Barrie Salmon	Tank Storage Association
Raman Sridhar	BP
Mike Boothman	Phillips 66
Ian Goldsworthy	Valero
Craig Pugh	Exxon
John Lilley	EEMUA
Carol Pickard	Total
Bruce Hopwood	Shell
Brian Armitage	Petroineos
Andy McCormick	Essar Oil (UK)
David Howard	Environment Agency
Mike Nicholas	Environment Agency

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	20-Feb-2013	Peter Davidson
0.1	All	Project sponsor comments incorporated	21-Feb-2013	Peter Davidson
0.2	All	Updated with working group comments	28-Feb-2013	Peter Davidson
0.3	All	Updated with further working group comments	16-May-2013	Peter Davidson
0.4	All	Updated with final comments from working group	11-June-2013	Peter Davidson
0.5	All	Updated with final comments from CA	1-July-2013	Peter Davidson
0.6	All	Update with CDOIF Stakeholder Comments	29-Aug-2103	Peter Davidson

CDOIF

Chemical and Downstream Oil Industry Forum

Guideline

Terminal Loading Operations Hazard Awareness

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members a guideline on hazard awareness during tanker loading operations at distribution terminal loading racks.

It is not the intention of this document to specify the training or competency needs of drivers or distribution terminal staff, nor replace any existing corporate policies or processes. The intent is to provide a reference for those organisations developing or wishing to review their existing distribution terminal loading operational training and competency needs.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to hazard awareness during distribution terminal loading operations.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Terminal Loading Operations Hazard Awareness".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

This guidance is not intended to be an authoritative interpretation of the law; however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for hazard awareness training, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Contents

FOREWORD	2
CONTENTS.....	3
1. EXECUTIVE SUMMARY.....	4
2. SCOPE	5
3. DISTRIBUTION TERMINAL LOADING OPERATIONS.....	6
3.1 Loading Rack Equipment	6
3.2 Loading Rack Processes.....	6
3.2.1 Training.....	7
3.2.2 Maintaining Competency.....	8
3.2.3 Dealing with a Hazard	9
3.3 Monitoring Performance.....	10
4. LOADING RACK SIGNAGE AND INFORMATION.....	11
ABBREVIATIONS.....	12
GLOSSARY OF TERMS	12
LEGAL CONTEXT.....	13
ACKNOWLEDGEMENTS.....	15
REVISION HISTORY.....	16

1. Executive Summary

A number of overfilling incidents have occurred during the loading of gasoline into road tankers. Overfilling has occurred due to the failure of people and equipment, resulting in an uncontrolled flow and significant quantities of gasoline being lost from containment¹. In each case there were unrecognised deficiencies in the architecture of the loading system which were exposed by a single failure. The deficiencies in the loading system have included the inability of the emergency shutdown system to stop gasoline flow. The majority of these occurrences were due to failure of the flow control valve.

Personnel have been exposed to risks of serious injury during overfilling incidents due to their presence in the spill area. In some cases personnel have purposely entered the spill area during attempts to diagnose faults and to stop the flow of gasoline.

A working group was commissioned under CDOIF to develop a guideline for hazard awareness during terminal loading operations. This guideline is not intended to be prescriptive in defining the individual training and competency needs, but aims to raise awareness within industry of existing good practice, and highlight where appropriate key areas against which duty holders may review their existing systems.

A second working group was commissioned to look into the architectures of overfill prevention systems, this guidance can be found in the CDOIF publication entitled 'CDOIF Guideline – Automatic Overfill Prevention Systems for Terminal Loading Racks'.

Note 1

Each tank compartment's overfill prevention sensor is set to provide ullage of not less than 150 litres between the point of it being tripped and overfilling. This is to ensure that all the product passed by the gantry flow control valve from the triggering of the overfill prevention sensor until flow is ceased will be contained within the compartment (even if the event is triggered at the maximum flow rate)

Note that the overfill prevention system plays no part in ensuring that the tanker is not overloaded nor in ensuring that the maximum degree of filling (ADR 4.3.2.2) has not been exceeded

2. Scope

This document provides guidance to help in raising hazard awareness of all those involved in filling operations at fuel distribution terminals.

Those involved in filling operations can be defined as:

- Drivers – employed through hauliers or directly with oil companies
- Distribution terminal staff and contractors.

This guideline should not be considered a full and comprehensive plan of training or competency requirements, but instead provide an overview of good practice for

- Raising awareness of hazards
- Recognising hazardous scenarios
- Dealing with an incident

Normal filling operations are out of the scope of this document. It is assumed that drivers have the necessary training and competency in the operation of the vehicle and its connections to the distribution terminal loading equipment.

For the purposes of this guidance overfilling means filling a compartment to the point that gasoline flows out of that compartment, for example into a vapour recovery system or through a pressure relief valve.

3. Distribution Terminal Loading Operations

3.1 Loading Rack Equipment

During normal operation, the distribution terminal automation system will transfer product into the tanker compartment, automatically stopping the flow of fuel when the preset volume has been transferred.

The introduction of an overfill prevention system greatly reduces the risk of an overfill. Typically these systems will automatically close a solenoid valve located on the loading rack on detection of any of the following conditions:

- High level detected by the earth/overfill prevention system
- High level in the vapour recovery knock-out pot
- Manual initiation via Emergency Shut Down (ESD) button

The override of these automated systems should be prohibited unless for planned maintenance or repair.

Further information on the design of overfill prevention systems can be found in the CDOIF publication 'CDOIF Guideline – Automatic Overfill Prevention Systems for Terminal Loading Racks'.

Should an overfill or other spill occur, it may be necessary for the driver, or other distribution terminal personnel to take action. Consideration should be given to the following:

- Installation of Emergency Shut-Down (ESD) activation points which are connected to the overfill prevention system. ESD activation points should be positioned and signed appropriately.
- Installation of audible/visual alarms which are activated on initiation of the ESD.
- Installation of Closed Circuit Television (CCTV), with images fed to the Central Control Room (CCR). The CCTV may provide a further mechanism by which a spill can be identified remotely by distribution terminal personnel.
- Installation of a loudspeaker system at each of the loading racks allowing two way communications with the CCR. The loudspeaker system should be positioned appropriately.
- Training of personnel to ensure that they remain vigilant during loading operations (refer to sections 3.2.1, and 3.2.2 for further information).

3.2 Loading Rack Processes

Loading rack processes can be complex, and may well differ from site to site even where those sites are owned and operated by the same company. Understanding how to use the equipment, and the procedures to follow should an incident occur or be suspected is critical to maintaining a high level of safety.

3.2.1 Training

Training is used to provide all those involved in the loading process at a distribution terminal with the necessary skills and knowledge to understand the safe operation of the loading system, emergency procedures, and occupational health and safety requirements. Operators should have processes in place to validate the effectiveness of these training programmes.

Where drivers have not completed a terminal's normal induction procedures (for example "spot loaders") they should be supervised throughout the loading process by a suitably qualified member of the terminal staff.

Reference should be made to the relevant standards, guidance and legal requirements when developing, maintaining and delivering competence based training. Consideration should be given to the following:

- Adopting a standardised training program for companies operating multiple sites to ensure commonality of processes.
- Local differences between sites where standardised training programmes have been adopted; for example the location of ESD push buttons.
- Providing information on how overfills can occur, and how early signs and potential causes can be identified. For example:
 - filling a compartment that already contains fuel that the driver is unaware of or does not take account of,
 - Known returns, where the customer did not take delivery
 - Unknown returns, due to delivery system failure or driver error
 - filling the wrong compartment,
 - failure of equipment intended to automatically stop fuel flow
- A clear procedure of what to do in case of overfill
- A clear procedure of what to do in the event of an ESD and/or Alarms
- Descriptions of the fuel types handled by the distribution terminal Sources of ignition. Examples of what can happen when these are ignited, distinguishing the special hazards presented by gasoline. Subject to risk assessment and the establishment of suitable protocols, these should be accompanied by demonstrations. The use of actual video evidence from incidents can also be used to reinforce safety messages.
- The use of video (for example CCTV footage) evidence may also be used to highlight unsafe practices, for example walking through product spills.

- Recognising the signs that overfill has occurred, through sensory detection and through identification that the automation has not operated as expected (for example meter overrun).
- The importance of reporting any loading problems, near misses and equipment defects to the terminal control room and/or tanker operating company. For example, an overrun of a preset during a loading procedure may be an indication that a flow control valve requires maintenance.
- Positioning of the vehicle. A vehicle parked too close or too far away from the loading gantry may cause manual handling issues when connecting and disconnecting, but could also place undue stress on loading arms and couplings leading to premature failure.

3.2.2 Maintaining Competency

Training is essential in highlighting the hazards associated with filling operations, however it should not be seen as a single activity that needs to be performed only once for new drivers, staff or contractors. Maintaining a high level of competence is an important factor in ensuring a high level of hazard awareness. Consideration should be given to the following:

- Repeating training at pre defined intervals for all personnel.
- Providing refresher training for those who have not visited the distribution terminal for a significant period of time, irrespective of the defined interval for repeat training.
- Periodic assessments to ensure operational tasks are carried out correctly (for example rack loading). This should include an assessment of what to do following overfill or activation of an ESD and/or other alarms.
- Utilising safety observations techniques to ensure correct procedures are being followed. Where unsafe practices are observed, additional training needs should be identified where appropriate.
- The use of regular tool-box talks and where appropriate periodic questionnaires (for example safe unsafe act [SUSA] reporting) to verify that competency has been maintained. Such techniques may also highlight deficiencies in the training program, or areas where further additional training is required.
- A periodic review of the training program to ensure that it is still relevant to current processes and legislation, and takes account of any trends identified during safety observations, tool box talks and assessments.
- Promoting shared learning between companies and other relevant industry sectors, for example through trade association initiatives.

3.2.3 Dealing with a Hazard

Training should provide the necessary information for drivers, staff and contractors at a distribution terminal should overfill occur during a filling operation. Unsafe acts may be due to safety culture issues with those involved in loading activities, rather than deficiencies in training programmes. Good communication and understanding between all parties involved in loading operations should be promoted at all levels. Key messages should include:

- Promoting a 'no blame culture' for initiation of ESD. If there are doubts concerning the equipment or the loading activity the first action should always be initiate the ESD.
 - If loading has not stopped automatically by the preset volume being reached, or via the earth/overfill protection system, the most appropriate action to take is to initiate the ESD.
 - Initiation of the ESD at the first signs that the loading process has not stopped automatically may ensure that overfill is averted, or at least minimised.
- The overriding principle in the event of an overfill is that personnel should leave the risk area, and not return until it is safe to do so. Any necessary emergency response should be by suitably trained and equipped teams. In addition:
 - It is important that all personnel on site are aware that an overfill has occurred so that the emergency plan can be safely activated.
 - Because gasoline presents particular hazards (such as those arising from large vapour clouds) it is essential that all loading gantries are evacuated until such time that the risk can be properly assessed. Attempting to start a vehicle on the loading gantry will provide an ignition source.
- Informing all those involved in loading activities that there is no expectation that the driver is to attempt to stop flow other than to initiate an ESD and inform the distribution terminal control room.
 - Informing the control room ensures that the correct personnel can be informed and initiate an appropriate action plan
 - Where it is safe to do so, the driver should consider closing the vehicle foot valves. Precise action will be dependent on the vehicle fittings and any specific site circumstances and loading processes
- ESD initiations will be investigated with a view to identifying ways for improving the system. These could include redesigning of arrangements to reduce inadvertent operation, improving procedures for loading and identifying where better training may be needed. Note that trend analysis of ESD initiations may reveal key leanings that could be shared externally through trade association initiatives.

- Simple signage on what to do if a hazard is detected or suspected should be provided in clear view of all personnel carrying out loading operations. Further information can be found in section 4.

3.3 Monitoring Performance

Ensuring the long term effectiveness of training and safe working practices during tanker loading operations can be achieved through performance monitoring. The following techniques may be employed to measure success:

- Any incidents reported during loading operations should be reviewed at regular stakeholder meetings. There may be a need for further training, or updates to existing training programs.
- Periodic review of safety observation reports may indicate where improvement to training programmes or additional tool box talks are required. Further information relating to behavioural safety observation techniques can be found in the following publications:
 - Human factors: Behavioural safety approaches - an introduction, <http://www.hse.gov.uk/humanfactors/topics/behaviouralintro.htm>
 - Step Change in Safety, Safety Observation System – Look this way, <http://stepchangeinsafety.net/ResourceFiles/Look%20this%20Way%202003.pdf>
- Performance indicators (or Key Performance Indicators [KPI's]) should be identified to measure performance and identify trends which may indicate where improvement to training programs, equipment maintenance or additional tool box talks are required. KPI's should be reviewed at regular stakeholder meetings. Examples of KPI's may include :
 - Number of wet probe alarm activations
 - Number of contaminations due to product left on board or crossovers
 - Percentage of drivers with up to date training
 - Number of incidents related to equipment failures
 - Percentage of maintenance procedures carried out on time

4. Loading Rack Signage and Information

Clear signage on the actions to take on detection of overfill may be a useful aid in raising hazard awareness with drivers, contractors and distribution terminal staff. Consideration should be given to providing a simple checklist displayed either at the loading arm or in the drivers cab. Care should be taken to ensure that the purpose and intent of the signage is fully understood by all those involved in loading operations.

The signage adopted should be dependent on individual site requirements, however one example could be:

- Activate ESD
- Notify other personnel in the area
- Evacuate the area
- Notify the control room
- Await further instruction

CDOIF

Chemical and Downstream Oil Industry Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations

Abbreviation	Description
CA	Competent Authority
CDOIF	Chemical and Downstream Oil Industry Forum
CCR	Central Control Room
CCTV	Closed Circuit Television
COMAH	Control of Major Accident Hazards
ESD	Emergency Shut Down
KPI	Key Performance Indicator
SUSA	Safe Un-Safe Act

Glossary of Terms

Loading	Loading is synonymous with the ADR related term 'filling'
Gasoline	low flashpoint liquid fuel, also known as petroleum spirit or petrol, including where blended with ethanol, where there is a significant probability of flammable vapour being present at normal loading temperatures and pressures.
Meter overrun	An alarm resulting from the preset/batch controller (the equipment used to transfer product into the tanker) detecting an overrun beyond the programmed volume of product to transfer.
Overfilling, Overflow	For the purposes of this guidance overfilling is considered to be filling a compartment to the point that gasoline flows out of that compartment, for example into a vapour recovery line or through a pressure relief valve .

Legal Context

In the context considered by this CDOIF Guideline the principal legal considerations are as follows. Note that this list is not exclusive but references those elements of legislation which are likely to be most relevant.

Act or Regulation	Main relevant sections	Notes
Health and Safety at Work etc Act 1974	Sections 2 (1)	The overarching legal framework and “enabling” Act under which H & S Regulations are made. Employers’ duty to ensure, sfairp, the health, safety and welfare of his employees Health and safety policy, organisation and arrangements
	2(3)	
	3(1)	
Control of Major Accident Hazards regulations 1999 (COMAH)	Regulations 4	Employers’ duty to ensure, sfairp, that “non-employees” are not put at risk Implements in GB the Seveso directive Prevent major accidents Mitigate their effects Major Accident Prevention Policy (MAPP) Safety report (SR) On site emergency plan
	5	
	7	
	9	
	Schedules 2 , 4 5	
Management of Health and safety at Work Regulations 1999	Regulation 3	Principles underlying the MAPP Contents of SR Emergency plans Risk assessment H & S Assistance Emergency procedures Information for employees Cooperation between employers Persons working in “host employers” undertakings Capabilities and training Temporary workers
	7	
	8	
	10	
	11	
	12	
	13	
	15	
Provision and Use of work Equipment regulations 1998 (PUWER)	Regulation 4	Suitability of work equipment Maintenance and inspection Identification and control of specific risks Information and instructions Training
	5 – 6	
	7	
	8 9	
Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009 (CDG)	Regulation 5	Implements ADR in GB See ADR 1.3 for requirement in relation to “Function specific” training, which covers more than the driver. Consignors and fillers/loaders have obligations.
Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR)	Regulation 5	Risk assessment Elimination or reduction of risk Area classification, selection of equipment, marking and “verification” of areas Antistatic clothing
	6	
	7	
	8	
	9 10	

CDOIF

Chemical and Downstream Oil Industry Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Reporting of Injuries Diseases and
Dangerous Occurrences
Regulations 1995 (RIDDOR)

Regulation 3
Schedule 2

Duty to report
Dangerous occurrences
Most relevant are DOs 16, 19, 20 and 21

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Daniel Brain (Chair)	Murco
Billy Pullar	Nustar Energy
Yvette Davis	Nustar Energy
Clive Dennis	Health and Safety Executive
Andrew White	Health and Safety Executive
Mike Gray	Health and Safety Executive
Simon Smeeton	Turners
Steve Jenkins	Shell
Linda Dixon	Chevron
Margot Akeroyd	Chevron
Vince Docherty	Exxon
Colin Fenwick	Wincanton
Nigel Atterton	Representing UNITE
Dave Brown	Representing UNITE
Paul Harrison	BP
Eddie Stephenson	BP
James Newey	BP
Graham Anderson	INEOS
Robbie Reid	INEOS
Andrew Baird	Suttons
Graham Arnold	DHL
Robert Harris	Amber Engineering Consulting Ltd.
Peter Davidson	UK Petroleum Industry Association

CDOIF

**Chemical and Downstream Oil
Industry Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	19-Jan-2011	PSD
1	All	Revised following working group comments	17-Feb-2011	PSD
2	All	Revised following final comments from working group	8-Mar-2011	PSD

CDOIF

Chemical and Downstream Oil Industries Forum

Guidance

The Use of External Contractors in the Management of Ageing Plant

Foreword

CDOIF members, as part of their role in promoting and leading on key sector process safety initiatives, have developed guidance on the use of external contractors in the management of ageing plant. This principally relates to the provision of inspection services for equipment containing hazardous substances, but can cover other services.

It is not the intention of this document to specify particular contractual arrangements, nor replace any existing corporate policies or standards. The intent is to provide a reference for those organisations developing or wishing to review their existing arrangements for engaging specialist expertise from outside their own organisation.

There are no limitations on further distribution of this guidance to other organisations outside of CDOIF membership, provided that:

1. It is understood that this guidance represents CDOIF's view of good practice as applied to the use of external contractors in the management of ageing plant.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The guidance is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guidance – The use of external contractors in the management of ageing plant".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the guidance except that it is believed to be substantially correct at the time of publication.

This guidance is not intended to be an authoritative interpretation of the law, however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for engaging specialist expertise, nor does it consider individual site requirements. Following the guidance is not compulsory and duty holders are free to take other action.

If the duty holder does follow the guidance they will normally be doing enough to comply with the law. Health and Safety inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.

Contents

Foreword	2
Contents	3
Executive Summary	4
1. Introduction	5
2. Understanding and agreeing the scope of the work to be done	7
2.1 Issues to consider	7
2.2 Points to address	7
3. Roles and Responsibilities	9
3.1 Arrangements for effective integrity management.....	9
3.2 Elements in the integrity management process	9
4. Planning of Inspection Work	11
4.1 What needs to be inspected?	11
4.2 How to inspect?.....	11
4.3 When should the inspection be carried out?	11
4.4 Who can carry out the inspection on behalf of the site operator?.....	12
5. Response to Examination Findings	13
5.1 Communication and management of actions	13
5.2 Resolving differences	13
6. Performance Monitoring, Audit and Review	14
6.1 Performance monitoring	14
6.2 Audit	14
6.3 Review	14
7. Summary and Conclusions	15
Abbreviations & Glossary	16
Acknowledgements	17
Other Relevant Publications	17
Revision History	18

Executive Summary

The COMAH Competent Authority identified, through their Strategic Priority on Ageing Plant, unsatisfactory outcomes arising from inadequately defined working arrangements between the site operators and the specialist contractors they may employ.

A working group was commissioned under CDOIF to develop this guidance to assist site operators and external contractors in this aspect of the asset management process. This is not intended to be prescriptive in defining the approach to be taken, but aims to highlight key factors that should be considered.

The guidance principally covers examinations of equipment providing containment to hazardous substances, but equally applies to other inspections or activities such as repair specification, design verification or fitness for service assessment.

While this document has been prepared to give advice to those who engage external contractors in the management of ageing plant, it is also to be of use to the service providers and provide a useful reference for site operators who engage with other company departments to provide such services.

The guidance recognises that the use of external contractors or consultants to provide specialist expertise in the management of ageing plant is common and provides a useful means to fill gaps in both resource and competence. It also recognises that there are many different models for such arrangements. However, any system will only be effective if key principles are applied.

It is important for all those involved in the supply chain to understand that the examination is not the end of the integrity management process. Assessment of the results and drawing conclusions to allow appropriate action to be taken, are the key outcomes. While tasks can be delegated, legal responsibilities cannot.

1. Introduction

Many site operators within the chemical and downstream oil industries use external contractors to provide specialist advice and capabilities, or additional resource, in the management of ageing plant. The use of such expertise is obviously welcome where it leads to a reduction of risk. However, issues have been known to arise. These include:

- Tasks given to those without the competence required.
- A failure to adequately define what is required of the parties involved.
- A failure to respond appropriately to the findings of a plant and equipment inspection.

Illustrative example

A site operator employed a specialist inspection company to carry out an examination of storage tanks used for toxic liquids.

The inspection company produced a report that included measured values for the tank shell thickness. However, it noted that these measurements were taken at un-corroded parts of the shell and that there were some significant areas of heavy pitting corrosion elsewhere. Recommendation was made that further work was required to assess the depth of corrosion and determine whether the remaining shell thickness met the minimum required.

The site operator made an assumption that because a competent and reputable company had inspected the tanks, all was well and the inspection report was filed away, and the tanks continued in service.

Comment

There was a mismatch between the expectations of the site operator and the inspection company. Consequently important work to assess the degradation and the suitability of the tanks for service was not undertaken. Opportunities to identify and correct the error were missed.

Effective integrity management requires systems of work, which allow deterioration of assets to be monitored so they do not fail in service. Such systems are characterised by:

- The site operator knowing what plant and equipment they have, and what the consequences of its failure will be. (An asset register with some form of criticality assessment can achieve this.)
- Roles and responsibilities being defined and communicated.
- Clarity of what is expected of the contracted service. (A clear written contract can achieve this.)
- The input of all appropriate parties (including on site operations teams and externally contracted specialists) to determine the inspection requirements.
- Planning arrangements to achieve execution of inspections.
- An appropriate response to inspection findings.
- Performance monitoring and review of the external service provision.

An illustration of an integrity management process is given in figure 1 below.

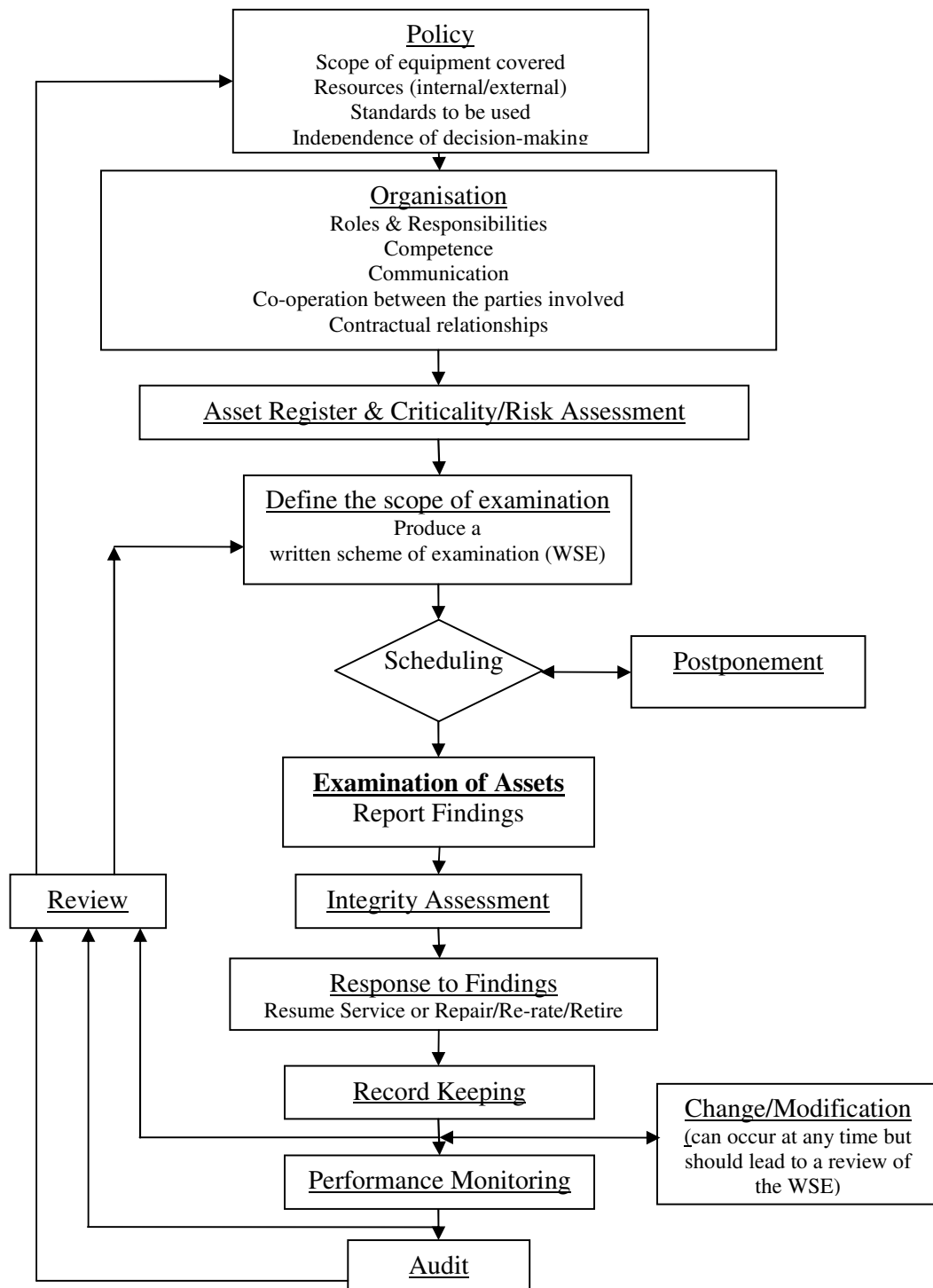


Figure 1 – A flowchart for the Integrity Management Process

(This flowchart is offered as an example only, to help the reader understand the process in which this guidance sits. It is not intended as complete or stand-alone guidance on integrity management.)

2. Understanding and agreeing the scope of the work to be done

When a site operator contracts out services to a supplier, there should be a clear understanding on both sides of what is required, and who is responsible for each task. This is to provide some level of assurance that all necessary aspects of asset integrity have been addressed, and that the responsibilities are allocated and understood.

In order to provide this assurance, it is important to understand the supply chain i.e. who is providing what service. Where site operators have outsourced activities to specialist contractors or consultancies, it is important to understand that those parties may themselves sub-contract certain aspects of the work, leading to an ever more complex supply chain. Failure to understand what is in place could result in competing priorities or a lack of understanding of others' needs.

Each site operator using third party expertise should clearly identify the individual(s) within their organisation responsible for managing the discussions with the third parties, ensure that this individual is competent to do this and that they are fully aware of the importance of their role in this process.

The parties involved should ensure that any agreement made in relation to the scope or requirements of the work is clearly documented.

2.1 Issues to consider

When determining the work to be done and how services will be procured, it is important to remember that whilst the work may be contracted out, the wider responsibilities for integrity management and the operation of critical equipment remain with site operator.

The following are issues to consider:

- How the contract with the external contractor will be placed?
 - This could be directly by the site operator, by a separate procurement department or even through a broker.
 - Whichever route is taken, it is important that all parties clearly understand what is required. This can be problematic as supply chains become more complex.
 - Information needs to be provided to the external contractor to allow them to sufficiently assess the task and provide a realistic quote.
- What work, if any, the site operator will carry out?
 - These responsibilities have to be clearly identified to the supplier.
- On what basis is the contract with the supplier to be placed?
 - This should not be decided solely on price, but should also consider the ability of the supplier to provide the standard of services required.
- Will the supplier place sub-contracts with others? If so:
 - How will the site operator maintain control of the work?
 - How will the site operator be assured of the competence of sub-contractor?
 - How will the site operator have confidence in the communication between all suppliers and their sub-contractors?
 - How will the sub-contractor be made aware of the end user's needs?

2.2 Points to address

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

- Be sure to understand how your supply chain works, those who will be involved, and how decisions are made.
- Clearly specify what will be required of the supplier and define the standards and competency requirements for the work to be undertaken (see chapter 3 of this guidance).
- Ensure that competent engineering input is available for the procurement process, not only to aid in the development of the specification, but also to assess the responses received.
- Recognise that where suppliers are involved in the development of an integrity management regime (including schemes of examination), they will require input of local and process knowledge from the site operator. This should be addressed within any contractual arrangements (see section 4).

Overall, it is important that the site operator or employer procuring services has the ability to act as an intelligent customer. Further guidance can be found on this subject on the HSE website (<http://www.hse.gov.uk/humanfactors/topics/customers.htm>).

3. Roles and Responsibilities

While a site operator may employ a specialist contractor to carry out a specific function, each party retains their own legal responsibilities. It is important to remember that while tasks can be delegated, responsibility under legislation cannot.

3.1 Arrangements for effective integrity management

When looking to secure external expertise, roles and responsibilities need to be considered to ensure that:

- All roles and responsibilities are either covered by one party or the other.
- Responsibilities under legislation are fully understood by both parties.
- Each party is competent to complete the duties assigned.
- The site operator is competent and able to act upon the information they receive.
- Levels of authority are adequately defined, and that these are appropriate to the criticality of the task.
- Arrangements are made to secure the effective co-operation between the parties involved in the process and that channels of communication are set up.

Roles and responsibilities should be determined and agreed as part of the procurement process (ref. Section 2). These should be reviewed periodically and updated accordingly (ref. section 6).

3.2 Elements in the integrity management process

Key elements that need to be considered when defining roles and responsibilities include:

- Approval or authorisation of key requirements (such as written schemes of examination, repair specifications or fitness for service assessments etc).
- Assessment of criticality/risk.
- The actual preparation of the written scheme of examination. Further information can be found in 'The mechanical integrity of plant containing hazardous substances: A guide to periodic examination and testing' a joint publication by SAFed and EEMUA (SAFed ref - IMG01 : EEMUA ref – Publication 231).
- Planning and scheduling of inspection activity (ref. Section 4).
- Preparation of equipment for examination (taking out of service, provision of access, cleaning, provision of 'safe systems of work' etc).
- Conducting the examination (which in itself may be made up of several constituent parts carried out by different parties).
- Reporting on the examination and provision of all findings.
- Assessment of the inspection findings, and providing a conclusion of whether or not equipment remains suitable for continued use.
- Fitness for service assessments where degradation or damage has occurred.
- Specification of repairs or remedial works, where necessary.
- Verification of completion of such repairs or remedial works.
- Maintaining copies of inspection records and associated documentation.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Illustrative example

A site operator required inspection of their pipework. They did not produce schemes of examination for the pipework but had procedures for the task, which identified internal erosion as a degradation mechanism for the pipework and required thickness checks at intervals along the pipe length and at every change of direction. They employed a qualified NDT contractor, who carried out ultrasonic thickness testing at the required locations on the line 'where accessible'.

The NDT did not include any thickness readings at the bend most likely to suffer internal erosion. There was no assessment made of the condition of the pipework at the supports, even though the design of those supports was one that would give rise to a risk of corrosion.

Comment

Competence is task specific. While the contractor was shown to be competent at carrying out ultrasonic thickness checks, they were not competent in pipework inspection.

The pipework was not appropriately assessed for internal erosion at the key first bend, and it was not assessed at all for other degradation mechanisms (such as corrosion at the supports).

A properly prepared scheme of examination would have identified all the degradation mechanisms and the likely locations, clearly defining the inspection requirements. This would have also made clear the accessibility requirements for the examination.

4. Planning of Inspection Work

It is important that appropriate planning and execution of inspection work is undertaken in order to achieve an effective inspection. There are several aspects of planning inspection work to be considered before the inspection takes place. The site operator defines what needs to be inspected with expert help as required. The timing of the inspection is defined in order to ensure safety of operation, and that the plant continues to be fit for purpose. The access provided and the time allowed must be adequate for the inspection team to complete the work. Those engaged to carry out the activity must be adequately trained, experienced and supervised allowing the client to be assured of competence. This section outlines what to consider when deciding what, how and when to inspect.

4.1 What needs to be inspected?

It is the site operator's responsibility to determine what needs to be inspected. They will understand the process and the operating conditions better than others. They should participate actively in identifying credible degradation mechanisms and specifying the correct extent and type of inspection required to detect these.

There are various inputs to this process:

- a) Legislative requirements.
- b) The plant history, maintenance regimes, the operating conditions, environmental conditions and the materials of construction. A cross-disciplinary team may need to be assembled to identify credible degradation and define an effective inspection regime. The relevant disciplines could include metallurgists, chemical engineers, plant operators, and mechanical engineers as well as expert inspectors.
- c) Degradation mechanisms. When engaging a specialist to carry out inspections, the site operator should explain the credible degradation mechanisms (actual and possible) before the extent of the inspection is defined, and the techniques able to detect such deterioration agreed.

4.2 How to inspect?

- a) All inspection activities shall be performed under a safe system of work i.e. Permit to Work or task specific method statement and risk assessment.
- b) The appropriate inspection technique should be understood and used to ensure the effective detection of any damage, deterioration or weakness which could affect safe operation. For example, screening techniques such as crack-detection or thickness measurements are used to detect defects or material loss over time.
- c) The probability of detection and the limitations for each of the techniques proposed as part of the inspection should be understood. By taking account of what is being measured and the accuracy of the measurements, confidence can be gained in the results of inspection, and the interval required before the next inspection.

4.3 When should the inspection be carried out?

The aim is to inspect at a frequency which allows any degradation to be detected, ensuring the continued safe operation of the equipment. Regulations may not prescribe specific inspection intervals, but require a competent person to set an appropriate

interval for each part of the system depending on a risk assessment or the remaining life principle.

- a) Risk based assessments may be used to determine an appropriate inspection scheme. The outcome of each inspection should be used to review the risk based assessment and inform future inspection intervals.
- b) For those items of equipment which are required to be taken out of service in order for inspection to be carried out, the inspection should be thoroughly planned. Due consideration should be given to scheduling downtime and the preparatory activities to provide clean, safe access to all relevant parts of the equipment such as: erection of scaffolding, removal of lagging and removal of inspection hatches. Entry to a vessel should be a permit controlled activity.
- c) If an upset event or excursion in operating conditions occurs, it should not be assumed that there is no change in the rate of degradation in the equipment. Consider performing a supplementary inspection, even if this is well within the period for which the equipment has been endorsed to operate.
- d) Where a uniform deterioration rate has been firmly established and conditions allow the monitoring to be effective, then a number of online monitoring devices are available, (to measure losses of thickness for example). The use of such devices does not remove the requirement to perform a thorough inspection. However they can inform inspection results, and help define inspection intervals.

4.4 Who can carry out the inspection on behalf of the site operator?

It is the site operator's responsibility to ensure that they appoint an external contractor or Inspector with appropriate competence to carry out an effective inspection. When appointing an external contractor:

- a) Examine the evidence of the contractor's competence and ensure that they are able to carry out an effective inspection. A number of organisations such as UKAS, EEMUA or SAFed can give guidance on acceptable qualifications for inspectors and the accreditation of inspection bodies. *(See reference section for specific guidance).*
- b) Inspection qualifications and non-destructive testing certification can lapse over time. Ensure that the Inspector or technician has current evidence of competence, for the technique(s) to be used before they start work. BINDT can advise on acceptable qualifications and competence of NDT technicians.
- c) Personnel associated with the inspection process shall retain their independence, be free from any conflicts of interest and shall act impartially.
- d) Responding to the findings of an inspection report, by a properly appointed competent external contractor, is a separate issue dealt with in the next section.

5. Response to Examination Findings

External expertise is commonly used in carrying out equipment examinations. However, examination results often require interpretation and conclusions need to be drawn to allow decisions to be made on what further action is necessary. These decisions can be made either by the site operator/customer, or by a specialist contractor. Therefore, careful allocation of roles and responsibilities (as discussed in section 3) should ensure that all necessary elements of the integrity management process are covered.

The key point is that it is important to remember that the examination is not the end of the integrity management process. Finding specialist expertise to conduct the examination may not be sufficient to meet all necessary requirements to ensure the continued integrity of the equipment involved. Similarly, it may not be sufficient to meet all the site operator's legal duties. Assessment of the results and drawing conclusions to allow appropriate action are the key outcomes.

5.1 Communication and management of actions

Measures to address the issues above can include:

- Clear communication of the output of the examination process so that the end user (e.g. operations department) knows what action to take (e.g. repair, removal from service, continued use etc).
- Demarcation of actions to clearly identify which are necessary requirements to allow return to or continued service and those that are advisory. Where relevant, actions should be provided with a target date or timescale (this may be of a form such as 'before return to service'). Actions may also set limits on service or operating conditions.
- Management systems to control the follow up from the examination and ensure that any actions are completed, whether they be allocated to the site operator or external contractor. This includes verification (including testing) of remedial actions or repairs.

5.2 Resolving differences

There may be situations where the site operator/customer does not agree with the advice or actions provided by a third party specialist, and does not feel it appropriate to be bound by such conditions. This may occur where it is felt that the consultant was being overly conservative. As external bodies are often employed to fill a gap in the specialist competencies of the site operator, it would be unwise to ignore their advice.

The site operator should have a formal process for dealing with differences of opinion. For example, this may seek to ensure that the level of competence of those making the final decision is at least equivalent to those making the original recommendation. Any site operator should ensure that the primary motivation in making decisions in this process is the integrity of the equipment and the safe operation of the site.

6. Performance Monitoring, Audit and Review

The relationships within an integrity management process can become complex. Especially as that process will often apply to a range of different equipment and can include a number of different parties. There is often potential for improvement and scope to learn from experience. Performance monitoring, audit and review should be used to maximise the opportunity for such benefits.

6.1 Performance monitoring

Performance may be measured in the following areas:

- Engagement of the contractor
 - Where contracts are placed with suppliers, the performance of that function should not be based solely on savings made, but also consider the suppliers quality of service and their ability to meet the needs of the original contract.
- Execution of the required examinations
 - Performance indicators can be used to assess the delivery of the process. This may include measuring the proportion of examinations undertaken on schedule, and other parameters.
- The response to the results of examination
 - Agreed actions closed within specified timescales

6.2 Audit

The relationships between site operators and external contractor are part of a larger management system. Therefore it is important that they are included as part of the wider audit arrangements of the asset management function.

6.3 Review

Routine performance monitoring and audits are expected to provide an input into a periodic review aimed at developing learning and improving risk control on site.

Illustrative example – Benefits of review

A site operator had used an independent external contractor to prepare a written scheme of examination of an insulated stainless steel distillation column. A second external contractor was employed to carry out the periodic thorough examinations. The scheme did not identify stress corrosion cracking of the vessel as a potential degradation mechanism, and it was not looked for during examinations. This was apparently because the inspection bodies had mistaken the materials of construction and therefore did not recognise the threat. However, the site maintenance team had encountered failures of the stainless steel bolted fastenings on the main body joint of the column. The failed parts were analysed by a specialist, who diagnosed chloride induced stress corrosion cracking (CISCC). Some years later leaks were found on the body of the vessel. Examination found that it too had suffered from CISCC, with through wall cracks now evident. Analysis found the column to be an unstable structure and required replacement, causing a significant period of plant downtime.

Comment

It can be argued that the original scheme of examination should have identified the threat of chloride induced stress corrosion cracking of the column, there were clearly issues with sharing information on materials of construction. However, the error should have been corrected once site maintenance staff had identified the degradation. It is important that site staff recognise the important knowledge they possess and have an input into the integrity management process even when tasks are contracted out to external bodies.

Summary and Conclusions

The use of external contractors or consultants to provide specialist expertise is common in the management of ageing plant and asset integrity. It provides a means to fill gaps in both resource and competence.

There are many different models for such arrangements. These have to cater for the differing management systems used by site operators and for the different areas where the specialist resource is required. This flexibility is welcome if it allows the customers or site operators to meet their needs. However, any system will only be effective if key principles are applied.

The customer/site operator should be able to:

- Know what they need,
 - So that they can define what is required of the supplier, but also so that they understand what is required of themselves.
- Assess what they receive,
 - So that they can understand whether the supplier meets their requirements.
- Know how and when to act
 - So that they are assured that remedial work is undertaken wherever necessary.

These are the principles of being an intelligent customer

Similarly the supplier of specialist services should be able to:

- Know what is required of them,
 - Not only so that they can fulfil their obligations, but also so that they can advise the customer of what they are not doing, but may be required
- Understand that they are part of a team,
 - So that there can be a clear flow of information and co-operation between them and the customer.
- Provide clear conclusions with justification,
 - So that they help the customer know the limits of the work done, and the action required of them.

It is important for the site operator/customer to understand that the examination is not the end of the integrity management process. Assessment of the results and drawing conclusions to allow appropriate action to be taken, are the key outcomes.

While tasks can be delegated, legal responsibilities cannot be delegated.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations & Glossary

Abbreviation	Description
BINDT	British Institute of Non-Destructive Testing
CA	Competent Authority
CDOIF	Chemical and Downstream Oil Industries Forum
EEMUA	Engineering Equipment and Materials Users Association
HSE	Health and Safety Executive
NDT	Non Destructive Testing
PSSR	Pressure System Safety Regulations
SAFed	Safety Assessment Federation
UKAS	United Kingdom Accreditation Service
WSE	Written Scheme of Examination

Term	Definition
Competent Person	A competent person is someone who has sufficient training and experience or knowledge and other qualities that allow them to enable the Site Operator to meet the requirements of health and safety law.
Criticality Assessment	An assessment of the consequences of failure of an item of plant or equipment to allow some prioritisation of maintenance and inspection activity. Criticality can be assessed with respect to a number of parameters (which may include safety, environment, business etc) depending on the definition applied by the duty holder to meet their needs. However, care needs to be taken to ensure that legislative requirements are met, e.g. guidance to the Control of Major Accident Hazards Regulations refers to the periodic examination and assessment of safety-critical components (here the term 'safety' should be interpreted to include matters affecting health, safety or environment).
Customer	In the context of this guidance the customer is the person procuring the service. A site operator will become a customer, but so will contractors if they sub-contract work packages.
Duty Holder	The person or organisation with the responsibility to meet the relevant legal requirements.
External Contractor, or Supplier	Organisation engaged to deliver the scope of services specified in the contract.
Inspection/Examination	Within this guidance these are considered interchangeable terms to describe various activities aimed at assessing the integrity of plant and equipment.
Site Operator	A person who is in control of the operation of the establishment or installation. A person may be an individual, corporate body or a partnership.
Written Scheme of Examination (WSE)	A plan used to define the scope and frequency of examinations to be carried out. (NB there are specific requirements for a WSE within the Pressure Systems Safety Regulations, where they apply) It should be noted that different terms may be used for this 'plan' where PSSR does not apply.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industries Forum, CDOIF, wish to record their appreciation to the working group members who were responsible for creating this guidance:

Name

Paul Stanworth (Chair)
Andrew Fowler
Chris Blackmore
Douglas Leech
Francis Drew
Bud Hudspith
Hugh Bray
Ian McCluskey
Jean Martin

Julian Hought
Kevin McKeown
Martin Denny
Miles Gardner
Alec Morrow
Nick Girdham
Paul Jackson
Peter Davidson
Phil Scott
Richard Hakeem
Richard Hulmes
Robin Luxmoore
Stefan Kukula
Stuart Pointer

Organisation

Health and Safety Executive
HFL Consulting Ltd
Institution of Chemical Engineers
Chemical Business Association
UM Group Ltd
Unite the Union
Tank Storage Association
Avantigas
Murco Petroleum Limited /
InSite Technical Services Ltd
HFL Consulting Ltd
Calor Gas Ltd
BP
Zurich
Lyondell Basell
Total
ABB
UK PIA
Chemical Industries Association
UK LPG
SAFed
EEMUA
EEMUA
Health and Safety Executive

Other Relevant Publications

Enforcement Policy Statement (www.hse.gov.uk/pubns/hse41.pdf)

Human factors: Intelligent customer capability
(<http://www.hse.gov.uk/humanfactors/topics/customers.htm>)

A guide to the Control of Major Accident Hazards Regulations 1999 (as amended), L111, HSE Books, ISBN 9780717661756

Safety of pressure systems. Pressure System Safety Regulations 2000, Approved Code of Practice. L122, HSE Books, ISBN 978 0 7176 1767 8

Safe use of work equipment. Provision and Use of Work Equipment Regulations 1998. Approved Code of Practice and Guidance, L22, HSE Books, ISBN 978 0 7176 6619 5

Mechanical Integrity: Use of third party expertise on high hazard sites, COMAH Competent Authority, Version 1/June 2010

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

The mechanical integrity of plant containing hazardous substances: A guide to periodic examination and testing' a joint publication by SAFed and EEMUA (SAFed ref - IMG01 : EEMUA ref – Publication 231).

Plant ageing - management of equipment containing hazardous fluids or pressure, HSE Research Report RR509, prepared by TWI Ltd, ABB Engineering Services, SCS (INTL) Ltd and Allianz Cornhill Engineering. <http://www.hse.gov.uk/research/rrpdf/rr509.pdf>

ISO/IEC 17020: 2012 'General Criteria for the Operation of Various Types of Bodies Performing Inspection'

BS EN ISO 9712:2012 'Non-destructive testing. Qualification and certification of NDT personnel'

Competence assurance of in-service inspection personnel (pressure equipment) – EEMUA Publication 193 (Engineering Equipment and Materials Users Association)

Guidelines on periodicity of examinations, Doc ref PSG01, Issue 2, 6/11/03 - Safety Assessment Federation Ltd

Users' guide to the inspection, maintenance and repair of above ground vertical cylindrical steel storage tanks – EEMUA Publication No 159 (Engineering Equipment and Materials Users Association)

API 510 Pressure vessel inspection code: In-service inspection, rating, repair, and alteration, 9th ed, June 2006 - American Petroleum Institute

CIRIA c736, Containment systems for the prevention of pollution. Secondary, tertiary and other measures for industrial and commercial premises, London : 2014

Best practice for the procurement and conduct of non-destructive testing. Part 1: Manual Ultrasonic Inspection, HSE Gas and Process Safety Technology Division, November 2000

Best practice for the procurement and conduct of non-destructive testing. Part 2: Magnetic Particle and Dye Penetrant Inspection, HSE Gas and Process Safety Technology Division, November 2001

Information for the procurement and conduct of non-destructive testing. Part 3: Radiographic Inspection in Industry, HSE Gas and Process Safety Technology Division, April 2008

Information for the procurement and conduct of non-destructive testing. Part 4: Ultrasonic Sizing Errors and their Implication for Defect Assessment. HSE Gas and Process Safety Technology Division, April 2008

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	23/03/15	P Stanworth

CDOIF

Chemical and Downstream Oil Industries Forum

Supplement to Guideline – ‘Environmental Risk
Tolerability for COMAH Establishments’

Complex Site Example

Whilst the CA cannot comment on the accuracy of any site specific data or assumptions, the worked example provided does demonstrate an appropriate interpretation and application of the CDOIF guidance, with a sufficient level of detail to allow the screening process to be complete

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Complex Site Case Study

Glossary of Terms used in Case Study

APIS – Air Pollution Information System
BLEVE – Boiling Liquid Expanding Vapour Explosion
CDOIF – Chemical and Downstream Oil Industries Forum
COMAH – Control of Major Accident Hazards
DEM – Digital Elevation Model
EHI - Environmental Harm Index
EA – Environment Agency
EI – Energy Institute
GIS – Geographical Information System
HAZID – Hazard Identification (Study)
HAZOP – Hazard and Operability (Study)
IES - Institute for Environment and Sustainability
LOPA – Layers of Protection Analysis
MAS – Major Accident Scenario
MATTE – Major Accident to the Environment
NRW – Natural Resources Wales
SAC – Special Area of Conservation
SEPA – Scottish Environmental Protection Agency
SIL – Safety Integrity Level
SSSI – Site of Special Scientific Interest
TifALARP – Tolerable if As Low As Reasonably Practicable

Overview of Approach

It is considered appropriate to review how the current CDOIF guidance might be applied to a complex site where there are multiple sources, pathways and receptors which have the potential to combine to enable the generation of a MATTE. Whilst the CDOIF guidance has been used as the basis for the assessment there are some important deviations from the approach which are necessary to make sure that the assessment remains focussed and presents a meaningful and thorough yet concise output in the context of a complex site.

This worked example follows the CDOIF guidance in terms of the degree of assessment required to demonstrate adequate risk controls are in place. Not all major accident scenarios will be assessed to the same extent, rather they are progressed until the frequency associated with the hazard has been reduced to an acceptable level (or to a point that is not a significant contributor to the overall Establishment risk).

The recommended approach of identifying all of the potential pollutant linkages for a complex site which has multiple potential receptors can lead to a lengthy table of results which ultimately provides only limited value in completing either a qualitative or quantitative assessment of risk to the environment. Instead, the CDOIF approach may be worked in reverse by identifying the most significant receptors (based on proximity, magnitude of impact, sensitivity, etc) and then working through the sources to identify which events could plausibly result in an impact at those locations. For example, where there are multiple designations and only subtle differences in the proximity of the sites then the most onerous receptor in terms of impact area/length thresholds should be selected. Consideration of groundwater is a critical element and it may require expertise to assess whether that particular feature should be considered as a receptor within the confines of the site, beyond the site boundary or whether the groundwater simply constitutes a pathway to convey contamination to a different receptor.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

The end point of this first stage is therefore to identify receptors (but without looking in detail at the rationale for designation, etc) and associated sources. This results in a manageable set of potential pollutant linkages for assessment.

The sources can then be characterised through review of the available process safety data to identify those major accident scenarios (MAS) which may have already been documented as having the potential to result in a source of contamination capable of generating a MATTE. This list of sources should then be critically reviewed to remove those unlikely to have a MATTE potential and supplemented by additional scenarios which may not have been considered as part of previous safety assessment work (e.g. tank floor failures).

For each asset there may be a range of plausible sources to the same receptor. To simplify the subsequent calculation steps each asset is assigned to its own compartment. Splitting each part of the site in this way will enable the process of assigning risks to be made transparent and can be effectively managed in a combined spreadsheet and geographic information system (GIS).

Having identified a potential set of sources and receptors the next stage is to identify what types of pathways might join the two – whether that be (for example) via overland flow routes, subsurface migration or via emissions to the atmosphere. Some pathways may be dismissed relatively quickly by completing a high level review of the significance of a release whilst others will inevitably require more detailed assessment of initiating frequencies for the release and assessment of the effectiveness of the barriers separating the source from the receptor.

The pathway assessment for a complex site may therefore be completed in three stages;

1. High level assessment to evaluate whether the link from the source to receptor via the defined pathways could result in a plausible MATTE (e.g. fire associated with a tank producing combustion products and its effect on a SSSI receptor via the air pathway).
2. Unmitigated risks taking into account the initiating frequency (i.e. is this already so low that the impact at the receptor is unlikely to be significant) and existing control measures which would limit the potential for a release from primary containment (e.g. Layers of Protection Analysis (LOPA) for bulk storage tanks).
3. Mitigated risk assessment considering the likely effectiveness of measures which would limit the potential for the source to reach the receptor (e.g. secondary/tertiary containment, emergency response plans, in-ground migration and effectiveness of pathway interruption measures, etc).

At the end of this stage the assessment is nearly complete since we have defined the sources and receptors, considered initiating frequencies, built in the engineering controls and considered the measures in place which could limit the chance of a significant quantity of contamination reaching the receptor. The potential level of risk can be viewed on an asset by asset basis (i.e. compartments), for each MAS and which may then be combined for each receptor.

The last stage is to assess the significance of the potential impact. This is left until last as the assessment process itself may assist in understanding how large of an area could be affected following a release. It is also possible to consider a conservative impact level at the unmitigated stage and a different (likely lower) level of impact following a more detailed review. The potential significance and the acceptability criteria to be used in the summation of the establishment risk follows the guidance outlined by CDOIF. The process is relatively straight forward based on the actual receptor(s) identified. This process results in the tolerability criteria being defined for the establishment and from there the results of the summed risks for the Establishment can be compared to this criteria. One potential area which should be addressed is where a site covers multiple hydraulic or surface flow catchments which may have different receptors.

In order to assist in demonstrating the approach an example process is outlined below for assessing the MATTE risk at a refinery site in South Wales.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Introduction

The case study which follows is based on the need to develop an assessment of the potential environmental risk posed by plausible major accident scenarios at a refinery, building on the existing process safety assessment and is focussed on completing an assessment of MATTE risks under the COMAH regulations taking into account current guidance from CDOIF.

For context the site is located approximately 3km from the coast and is surrounded by numerous small streams which eventually discharge into an ecologically sensitive, and statutorily designated, site (*these are therefore considered as the potential receptors and each was assigned the highest level receptor type based on the ultimate receiving water body which is designated as a SAC*). The geology at the site is a mixture of mudstones, siltstones and sandstones which are folded and dip steeply towards the north and south indicating the presence of a syncline through the northern part of the site. The shallowest bedrock unit is typically mudstone which is overlain by a veneer of made ground comprising gravelly clay. Groundwater beneath the site is classified as being within a Secondary A aquifer with the predominant flow being via fractures and fissures. A groundwater high is located in the north of the site and groundwater flow is generally radial from this point resulting in a range of different receptors for site derived contamination within 5 principal catchments across the main site and a further one at the jetty to the south. **Figure 1** provides background to the site setting.



Figure 1 – Environmental Setting

Receptor Review

The first part of the process is to identify whether there is/are source-pathway-receptor pollutant linkages at the site. This was undertaken in a conservative manner and at a high level. For instance, there are numerous small streams located around

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

the periphery of the site which drain in to a SAC/SSSI (which have marginally different extents). The site is also underlain by groundwater in a Secondary A aquifer and is surrounded, to a large extent, by farmland. A qualitative appraisal of these receptors indicated that the SAC was likely to be the most sensitive and as such was used as the basis for determining the potential for a MATTE to exist based on the potential aerial extent of impact. At this stage no consideration was taken of the length of adjoining water courses (which might remove them from being MATTE receptors) rather it was assumed these formed an integral part of the SAC and they acted as a pathway which itself was not considered to have any mitigation potential at this stage.

Specific details regarding the SAC/SSSI designations are as follows;

- SSSI – The designation is based on a combination of geology and ecology depending on location. Various estimates of the area are provided depending on source information although the formal citation estimates the area to be approximately – 2,190 hectares.
- SAC – The SAC covers a very large area. Review of various designations for the SAC indicate that the key Estuary Habitat covers a similar extent to the SSSI (albeit it includes the full area of the water body. In addition the intertidal mudflats and to some extent the Atlantic salt meadows also cover a similar area as the SSSI. This specific component of the overall SAC was considered as the sensitive receptor when working out potential areas of contamination.

Overall the SAC/SSSI designation aspect is relatively complex so a conservative approach was adopted and simply assumed that the SAC was the most sensitive potential receptor. Further information on these and other receptors are provided in the full submission and in other relevant environmental reports for the site.

A set of CDOIF tables which outlines the process for receptor selection is provided later in the case study – once the plausible sources for each MAS have been identified.

Groundwater is a more challenging receptor class for the site given the aquifer designation. It was, however, discounted as being a receptor in its own right for several reasons relating primarily to existing groundwater quality, extent of site ownership, the low likelihood of it being exploited in the future, etc. Instead groundwater was considered as a potential pathway with the various surface water features located around the periphery of the site being considered the primary receptor and which were classified based on their links to the designated site located to the south of the site. Groundwater outside the site boundary was considered a potential receptor but of lower sensitivity than the surface water receptors (i.e. if there was a MATTE potential for groundwater there would also be a potential for a MATTE relating to the surface waters and adjoining SAC).

If groundwater was considered to be a receptor then it would be classified as severity level 2 as Level 3 would require $>1\text{km}^2$ to be contaminated. Given the nature of flow in the bedrock the actual breadth of contamination is likely to be limited and therefore plumes in excess of 2-3km would be required to exceed this lower level threshold. In addition, the submitted report contains a wide range of reasons why groundwater on-site should not be considered a receptor in its own right (acknowledging that there is a wide range of regulation in place to capture contamination of groundwater on site were it to occur). Notwithstanding this it is acknowledged that this receptor could be at risk and may be affected by different MAS pathways and have different mitigation and this should be considered carefully for sites where groundwater may be a significant receptor. Groundwater pathways to the same receptors which may be affected by overland transport of contamination following a release have been assessed and mitigation measures applied separately based on the pathway analysis. For example, penetration into the ground and migration as a dissolved phase plume towards surface water carries with it the potential to mitigate the level of impact and this would clearly not be applicable for overland routes. Similarly the affect of secondary and tertiary containment is nullified if the contaminants could penetrate into the ground and migrate within groundwater. These are all aspects which will be covered in more detail as part of the Stage 3 assessment as needs dictate.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

For this complex site the consideration of receptors was stopped at this stage without the need to consider in more detail the specific rationales for designation, species at risk, etc. A conservative view was taken in terms of the magnitude of potential impact which would subsequently be reviewed once information on the MAS and subsequent environmental risk assessment had been undertaken. For this refinery site it was assumed that the majority of the MAS had the potential to impact between 25 to 50% of the area, designated population or associated linear features (Major/Severity Level 3 in the CDOIF classification scheme). The purpose of the tolerability review is to ensure that appropriate tolerability thresholds are used to screen the site risks against. If this is done conservatively there should be no need to consider each potential receptor in more detail than necessary.

Regarding the SAC/SSSI receptors; in this case study professional judgement was used to select the worst case combination of severity and duration which resulted in the SAC being selected from which to assess the relevant severity and duration criteria. It will be necessary to look at receptors again, in more detail, if there is an intolerable risk and/or if certain mitigations would only work for one receptor and not another. In this case study the mitigation measures applied are applicable to both.

The next step for this case study was then to produce an assessment of environmental risk taking into account the information contained within the existing Process Safety Report to satisfy applicable environmental aspects of the COMAH regulations.

It should be noted that the CDOIF guidance advocates completing the first stage assessment work in a qualitative manner comprising two steps;

1. to establish first whether there is a pollutant linkage and if there is, using information on volumes of product stored etc, determine the potential degree of impact that a site might have on the identified receptors; and
2. identify the relevant scenarios and associated initiating frequencies and sum these for the Establishment.

The result at Step 2 is then compared against the tolerable thresholds determined from Step 1. Exceedance of acceptability criteria after Stage 1 may require more detailed assessment at Stage 2.

For a complex site this simple breakdown of steps requires some supplementary steps to produce a meaningful output which is transparent and can be reviewed appropriately by the Competent Authority. Given the likely large range of scenarios and number of assets present a methodical approach is required. From experience on working on a range of complex sites completing an 'unmitigated' assessment in a qualitative manner is likely to result in an intolerable risk being generated. Whilst Stage 2 of the process outlined by CDOIF incorporates quantitative risk assessment measures there is a wide range of non-quantitative, relatively simple aspects which can be factored in at Step 2 of the Stage 1 process. The following sections of this example outline how the refinery site was broken down into compartments and how the unmitigated and mitigated risks were evaluated at a level commensurate with that outlined as Stage 1, step 2 above.

In the case study, the site was split into 49 main compartments which were then divided into 117 sub-compartments for detailed review and assessment.

Site Compartments

When dealing with a large site and where there is unlikely to be a 'simple' solution by means of a screening process for individual assets, it is necessary to begin by splitting the site into smaller, more manageable pieces. There are many approaches which could be taken depending on site size and complexity. For sites which are both large and complex, compartmentalisation is an approach which provides a high level of flexibility when integrating process safety data and assessing/presenting the overall level of risk. Compartments would typically be defined on the basis of the asset type and location on site. Tanks, pipelines and processing areas would typically be assigned to their own compartment to allow

CDOIF

Chemical and Downstream Oil Industries Forum

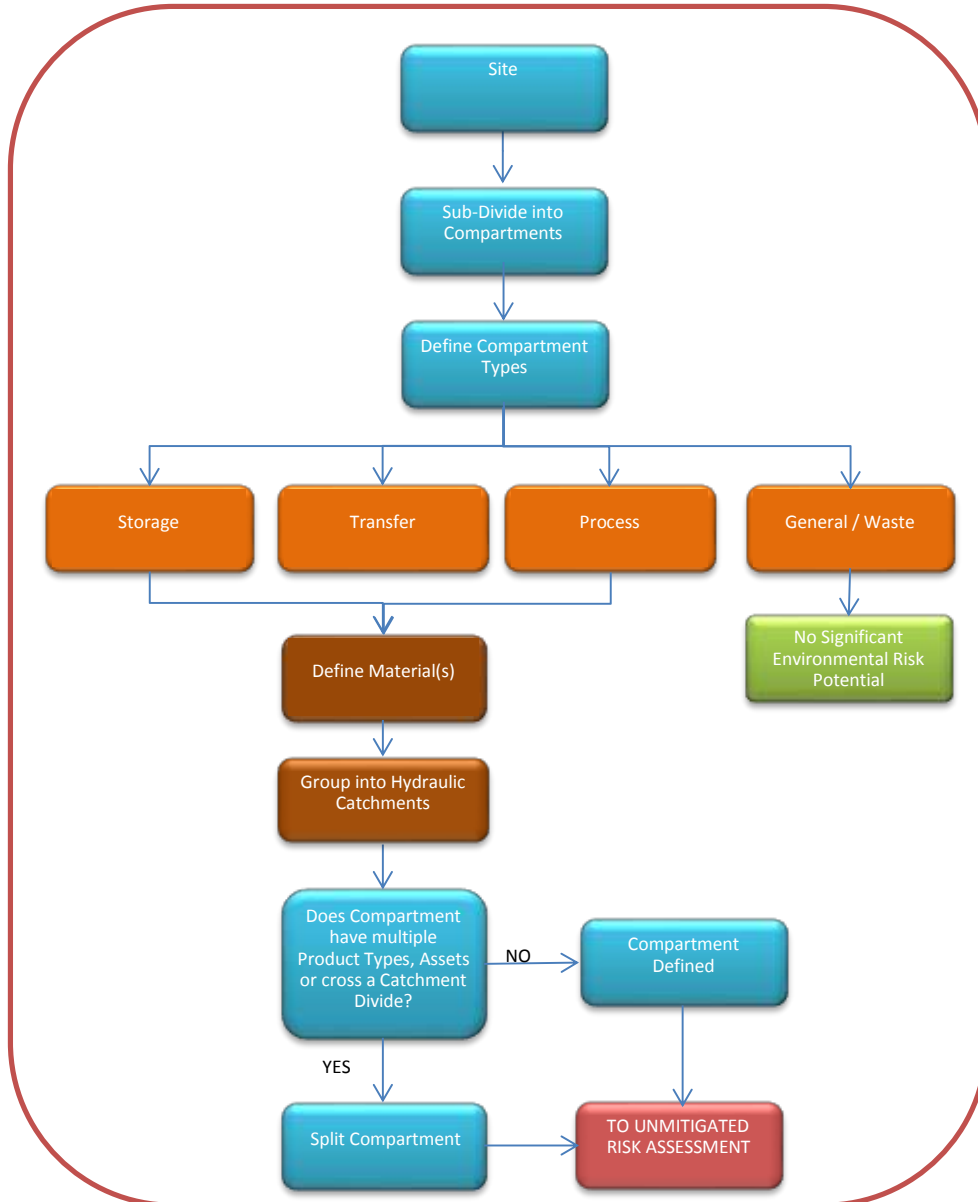
CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

generation of individual risk levels for each piece of plant. These compartments could be further split to differentiate, for example, those tanks which share a common form of secondary containment or where a particular process plant is formed of a number of interconnecting sub-units. Compartments would then also be split based on the environmental setting of the site – particularly where releases via the subsurface pathway or overland could impact upon different environmental receptors as a result of differences in flow direction.

In order to help group risks for different receptors together a series of hydraulic catchments have been defined for the site. These catchments group compartments together based on the specific surface water receptor which is most likely to receive direct run-off or baseflow following a release. The main site catchments are A-E while the jetty itself is catchment F. Catchment definitions are important for a large site since there may be properties associated with the specific which may contribute to development of specific mitigation factors or which may require specific response approaches to deal with a release. In addition the specific distances to receptors within a defined catchment are important when considering mitigation based on in-ground attenuation and when considering the influence of secondary and tertiary containment provisions. For note in the case study catchment B only comprises office buildings and presents no significant MATTE potential.

Figure 2 provides an overview of the process used to split this site into compartments and the type of information which has been collected on each of the assets to enable commencement of assessing relevant accident scenarios. This figure also illustrates the location of each of the catchments across the main site.

Figure 2 – Site compartmentalisation Process

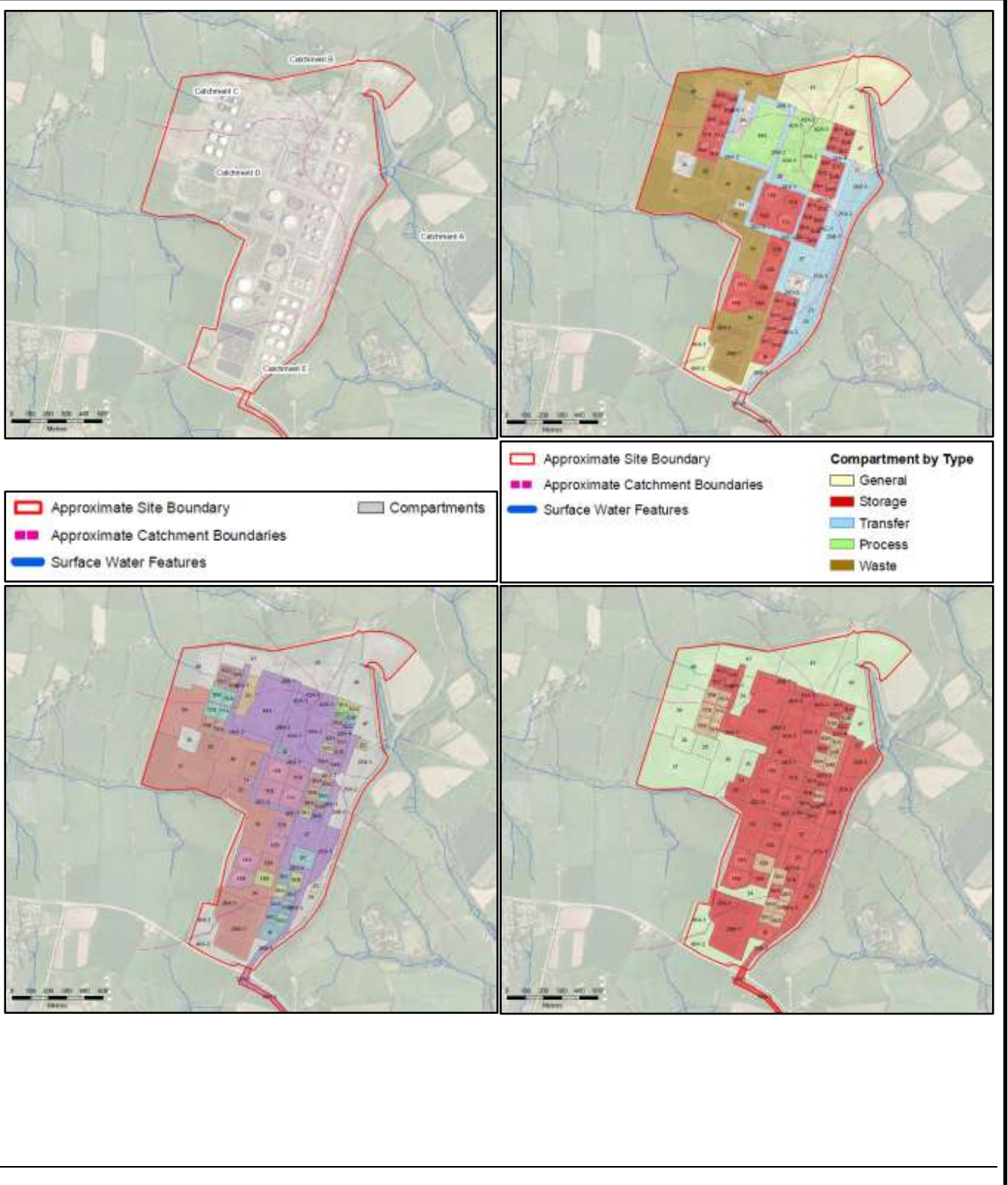


Following the process outlined above each of the compartments was assigned a 'Type'. For each of these, the material or range of materials was assigned (since different materials will have a different potential environmental impact) and the location on site was reviewed to assess the need to split the compartments. To enable the process to be visually inspected a Geographic Information System (GIS) was used to collate the results from the process. **Figure 3** illustrates the result from the compartment derivation process for the case study site.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.



CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

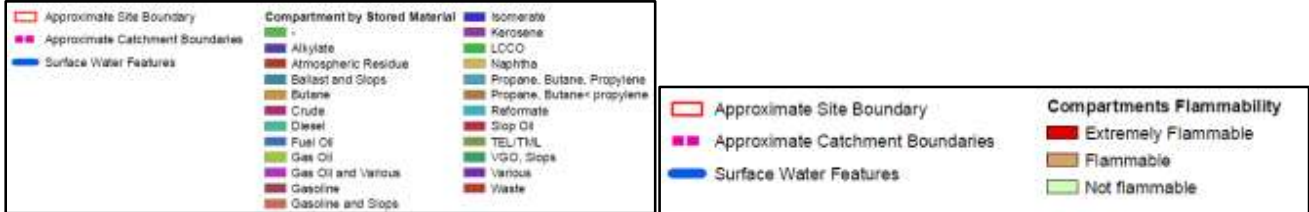


Figure 3 – Site compartments and attributes

Assessing Unmitigated Risks

Having identified that the site contains storage and process equipment that has the potential to generate an environmental impact, the next step was to use the process safety information already generated for the site to begin to assess the level of that risk. As with the compartmentalisation this aspect followed a process to identify the specific assets which could generate a release and to define the initiating events and associated event frequencies in order to assess the significance of each MAS. As part of this process a total of twelve MAS were identified with MATTE potential covering each of the assets. These included groupings of some scenarios within the process area to simplify the approach. For example, more than 3,500 individual release scenarios were identified for process plant at the site. These were screened initially based on product type, release phase (liquid/gas) and potential volume. Once screened the individual scenario initiating frequencies were grouped to enable categorisation into two main MAS; process related release to air and process related release to ground.

The process for assessing the unmitigated risk level at the site is illustrated in **Figure 4**.

In the case study assessment each individual compartment was then reviewed alongside the identified MAS to identify which plausible scenarios were considered to have the potential to result in a major accident to the environment. Where a credible event was considered unlikely to result in a significant impact it was screened out at this stage of the assessment. The potential for a significant environmental impact was discounted even where there was a potentially significant risk to human health or potential for fatalities under the following scenarios:

- Boiling Liquid Expanding Vapour Explosion (BLEVE) – In this scenario the mechanism for the incident was considered unlikely to result in a significant release of liquid on to or in to the ground. Whilst the explosion has the potential to generate a loss of life and release of combustion products into the atmosphere it was not considered that this presented a significant environmental risk.
- Explosions – As with BLEVEs the most likely pathway for a release into the environment was considered to be via the atmosphere and for the same reasons as a BLEVE was considered unlikely to be significant.
- Small volume releases. In some process release scenarios a relatively small volume release could have a catastrophic effect on the safety of personnel working on the plant (e.g. as a result of a flash fire occurring). The risk to the environment from a small release of liquid hydrocarbons may, however, be negligible – particularly when mitigation through secondary and tertiary containment are considered.

Whilst BLEVE and explosions as initiating events have been discounted with respect to the air pathway, however, if the event was associated with an initial leak of liquid (above the threshold volume considered to be significant) then these scenarios were assessed further and were considered to have potential to result in a major accident to the environment. In addition the Buncefield type scenario of fire/explosion with subsequent addition of fire water was included as a scenario. The source of interest here is the firewater itself and not necessarily the release of liquid associated with the initiating event. The initiating event frequency for a fire was generated from the LOPA assessment. As with the BLEVE and explosions the air pathway related to the fire event was discounted as not having significant MATTE potential.

The threshold volumes for MATTE level events will differ between sites based on the site setting and location of the compartment within the site as well as the product type. With respect to the scale of liquid releases which may or may not be significant to the environment at the case study site a review of toxicity, mobility and flammability was completed in order to classify the material by these parameters. Overall, given the specific site setting, a release of less than 10m³ was considered unlikely to have significant potential to generate a major accident to the environment and those release scenarios with a lower liquid release volume were screened out. This volume criteria was selected on the basis of the site setting, location of the main process and storage infrastructure within the site and findings from some initial transport assessments including knowledge of the containment provisions present on site. Such a volume may not be appropriate as a screen in all cases and the ability to screen out may be limited by the availability of existing environmental risk studies at the subject site.

As part of the process of discounting scenarios relating to the air pathway an assessment of the potential significance of a

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

release to the atmosphere was still required to justify its omission. For those scenarios where a gas itself may be released, rather than the combustion products, the toxicity of the gas was reviewed. For natural gas, butane, propane, etc, the gas itself was not considered toxic and unignited releases are ultimately unlikely therefore to present a significant environmental risk. Given the location of the storage vessels for these gases, a release of sufficient magnitude to cause an asphyxiation risk to environmental receptors was also deemed highly unlikely and that dispersion of the gas in the atmosphere would rapidly reduce this risk in any case. In two cases, however, the release was considered to be potentially significant in an environmental context for releases of hydrogen fluoride (HF) and hydrogen sulphide (H₂S) and the release scenarios for the process plant with the potential to generate these emissions were evaluated further.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

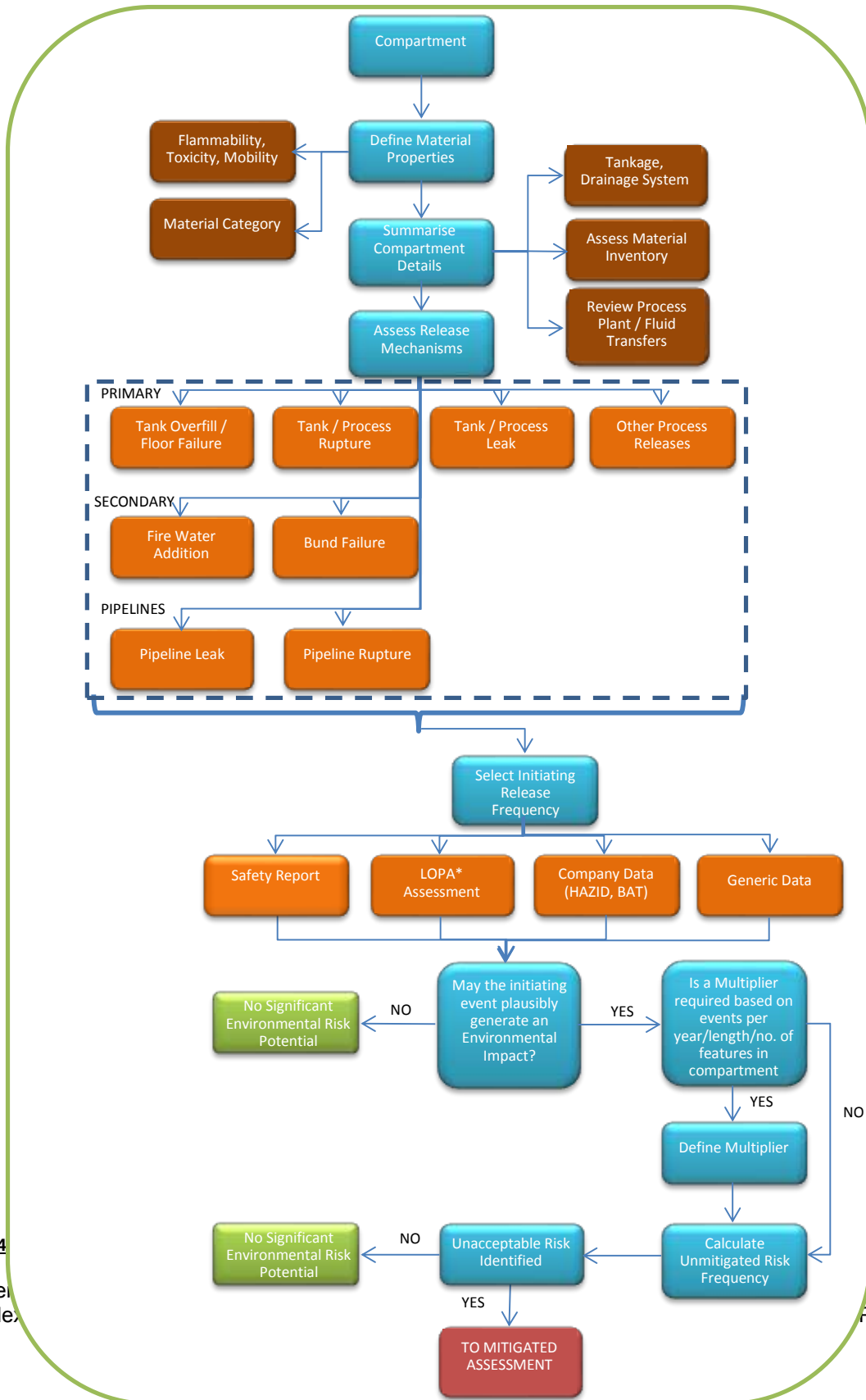


Figure 4

Supple
Comple

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

For the combustion products from fires, explosions and BLEVE scenarios the risk was reviewed through reference to the Air Pollution Information System (APIS); (<http://www.apis.ac.uk>). APIS draws upon a very considerable body of evidence and sets out information on releases to air for a large range of pollutants. As the pollutants of interest which may be associated with an explosion or fire are by nature short-term events, the starting point for identification of potential impacts is to consider the sensitivity of receptors to short term, but potentially high dose events resulting from direct exposure to pollutants and through deposition to ground and their subsequent uptake. Where the feature of interest is fauna, then these were considered to be largely dependent upon the maintenance of the health of the underlying floral habitat and general ecosystem.

Fires and explosions have the potential to release to air a number of substances that are potentially polluting both due to direct toxic effects and due to deposition and subsequent uptake. The APIS website sets out evidence relating to the potential impacts of atmospheric pollutants on protected habitats, both flora and fauna. This evidence, gathered from a wide range of sources, was used as the primary source of information to define those pollutants that are of interest and assess the potential for significant impacts on habitats.

On the basis of the evidence set out, emissions of oxides of nitrogen and associated deposition of nutrient nitrogen and acid nitrogen were considered to be potentially significant pollutants from a fire or explosion which might have potential to result in a major accident to the environment. In general terms the generation of these pollutants from a fire or explosion was considered unlikely to generate concentrations which would significantly alter the annual mean criteria as set out by the European Union. This review was considered to be sufficient to eliminate combustion products as having a significant potential to generate a significant accident to the environment.

Similarly the potential for nitrogen derived acid and an increase in nutrients affecting the flora in the area were considered to be negligible from this type of short term emission to the atmosphere.

As part of the review of the potential scenarios it may, in some instances, be necessary to conceptualise each asset and combine this with information generated from existing hazard identification studies (HAZID Studies) to identify those scenarios which need further consideration. By way of example, **Figure 5** illustrates a range of release events which could be generated from a liquid hydrocarbon storage tank. This could be expanded to include initiating event summaries or the information could be populated in a bow-tie diagram.

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

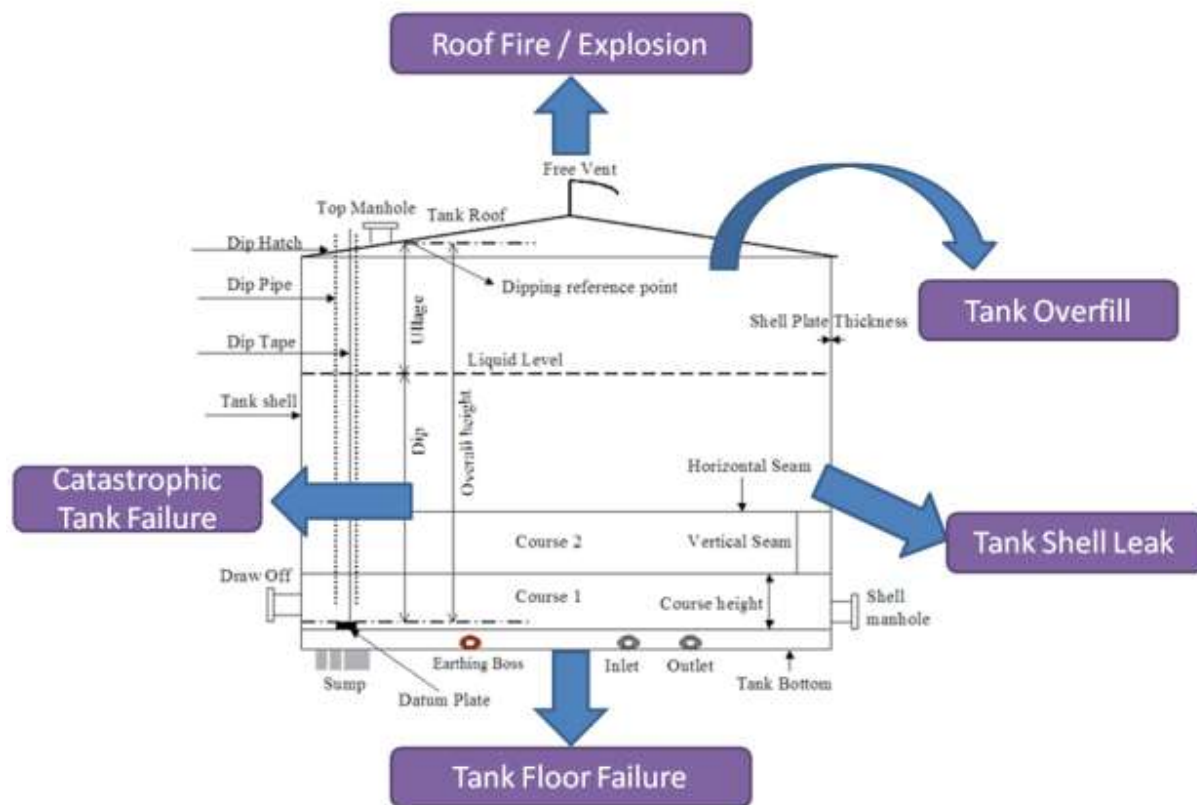


Figure 5 – Illustrative set of sources of potential environmental impact from a bulk storage tank

In the tank compartments event review, the tank floor scenario did not feature in the process safety report as a result of it being low risk in terms of generating potential harm to human health, and the release is also often gradual in effect, not catastrophic. Conversely the potential for a roof fire may not be considered further in the environmental assessment if the emission to atmosphere of hydrocarbon combustion products is not considered significant as outlined above (unless as an initiating event this may result in loss of structural integrity of the tank and a significant volume of stored product being lost to ground).

Typically anywhere between 1 and 6 plausible MAS were identified per compartment based on the review of process safety data. For each event a bow-tie assessment was completed to better illustrate the scenarios and associated potential outcomes. For the site as a whole this resulted in a total of 394 plausible event scenarios which could result in a MATTE (noting that the summed combinations for the 3,500+ process area related release events resulted in 8 MAS for 6 defined process compartments).

During the course of the assessment to this stage a range of information on sources, pathways and receptors has been obtained and as part of the demonstration that the guidance has been followed the CDOIF tables for documenting the process have been populated as outlined in the following section. In order to better understand the result of the unmitigated risk assessment further analysis has been completed within a workbook designed to capture the extensive list of pollutant linkages

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

for each MAS ahead of completing more detailed assessment. Details on this step of the process are provided in subsequent sections of this case study example.

Unmitigated Risk - CDOIF Tables

A summary of the key data collated during the initial stages of the assessment is provided below in order to illustrate how the complex site was assessed and how this meets the data requirements/expectations for the CDOIF tables (Annex 5, CDOIF, 2013). These have been supplemented in the case study work with detailed information for each compartment which includes information on tank construction, storage /operational volumes, construction, etc as well as details on the bunds in which the tanks sit. Detailed information on the MATTE scenarios, receptors, CDOIF tolerability levels, etc have also been provided on a compartment/scenario basis providing a transparent process by which changes to the scenario or site conditions can be rapidly incorporated.

Table 1 – MATTE Potential Summary

The data requirements for this table were summarised by compartments which identified the product type within each which had MATTE potential. In order to complete Table 1 it is necessary to also complete Tables 2 and 3. In the examples provided below the information is limited and for illustration purposes only. In support of subsequent prioritisation further information on why a certain receptor and MATTE severity level have been selected will be required. In order to keep the process relatively simple only the worst case impact has been considered from this point and it is worth noting that this should be continually reviewed through mitigation so that those initially less sensitive receptors are not overlooked in the procedure should some mitigation aspects only provide a risk reduction for certain receptors (e.g. emergency response for surface water receptors, etc).

Transposing the data generated for the site results in the following CDOIF Table 1;

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 1 - MATTE Potential Summary Matrix

Row	DETR Table Ref	Receptor Type See table 2	MATTE threshold See Table 3	MATTE Severity Level	Substance / group of substances					
					1	2	3	4	5	6
1	1	Designated Land / Water Sites (Nationally Important)	>0.5ha or 10-50% of site area, associated linear feature or population	2	✓	✓	✓	✓	✓	✓
2	2	Designated Land / Water Sites (Internationally Important)	25-50% of site area, associated linear feature or population	3	✓	✓	✓	✓	✓	✓
3	3	Other designated Land	10 - 100ha or 10-50%	n/a						
4	4	Scarce Habitat	2-20ha or 10-50%	n/a						
5	5	Widespread Habitat - Non-designated Land	>10ha	n/a						
5	5b	Widespread Habitat - Non designated Land	Contamination of aquatic habitat which prevents fishing or aquaculture or renders is inaccessible to the public.	n/a						
7	6	Groundwater Body - Source Protection Zone (SPZ) for Public Drinking Water Supplies (Note - refer to EA website for SPZ aquifer maps.)	>1ha SPZ or >1000 person-hours interruption	n/a						
8	6	Groundwater Body (non-SPZ)	1-100ha of groundwater body where the WFD status has been lowered*	2 (off site)	✓	✓	✓	✓	✓	✓
9	6	Groundwater (non-groundwater body wrt Water Framework Directive)	Please indicate if non groundwater body is a pathway to another receptor.	Pathway Only (on site)						
10	7	Soil or sediment (i.e. as receptor rather than purely a pathway)	Contamination of 10-100ha of land etc. as per Widespread Habitat; Contamination sufficient to be deemed environmental damage (Environmental Liability Directive)	2	✓	✓	✓	✓	✓	✓
11	8	Built environment	Damage above a level at which designation of importance would be withdrawn.	n/a						
12	9	Various receptors								
13	10	Particular species	Loss of 1-10% of animal or 5-50% of plant ground cover.	n/a						
14	11	Marine	>2ha littoral or sub-littoral zone, >100ha of open sea benthic community, >100 dead sea birds (>500 gulls), >5 dead/significantly impaired sea mammals	2	✓	✓	✓	✓	✓	✓
15	12	Fresh and estuarine water habitats	WFD Chemical or ecological status lowered by one class for >2km of watercourse or >10% area (estuaries or ponds) or >2 ha of estuaries and >2ha of ponds. Plus interruption of drinking water supplies, as per DETR Table 6	2	✓	✓	✓	✓	✓	✓

* For the purpose of this assessment this is only considered to be relevant outside the site boundary for reasons as described in the report text.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 2 – Receptor Detail

Rather than try and identify every plausible receptor and threshold exceedance a review of the plausible pathways was undertaken and a conservative selection for the receptor was made given the sites environmental setting. Whilst there are a number of surface water receptors around the periphery of the site it was assumed each would feed directly into the SAC to the south of the site without any meaningful mitigation and therefore the assessment assumed a worst case threshold for the most sensitive receptor. The receptor for each compartment was identified in the assessment tables generated.

Table 2 - Receptor Detail

Row	DETR Table Ref	Receptor Type	MATTE threshold	Receptor Detail
2	2	Designated Land / Water Sites (Internationally important)	25-50% of site area, associated linear feature or population	<p>Habitats which contribute to the primary reason for selection of this site as a SAC include the type of Estuary, presence of large shallow inlets and bays and the presence of reefs. Further details may be found here: http://jncc.defra.gov.uk/protectedsites/sacselection/sac.asp?EUCode=UK0013118</p> <p>The species that are a primary reason for selection of this site as a SAC are grey seal and Shore dock. Shore dock may be the most sensitive receptor as it grows on rocky, sandy and raised beaches, shore platforms and the lower slopes of cliffs, and rarely in dune stacks. Plants can be found growing in isolation on the strand line, through to tall herb perennial communities at the base of flushed cliffs. However, it occurs only where a constant source of freshwater, running or static, is available. It is most commonly found growing by the side of streams entering beaches, on oozing soft-rock cliffs, and in rock clefts where flushing occurs. Populations of shore dock are known to fluctuate according to the severity of winter storms.</p> <p>Additional species present as a qualifying feature but which are not a primary reason for the site selection include Sea lamprey, River lamprey, Aline Shad, Twale shad and Otter.</p> <p>This MATTE threshold was selected on a conservative basis without detailed assessment of the linkage to the primary classification receptors. A linear feature associated with this site is considered to be a single stream (>2km in length from the site) and not all of the surface waters which discharge into Milford Haven.</p>

Table 3 – MATTE Scenarios

The MATTE scenarios were tabulated for each compartment but assuming the worst case receptor only. All credible scenarios were considered to have the potential to affect the same most sensitive receptor. Clearly, if through mitigation, this receptor was discounted or inherited receptor specific mitigation measures then an analysis of alternative receptors would need to be undertaken. For simplicity the key objective was seen to be the selection of an appropriate (conservative) tolerability threshold. Where appropriate, as the assessment is progressed certain scenarios may be grouped into lower severity threshold groups which will result in an adjustment in how the overall Establishment Risks are summed.

Table 3- MATTE Scenarios

Row	DETR Table Ref	Receptor Type	MATTE threshold	Credible MATTE Scenarios
2	2	Designated Land / Water Sites (Internationally important)	25-50% of site area, associated linear feature or population	<p>All Scenarios are considered to have the potential to result in an impact at the SAC by the nature of the presence of surface water features at the site boundaries which drain into the SAC. Of all the individual MAS/Compartment scenarios 34 of them are considered likely to have a lesser effect (MATTE threshold of 2) at this ultimate receptor. Others have been screened out completely. Please see the accompanying MATTE assessment worksheets for a detailed assessment on the scenarios for each compartment, potential receptor that could be affected and the selected MATTE level. By way of a summary the following represents a selection of the credible scenarios which could plausibly result in this level of impact from a storage tank compartment:</p> <ul style="list-style-type: none"> Overfilling of a Storage Tank Fire associated with a Storage Tank Catastrophic Tank Failure Tank Leak Tank Floor Release Bund failure resulting in release of product from secondary containment Addition and release of fire water from secondary containment

Table 4 – Dangerous Substances with Environmental Risk

At the case study site the substances are generally straight forward in terms of categorising the inventory and risk drivers for

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

environmental impact. The table below provides a summary for some of the site's inventory. In addition due consideration has been given to a range of intermediate products, additives and process related chemicals. In particular the potential for H₂S and HF releases was considered as a result of MAS associated with specific process equipment.

Table 4 - Dangerous Substances with Environmental Risk

Substance Reference	Substance (or group of substances)				Maximum Inventory	Description	Physical State	(Max Tank) Quantity	Ref for info
	Comm Name	IUPAC Name	CAS Number	CHIP Index					
1	Crude	See appended site MSDS sheets for more detailed information on this substance.			R12, R36, R50, R57, R59, R63, R66, R69, R70, R73, R75, R78, R80, R83, R84, R86, R87, R88, R90, R91, R92, R93, R94, R95, R96, R97, R98, R99, R100, R102, R103, R104, R105, R106, R107, R108, R109, R110, R111, R112, R113, R114, R115, R116, R117, R118, R119, R120, R121, R122, R123, R124, R125, R126, R127, R128, R129, R130, R131, R132, R133, R134, R135, R136, R137, R138, R139, R140, R141, R142, R143, R144, R145, R146, R147, R148, R149, R150, R151, R152, R153, R154, R155, R156, R157, R158, R159, R160, R161, R162, R163, R164, R165, R166, R167, R168, R169, R170, R171, R172, R173, R174, R175, R176, R177, R178, R179, R180, R181, R182, R183, R184, R185, R186, R187, R188, R189, R190, R191, R192, R193, R194, R195, R196, R197, R198, R199, R200, R201, R202, R203, R204, R205, R206, R207, R208, R209, R210, R211, R212, R213, R214, R215, R216, R217, R218, R219, R220, R221, R222, R223, R224, R225, R226, R227, R228, R229, R230, R231, R232, R233, R234, R235, R236, R237, R238, R239, R240, R241, R242, R243, R244, R245, R246, R247, R248, R249, R250, R251, R252, R253, R254, R255, R256, R257, R258, R259, R260, R261, R262, R263, R264, R265, R266, R267, R268, R269, R270, R271, R272, R273, R274, R275, R276, R277, R278, R279, R280, R281, R282, R283, R284, R285, R286, R287, R288, R289, R290, R291, R292, R293, R294, R295, R296, R297, R298, R299, R300, R301, R302, R303, R304, R305, R306, R307, R308, R309, R310, R311, R312, R313, R314, R315, R316, R317, R318, R319, R320, R321, R322, R323, R324, R325, R326, R327, R328, R329, R330, R331, R332, R333, R334, R335, R336, R337, R338, R339, R340, R341, R342, R343, R344, R345, R346, R347, R348, R349, R350, R351, R352, R353, R354, R355, R356, R357, R358, R359, R360, R361, R362, R363, R364, R365, R366, R367, R368, R369, R370, R371, R372, R373, R374, R375, R376, R377, R378, R379, R380, R381, R382, R383, R384, R385, R386, R387, R388, R389, R390, R391, R392, R393, R394, R395, R396, R397, R398, R399, R400, R401, R402, R403, R404, R405, R406, R407, R408, R409, R410, R411, R412, R413, R414, R415, R416, R417, R418, R419, R420, R421, R422, R423, R424, R425, R426, R427, R428, R429, R430, R431, R432, R433, R434, R435, R436, R437, R438, R439, R440, R441, R442, R443, R444, R445, R446, R447, R448, R449, R450, R451, R452, R453, R454, R455, R456, R457, R458, R459, R460, R461, R462, R463, R464, R465, R466, R467, R468, R469, R470, R471, R472, R473, R474, R475, R476, R477, R478, R479, R480, R481, R482, R483, R484, R485, R486, R487, R488, R489, R490, R491, R492, R493, R494, R495, R496, R497, R498, R499, R500, R501, R502, R503, R504, R505, R506, R507, R508, R509, R510, R511, R512, R513, R514, R515, R516, R517, R518, R519, R520, R521, R522, R523, R524, R525, R526, R527, R528, R529, R530, R531, R532, R533, R534, R535, R536, R537, R538, R539, R540, R541, R542, R543, R544, R545, R546, R547, R548, R549, R550, R551, R552, R553, R554, R555, R556, R557, R558, R559, R560, R561, R562, R563, R564, R565, R566, R567, R568, R569, R570, R571, R572, R573, R574, R575, R576, R577, R578, R579, R580, R581, R582, R583, R584, R585, R586, R587, R588, R589, R590, R591, R592, R593, R594, R595, R596, R597, R598, R599, R600, R601, R602, R603, R604, R605, R606, R607, R608, R609, R610, R611, R612, R613, R614, R615, R616, R617, R618, R619, R620, R621, R622, R623, R624, R625, R626, R627, R628, R629, R630, R631, R632, R633, R634, R635, R636, R637, R638, R639, R640, R641, R642, R643, R644, R645, R646, R647, R648, R649, R650, R651, R652, R653, R654, R655, R656, R657, R658, R659, R660, R661, R662, R663, R664, R665, R666, R667, R668, R669, R670, R671, R672, R673, R674, R675, R676, R677, R678, R679, R680, R681, R682, R683, R684, R685, R686, R687, R688, R689, R690, R691, R692, R693, R694, R695, R696, R697, R698, R699, R700, R701, R702, R703, R704, R705, R706, R707, R708, R709, R710, R711, R712, R713, R714, R715, R716, R717, R718, R719, R720, R721, R722, R723, R724, R725, R726, R727, R728, R729, R730, R731, R732, R733, R734, R735, R736, R737, R738, R739, R740, R741, R742, R743, R744, R745, R746, R747, R748, R749, R750, R751, R752, R753, R754, R755, R756, R757, R758, R759, R760, R761, R762, R763, R764, R765, R766, R767, R768, R769, R770, R771, R772, R773, R774, R775, R776, R777, R778, R779, R780, R781, R782, R783, R784, R785, R786, R787, R788, R789, R790, R791, R792, R793, R794, R795, R796, R797, R798, R799, R800, R801, R802, R803, R804, R805, R806, R807, R808, R809, R810, R811, R812, R813, R814, R815, R816, R817, R818, R819, R820, R821, R822, R823, R824, R825, R826, R827, R828, R829, R830, R831, R832, R833, R834, R835, R836, R837, R838, R839, R840, R841, R842, R843, R844, R845, R846, R847, R848, R849, R850, R851, R852, R853, R854, R855, R856, R857, R858, R859, R860, R861, R862, R863, R864, R865, R866, R867, R868, R869, R870, R871, R872, R873, R874, R875, R876, R877, R878, R879, R880, R881, R882, R883, R884, R885, R886, R887, R888, R889, R890, R891, R892, R893, R894, R895, R896, R897, R898, R899, R900, R901, R902, R903, R904, R905, R906, R907, R908, R909, R910, R911, R912, R913, R914, R915, R916, R917, R918, R919, R920, R921, R922, R923, R924, R925, R926, R927, R928, R929, R930, R931, R932, R933, R934, R935, R936, R937, R938, R939, R940, R941, R942, R943, R944, R945, R946, R947, R948, R949, R950, R951, R952, R953, R954, R955, R956, R957, R958, R959, R960, R961, R962, R963, R964, R965, R966, R967, R968, R969, R970, R971, R972, R973, R974, R975, R976, R977, R978, R979, R980, R981, R982, R983, R984, R985, R986, R987, R988, R989, R990, R991, R992, R993, R994, R995, R996, R997, R998, R999, R1000, R1001, R1002, R1003, R1004, R1005, R1006, R1007, R1008, R1009, R1010, R1011, R1012, R1013, R1014, R1015, R1016, R1017, R1018, R1019, R1020, R1021, R1022, R1023, R1024, R1025, R1026, R1027, R1028, R1029, R1030, R1031, R1032, R1033, R1034, R1035, R1036, R1037, R1038, R1039, R1040, R1041, R1042, R1043, R1044, R1045, R1046, R1047, R1048, R1049, R1050, R1051, R1052, R1053, R1054, R1055, R1056, R1057, R1058, R1059, R1060, R1061, R1062, R1063, R1064, R1065, R1066, R1067, R1068, R1069, R1070, R1071, R1072, R1073, R1074, R1075, R1076, R1077, R1078, R1079, R1080, R1081, R1082, R1083, R1084, R1085, R1086, R1087, R1088, R1089, R1090, R1091, R1092, R1093, R1094, R1095, R1096, R1097, R1098, R1099, R1100, R1101, R1102, R1103, R1104, R1105, R1106, R1107, R1108, R1109, R1110, R1111, R1112, R1113, R1114, R1115, R1116, R1117, R1118, R1119, R1120, R1121, R1122, R1123, R1124, R1125, R1126, R1127, R1128, R1129, R1130, R1131, R1132, R1133, R1134, R1135, R1136, R1137, R1138, R1139, R1140, R1141, R1142, R1143, R1144, R1145, R1146, R1147, R1148, R1149, R1150, R1151, R1152, R1153, R1154, R1155, R1156, R1157, R1158, R1159, R1160, R1161, R1162, R1163, R1164, R1165, R1166, R1167, R1168, R1169, R1170, R1171, R1172, R1173, R1174, R1175, R1176, R1177, R1178, R1179, R1180, R1181, R1182, R1183, R1184, R1185, R1186, R1187, R1188, R1189, R1190, R1191, R1192, R1193, R1194, R1195, R1196, R1197, R1198, R1199, R1200, R1201, R1202, R1203, R1204, R1205, R1206, R1207, R1208, R1209, R1210, R1211, R1212, R1213, R1214, R1215, R1216, R1217, R1218, R1219, R1220, R1221, R1222, R1223, R1224, R1225, R1226, R1227, R1228, R1229, R1230, R1231, R1232, R1233, R1234, R1235, R1236, R1237, R1238, R1239, R1240, R1241, R1242, R1243, R1244, R1245, R1246, R1247, R1248, R1249, R1250, R1251, R1252, R1253, R1254, R1255, R1256, R1257, R1258, R1259, R1260, R1261, R1262, R1263, R1264, R1265, R1266, R1267, R1268, R1269, R1270, R1271, R1272, R1273, R1274, R1275, R1276, R1277, R1278, R1279, R1280, R1281, R1282, R1283, R1284, R1285, R1286, R1287, R1288, R1289, R1290, R1291, R1292, R1293, R1294, R1295, R1296, R1297, R1298, R1299, R1300, R1301, R1302, R1303, R1304, R1305, R1306, R1307, R1308, R1309, R1310, R1311, R1312, R1313, R1314, R1315, R1316, R1317, R1318, R1319, R1320, R1321, R1322, R1323, R1324, R1325, R1326, R1327, R1328, R1329, R1330, R1331, R1332, R1333, R1334, R1335, R1336, R1337, R1338, R1339, R1340, R1341, R1342, R1343, R1344, R1345, R1346, R1347, R1348, R1349, R1350, R1351, R1352, R1353, R1354, R1355, R1356, R1357, R1358, R1359, R1360, R1361, R1362, R1363, R1364, R1365, R1366, R1367, R1368, R1369, R1370, R1371, R1372, R1373, R1374, R1375, R1376, R1377, R1378, R1379, R1380, R1381, R1382, R1383, R1384, R1385, R1386, R1387, R1388, R1389, R1390, R1391, R1392, R1393, R1394, R1395, R1396, R1397, R1398, R1399, R1400, R1401, R1402, R1403, R1404, R1405, R1406, R1407, R1408, R1409, R1410, R1411, R1412, R1413, R1414, R1415, R1416, R1417, R1418, R1419, R1420, R1421, R1422, R1423, R1424, R1425, R1426, R1427, R1428, R1429, R1430, R1431, R1432, R1433, R1434, R1435, R1436, R1437, R1438, R1439, R1440, R1441, R1442, R1443, R1444, R1445, R1446, R1447, R1448, R1449, R1450, R1451, R1452, R1453, R1454, R1455, R1456, R1457, R1458, R1459, R1460, R1461, R1462, R1463, R1464, R1465, R1466, R1467, R1468, R1469, R1470, R1471, R1472, R1473, R1474, R1475, R1476, R1477, R1478, R1479, R1480, R1481, R1482, R1483, R1484, R1485, R1486, R1487, R1488, R1489, R1490, R1491, R1492, R1493, R1494, R1495, R1496, R1497, R1498, R1499, R1500, R1501, R1502, R1503, R1504, R1505, R1506, R1507, R1508, R1509, R1510, R1511, R1512, R1513, R1514, R1515, R1516, R1517, R1518, R1519, R1520, R1521, R1522, R1523, R1524, R1525, R1526, R1527, R1528, R1529, R1530, R1531, R1532, R1533, R1534, R1535, R1536, R1537, R1538, R1539, R1540, R1541, R1542, R1543, R1544, R1545, R1546, R1547, R1548, R1549, R1550, R1551, R1552, R1553, R1554, R1555, R1556, R1557, R1558, R1559, R1560, R1561, R1562, R1563, R1564, R1565, R1566, R1567, R1568, R1569, R1570, R1571, R1572, R1573, R1574, R1575, R1576, R1577, R1578, R1579, R1580, R1581, R1582, R1583, R1584, R1585, R1586, R1587, R1588, R1589, R1590, R1591, R1592, R1593, R1594, R1595, R1596, R1597, R1598, R1599, R1600, R1601, R1602, R1603, R1604, R1605, R1606, R1607, R1608, R1609, R1610, R1611, R1612, R1613, R1614, R1615, R1616, R1617, R1618, R1619, R1620, R1621, R1622, R1623, R1624, R1625, R1626, R1627, R1628, R1629, R1630, R1631, R1632, R1633, R1634, R1635, R1636, R1637, R1638, R1639, R1640, R1641, R1642, R1643, R1644, R1645, R1646, R1647, R1648, R1649, R1650, R1651, R1652, R1653, R1654, R1655, R1656, R1657, R1658, R1659, R1660, R1661, R1662, R1663, R1664, R1665, R1666, R1667, R1668, R1669, R1670, R1671, R1672, R1673, R1674, R1675, R1676, R1677, R1678, R1679, R1680, R1681, R1682, R1683, R1684, R1685, R1686, R1687, R1688, R1689, R1690, R1691, R1692, R1693, R1694, R1695, R1696, R1697, R1698, R1699, R1700, R1701, R1702, R1703, R1704, R1705, R1706, R1707, R1708, R1709, R1710, R1711, R1712, R1713, R1714, R1715, R1716, R1717, R1718, R1719, R1720, R1721, R1722, R1723, R1724, R1725, R1726, R1727, R1728, R1729, R1730, R1731, R1732, R1733, R1734, R1735, R1736, R1737, R1738, R1739, R1740, R1741, R1742, R1743, R1744, R1745, R1746, R1747, R1748, R1749, R1750, R1751, R1752, R1753, R1754, R1755, R1756, R1757, R1758, R1759, R1760, R1761, R1762, R1763, R1764, R1765, R1766, R1767, R1768, R1769, R1770, R1771, R1772, R1773, R1774, R1775, R1776, R1777, R1778, R1779, R1780, R1781, R1782, R1783, R1784, R1785, R1786, R1787, R1788, R1789, R1790, R1791, R1792, R1793, R1794, R1795, R1796, R1797, R1798, R1799, R1800, R1801, R1802, R1803, R1804, R1805, R1806, R1807, R1808, R1809, R1810, R1811, R1812, R1813, R1814, R1815, R1816, R1817, R1818, R1819, R1820, R1821, R1822, R1823, R1824, R1825, R1826, R1827, R1828, R1829, R1830, R1831, R1832, R1833, R1834, R1835, R1836, R1837, R1838, R1839, R1840, R1841, R1842, R1843, R1844, R1845, R1846, R1847, R1848, R1849, R1850, R1851, R1852, R1853, R1854, R1855, R1856, R1857, R1858, R1859, R1860, R1861, R1862, R1863, R1864, R1865, R1866, R1867, R1868, R1869, R1870, R1871, R1872, R1873, R1874, R1875, R1876, R1877, R1878, R1879, R1880, R1881, R1882, R1883, R1884, R1885, R1886, R1887, R1888, R1889, R1890, R1891, R1892, R1893, R1894, R1895, R1896, R1897, R1898, R1899, R1900, R1901, R1902, R1903, R1904, R1905, R1906, R1907, R1908, R1909, R1910, R1911, R1912, R1913, R1914, R1915, R1916, R1917, R1918, R1919, R1920, R1921, R1922, R1923, R1924, R1925, R1926, R1927, R1928, R1929, R1930, R1931, R1932, R1933, R1934, R1935, R1936, R1937, R1938, R1939, R1940, R1941, R1942, R1943, R1944, R1945, R1946, R1947, R1948, R1949, R1950, R1951, R1952, R1953, R1954, R1955, R1956, R1957, R1958, R1959, R1960, R1961, R1962, R1963, R1964, R1965, R1966, R1967, R1968, R1969, R1970, R1971, R1972, R1973, R1974, R1975, R1976, R1977, R1978, R1979, R1980, R1981, R1982, R1983, R1984, R1985, R1986, R1987, R1988, R1989, R1990, R1991, R1992, R1993, R1994, R1995, R1996, R1997, R1998, R1999, R2000, R2001, R2002, R2003, R2004, R2005, R2006, R2007, R2008, R2009, R2010, R2011, R2012, R2013, R2014, R2015, R2016, R2017, R2018, R2019, R2020, R2021, R2022, R2023, R2024, R2025, R2026, R2027, R2028, R2029, R2030, R2031, R2032, R2033, R2034, R2035, R2036, R2037, R2038, R2039, R2040, R2041, R2042, R2043, R2044, R2045, R2046, R2047, R2048, R2049, R2050, R2051, R2052, R2053, R2054, R2055, R2056, R2057, R2058, R2059, R2060, R2061, R2062, R2063, R2064, R2065, R2066, R2067, R2068, R2069, R2070, R2071, R2072, R2073, R2074, R2075, R2076, R2077, R2078, R2079, R2080, R2081, R2082, R2083, R2084, R2085, R2086, R2087, R2088, R2089, R2090, R2091, R2092, R2093, R2094, R2095, R2096, R2097, R2098, R2099, R2100, R2101, R2102, R2103, R2104, R2105, R2106, R2107, R2108, R2109, R2110, R2111, R2112, R2113, R2114, R2115, R2116, R2117, R2118, R2119, R2120, R2121, R2122, R2123, R2124, R2125, R2126, R2127, R2128, R2129, R2130, R2131, R2132, R2133, R2134, R2135, R2136, R2137, R2138, R2139, R2140, R2141, R2142, R2143, R2144, R2145, R2146, R2147, R2148, R2149, R2150, R2151, R2152, R2153, R2154, R2155, R2156, R2157, R2158, R2159, R2160, R2161, R2162, R2163, R2164, R2165, R2166, R2167, R2168, R2169, R2170, R2171, R2172, R2173, R2174, R2175, R2176, R2177, R2178, R2179, R2180, R2181, R2182, R2183, R2184, R2185, R2186, R2187, R2188, R2189, R2190, R2191, R2192, R2193, R2194, R2195, R2196, R2197, R2198, R2199, R2200, R2201, R2202, R2203, R2204, R2205, R2206, R2				

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Initiating event frequencies for each scenario were then adjusted based on appropriate multiplier factors and/or any other inherent mitigation measures. Multipliers take into account the quantity of a particular feature while the inherent mitigation is tasked with considering the in-built engineering controls which would limit the potential for the event to occur (i.e. associated with keeping materials within the primary containment vessel). The inherent mitigation can be illustrated on the left-hand side of a bow-tie in the form of barriers as illustrated in **Figure 6** for a **tank overfill event**. These are typically the elements of process safety which factor directly into the environmental risk assessment.

Multiple bow-ties may be required for each MAS and receptor to fully describe the barriers and mitigation processes considered in the assessment. The use of bow-ties in this case study has been incorporated to aid illustration and their use in actual assessments may not be required depending on the complexity of the barrier and mitigation analysis required.

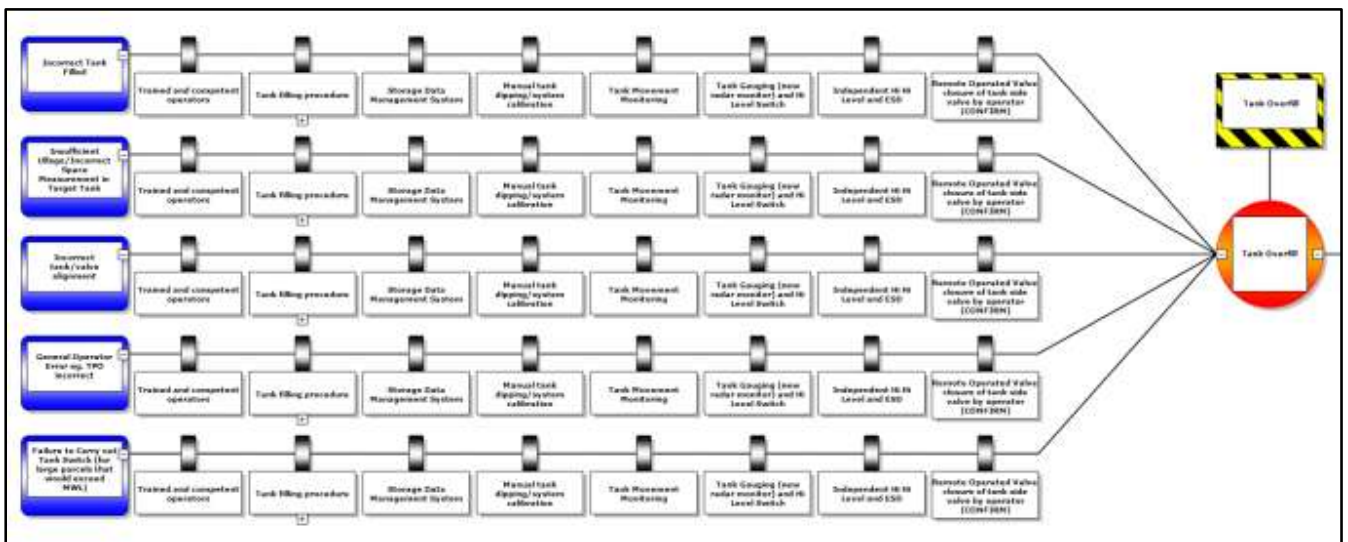


Figure 6 – Illustrative Bow-Tie barrier analysis for Tank Overfill Event

Each of these barriers represents proactive measures to prevent the event from happening and therefore can be considered as part of the unmitigated risk. Measures which could reduce the impact after the event (e.g. secondary and tertiary containment, contaminant fate and transport modelling, etc.) were used in the mitigation assessment stage and appear on the right hand side of the bow-tie.

In process safety, the role of these engineering controls may be assessed as part of a combined layers-of-protection analysis (LOPA) which itself considers the different safety intervention levels which form part of the operation of the asset. The end point of this process is a final unmitigated risk value which represents the probability of the event occurring once all of the aspects on the left hand side of the bow-tie are in place. It may be appropriate to sum the initiating frequencies for each branch on the left hand side of the bow-tie for each central event.

Summation of all scenarios within each individual compartment can then be used to provide an indication of the contribution of the risk from that asset to the combined total for all compartments at the site (or within a particular catchment with the potential to affect the same environmental receptor).

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

In the case study the contribution from each compartment was summed for each of the scenarios and this was converted to a percentage contribution of the intolerable criteria as defined by the guidance. At the unmitigated stage there is a requirement to qualitatively assess the potential severity of harm on an environmental receptor as outlined above. Based on the site setting and professional judgement considering the mechanisms for release, the volumes involved and the transport routes to the receptors a conservative selection of a potential 'Major' accident to the environment was selected for all events. Based on a medium term duration (greater than 1 but less than 10 years), this equated to a tolerability level of **B** and with a resultant intolerable criteria of 1×10^{-3} per year for each potentially affected surface water receptor (*see Tables 1 to 3 for information on criteria*). For some MAS, particularly those with a small potential release volume, the tolerability level was reduced to **A** (41 of the initial 384 scenarios). Examples where the MATTE tolerability criteria were reduced following an initial review of the initiating frequency data included;

- Releases associated with tanker failures at the road loading terminal – primarily due to its position within the site , provision of dedicated containment provisions and presence of hard standing;
- Releases from pipework due to the relatively small volumes involved;
- Releases to ground within the Process Areas due to presence of hardstanding, dedicated tertiary containment and relatively small volume releases.

Severity levels of 0 were effectively assigned to those scenarios not considered to have a MATTE potential. For completeness these MAS were retained within the assessment process for transparency and to enable revisions if required in the future.

The resultant distribution of potential **unmitigated** environmental risks at the site can then be presented in a map as shown in **Figure 7**. A map has been used as the data is geographic and this approach enables visualisation of risk drivers on a single image rather than through generation of multiple tables and/or matrices. With an excel and GIS linked system the contributions from individual MAS across the site or summed total risks by catchment/receptor can be presented.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

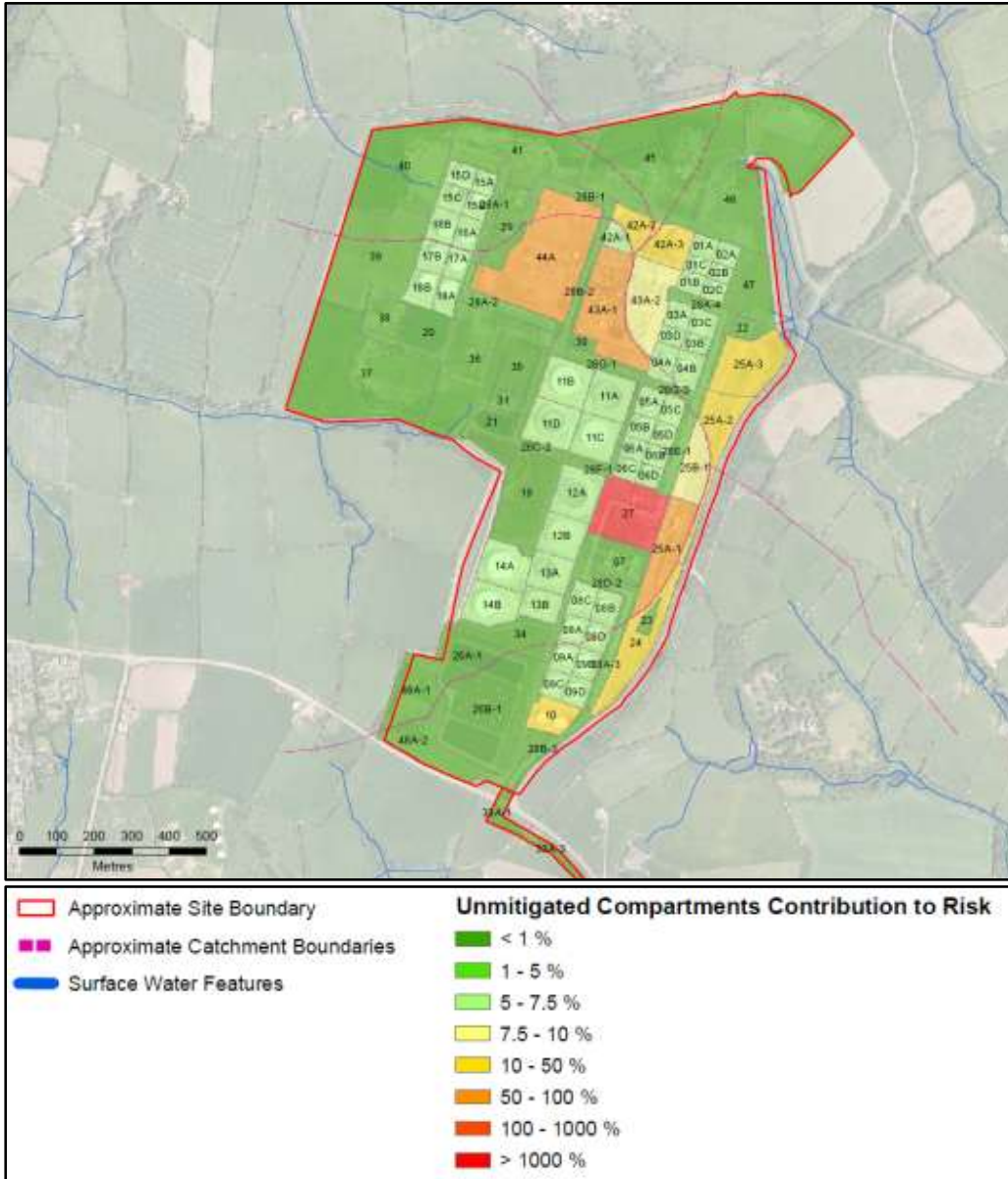


Figure 7 – Unmitigated risk contribution as a proportion of the intolerable risk frequency. Results above 100% indicate that an individual compartment would be capable of presenting an intolerable risk.

In this figure those compartments which are green contribute least to the overall environmental risk for a given receptor whilst those which are orange and red contribute the most. This combined with a ranked list of compartments and events can then be used to focus on those areas where mitigation assessments will make the biggest difference. In addition to the holistic view of risk presented in this figure it is also possible to present site wide data for each individual event type to identify whether it is individual events or individual compartments which contribute the most to the risk.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

At the unmitigated stage, and particularly for large and complex sites, the likelihood is that the risk will be intolerable and that further assessment will be required. In the case study site the unmitigated risk was several of orders of magnitude above the intolerable threshold (as illustrated by individual compartments contributing more than 100% of the intolerable threshold level of risk) and more detailed assessment of the potential impact on the environment from a range of MAS was required.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Assessing the Mitigated Risk

The mitigation aspect is concerned with identifying barriers or attenuation processes which could limit the impact following an event. There is a wide range of mitigation elements which could be considered. In the case study these were limited to the following elements:

- Secondary containment;
- Tertiary containment;
- Attenuation of overland flow;
- Assessment of ground penetration rates;
- Saturated zone attenuation; and
- Effectiveness of emergency response.

Each of the mitigation aspects can be illustrated in the bow-tie diagram. The following extract, presented as **Figure 8**, illustrates the wide range of mitigation measures which could be effective in reducing the chance of significant environmental impact following a **tank overflow event**.

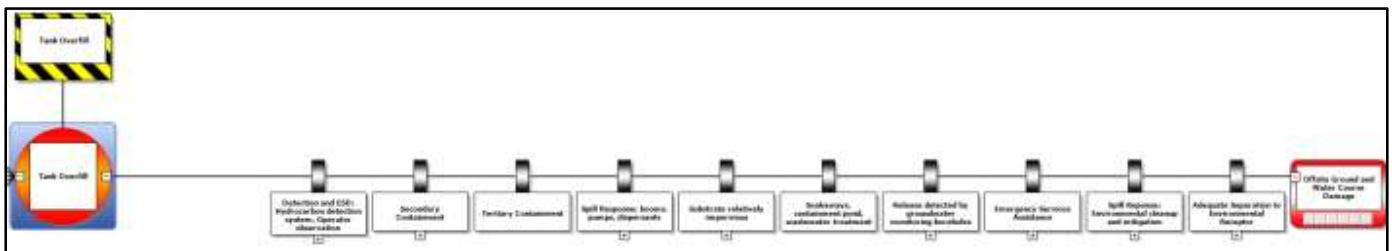


Figure 8 – Illustrative Bow-Tie mitigation analysis

For each mitigation measure there is then a series of assessments which may be completed to better understand the potential effectiveness in reducing the potential environmental impact at the receptor.

Depending on the level of unmitigated risk an assessment of which barriers will produce the most economical (time and cost) way of demonstrating that the Establishment risk is ALARP should be selected. The barriers generally fall into two categories;

- Engineering Controls; and
- Environmental Assessment.

For engineering barriers there is a wide range of published literature data which may be used to determine an appropriate range of mitigation factors for these features based on site specific conditions.

Environmental barriers may require more detailed assessment using site derived data to better estimate the fate and transport of the materials involved in the MATTE scenario but could also include qualitative assessments of a sites preparedness/ability to identify, intercept and/or remediate a release following an incident. Based on the CDOIF guidance the more complex assessments will fall into Stage 2 of the process while credit for existing safety measures which are appropriate for consideration in the event of a release (e.g. bund wall stability, tertiary containment provisions, presence of bund vapour monitors, etc) could and should be included in Stage 1 Step 2.

Taking the example shown in **Figure 9**, a release of product into secondary containment may result in penetration into the ground. In this instance the rate of this penetration and the resultant movement of product away from the tank can be

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

assessed quantitatively using stochastic modelling tools. For this mitigation barrier it then becomes possible to assign a mitigation factor which represents the likelihood of that barrier being successful in limiting the potential impact at the receptor. This process may also identify secondary ‘events’ which will then require a more detailed assessment in their own right; for example the failure of the bund wall as a result of an overflow event.

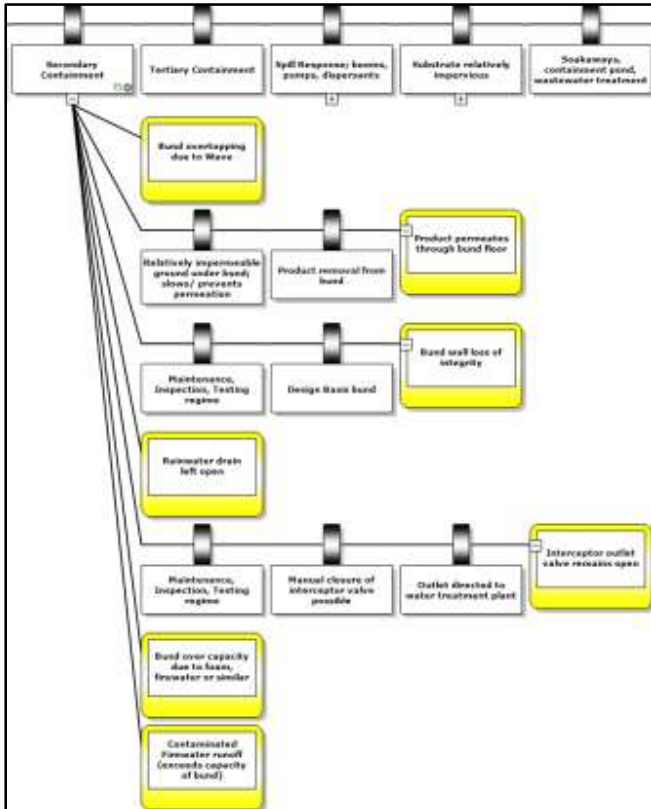


Figure 9 – Illustrative Bow-Tie barrier assessments

The process of assessing mitigation measures for each of the events may be presented in a flow chart as illustrated in **Figure 10**. The intention here is to incorporate a range of mitigation measures for each event in a methodical way and taking into account an increase in complexity as the assessment progresses. At the same time the degree and cost of assessment was kept aligned with the resultant level of risk with only more detailed assessment being undertaken for those scenarios which were identified as driving the risk and to a point at which the risk could be demonstrated to be at least TifALARP. The range of mitigation steps and the order in which those should be assessed will vary between sites.

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

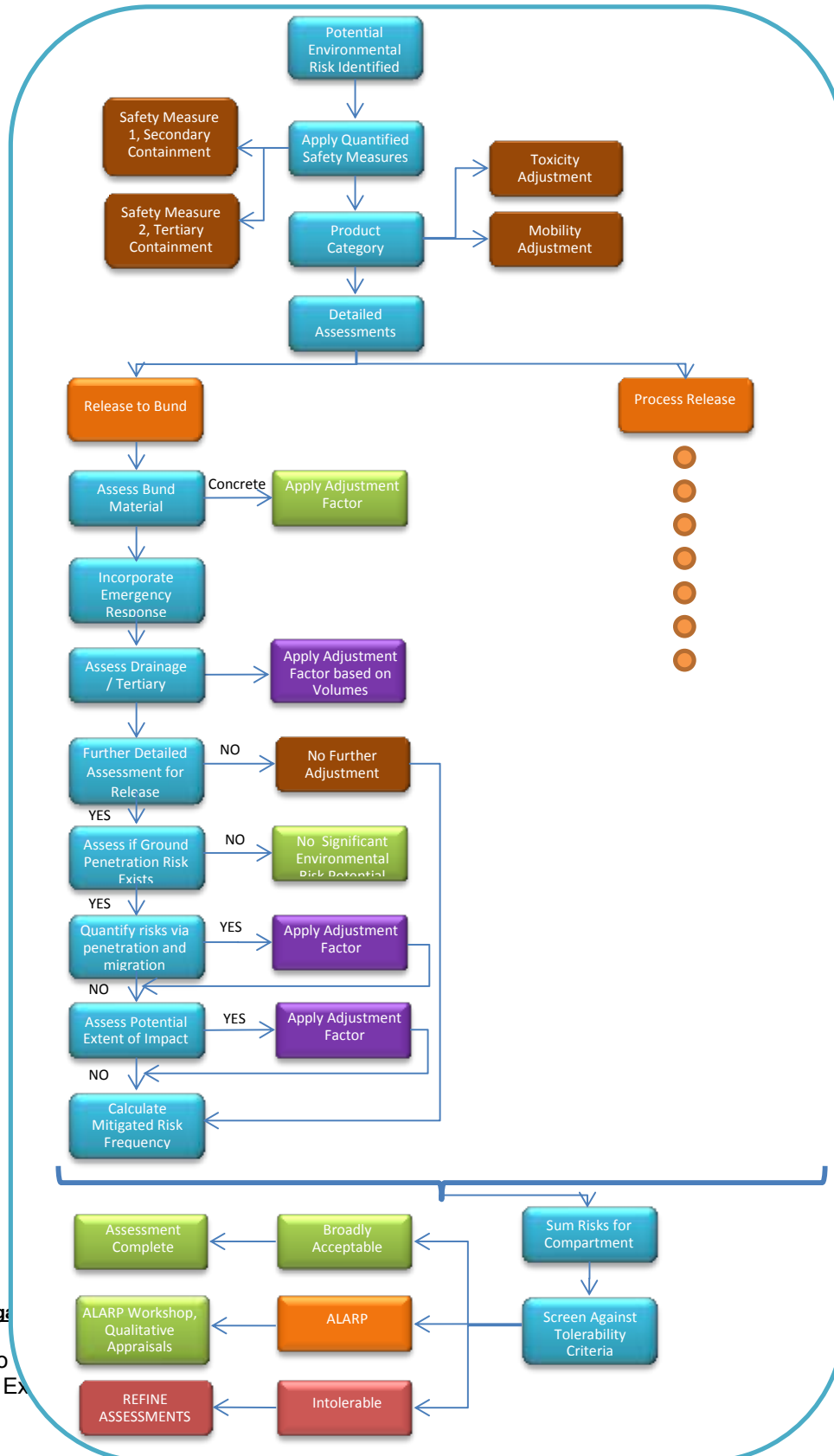


Figure 10 – Mitigation

Supplement to
Complex Site Ex

Example Mitigation Assessments

Mitigation would typically incorporate a range of aspects which would have the capability of limiting the potential for a release to reach a sensitive receptor. In essence these aspects consider the effectiveness of interrupting the pathway between the source and the receptor at potential risk. At its most basic, mitigation can take into account the preparedness of a site to respond to an incident both in terms of identifying that a release has occurred and that there is sufficient suitable equipment to contain and recover the released material.

The detection of a leak may be quantified by incorporating engineering controls which will aid the site – for example through inclusion of vapour monitors within bunds which could detect a liquid release from a tank overflow enabling additional controls to be implemented (e.g. drain valve closures, etc). As this example element of mitigation is an engineering control, there are recognised methods and data available to help quantify its likely effectiveness in terms of enabling the site to respond efficiently to the event and as such a numerical adjustment to the unmitigated release frequency may be applied.

For more qualitative elements, such as the ability of a site to respond, this may present more of a challenge to produce a numerical adjustment for. If a site has already demonstrated its practical ability to prevent a significant impact from a particular type of event then an adjustment factor may be generated with the effect of reducing the risk (albeit this is likely to be from a very small data set). Alternatively this aspect could be maintained for consideration in demonstrating that the risk is ALARP – that is that there is a procedure in place which has been assessed as likely to be effective through drills but which has not demonstrated its direct effectiveness and as such has not been quantitatively assessed. The Energy Institute QHRA¹ guidance will also assist sites in making qualitative assessments of human reliability and the role that may have in mitigation associated with procedures which involve human intervention.

Lastly, depending on the type of MAS, site specific parameter information could be assimilated from which the likelihood of a response being effective may be quantified.

In the case study site specific data was used to help assign mitigation factors following an overflow of a tank. The first step in the assessment was undertaken using a stochastic decision tree which considered a weighted range of input parameters from which those combinations which might lead to prevention of a significant release from occurring could be identified.

In this case the decision tree considered the following aspects:

- Potential overflow volumes;
- Area of the bund;
- Head of product which may exist in the bund (calculated from the above);
- Spill duration (i.e. how long might the product be sat in the bund before intervention is possible);
- Hydraulic conductivity of the bund floor; and
- Porosity of the underlying formation.

Values for each parameter were selected based on one or more of: site specific data, engineering drawings, literature sources and/or professional judgement. Where there was a range of possible values for a parameter each one was given a weighting based on an assumed likelihood. For example, the hydraulic conductivity of the bund floor may be variable based on a range of tests conducted at the site and the distribution of these results was used to define the lowest, most likely and upper end

¹ <https://www.energyinst.org/technical/human-and-organisational-factors/qhra>

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

estimates for this parameter.

A calculation was then completed at each step of the decision tree to ultimately produce an estimate of the volume of unrecovered product which might then penetrate the ground for each of a range of different spill volumes and durations. Where product had the potential to penetrate beyond a recoverable depth (1 m was used in the case study) a potential risk was considered to exist and the planned response was considered to have the potential to fail to mitigate the potential impact from the release. Given the range of parameter values and the number of calculation steps the decision tree grew into a 5 step process containing a total of 49 branches, each with an associated probability of occurring and a final calculated depth of penetration into the bund floor as a result of a range of plausible overfill events. All those probabilities where the resultant depth was greater than 1m were summed to generate an assessment of the likelihood that the response could fail to prevent a major accident to the environment from occurring. The assessment would then move on to the next mitigation step if required.

Having reduced the assessed risk by an approximate factor of 0.8 (i.e. there was calculated to be an 80% chance that the response to product recovery would effectively mitigate the environmental risk) a review was completed to assess whether further mitigation was required. In this case there were a number of compartments where consideration of additional mitigation measures was considered necessary.

For the tank overfill event the next step was to consider the implication of loss of containment through the bund floor. In this instance a source term could be generated for use in a fate and transport model which evaluated the migration rate of the most toxic and mobile component within the released product. Different assessments, producing different results were generated for each product type within each catchment and taking into consideration the distance from each tank to the nearest down gradient receptor.

When completed stochastically, using a range of model input values for each variable, the output provided a range of potential contaminant concentrations at different probability levels. The assessment was completed using the UK Regulator's adopted approach to assessing risks in groundwater and resulted in two-dimensional plume extents for different probability thresholds. **Figure 11** illustrates the results for the benzene component of the crude oil plumes for one specific compartment for two percentile levels; 50th percentile and 99th percentile. The results from this assessment were then evaluated based on the use of an appropriate acceptable target concentration at the receptor. In this instance a toxicity based threshold for benzene of 300 microgrammes per litre ($\mu\text{g/l}$) was used assuming crab larvae as the sensitive species at the receptor. It should be noted that for assessment of a MATTE this was considered an appropriate concentration to use rather than the EQS limits of 8-50 $\mu\text{g/l}$ (depending on whether an annual average or maximum allowable concentration is selected). No account of dilution was made due to the nature of the surface water courses (small streams with potential for significant baseflow contribution with limited or no upstream flow).

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

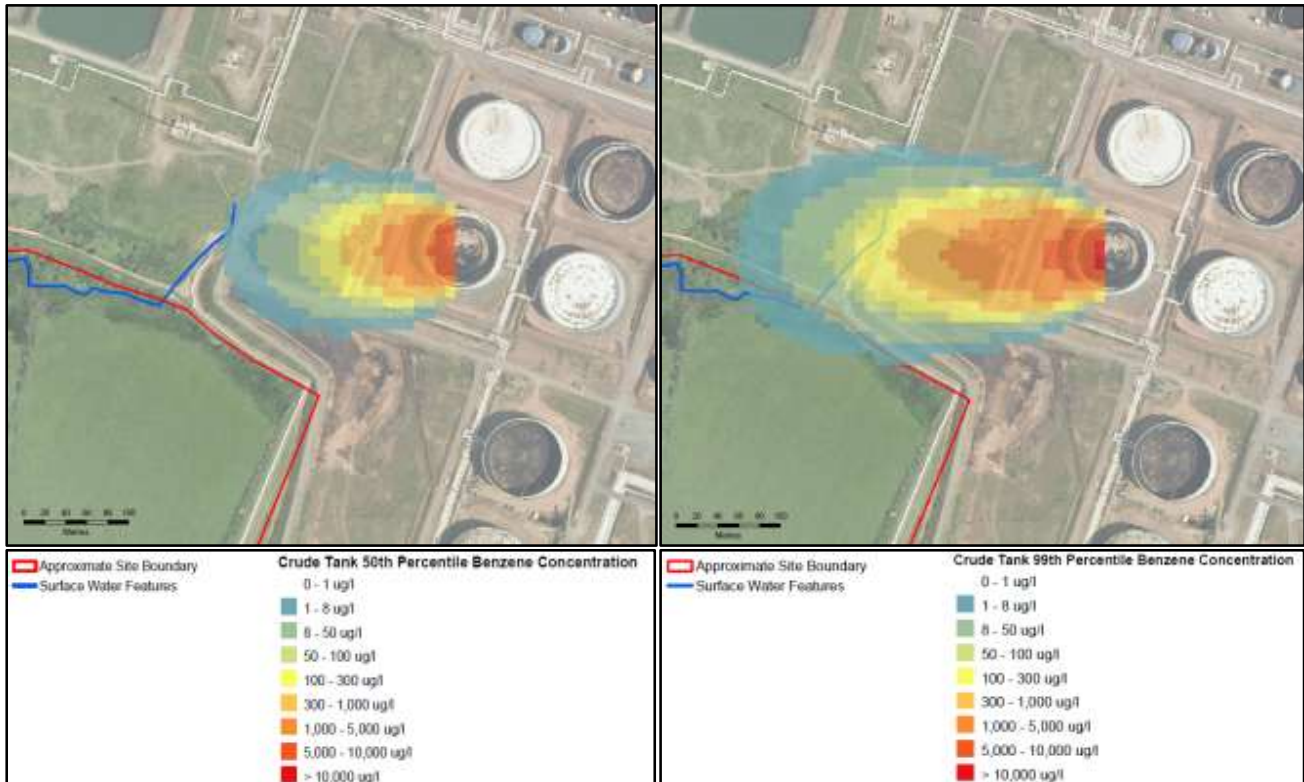


Figure 11 – Simulated dissolved phase concentrations in underlying groundwater from a crude release into secondary containment.

The 50th percentile plume indicated that the toxicity based threshold was not exceeded at the receptor and therefore an adjustment factor greater than 0.5 was likely to be applicable. At the 99th percentile the toxicity threshold was simulated to extend close to the surface water receptor and therefore a maximum adjustment factor of 0.01 was adopted. When applied to the initiating frequency and taking into account the already reduced risk of a significant subsurface source being generated, the overall adjustment along this pathway was reduced by a factor of 200 (i.e. the risk of a significant environmental impact at the surface water receptor from that event within that compartment was estimated to be 200 times lower than indicated by the unmitigated risk frequency).

In addition to the numerical calculations based on contaminant fate and transport, the risks following a release to secondary containment also considered the site setting and likelihood that even if product reached groundwater there would still be time (based on groundwater velocities) to attempt to recover/remediate the resultant plume of product. In this case it was assumed that a remedial approach would have a 50 per cent chance of being effective in minimising the subsequent risk of a major accident to the environment.

Overall reduction factors for this single major accident scenario at the site ranged from just 2 where a tank was close to a receptor and contained a gasoline component which only enabled an emergency response factor to be considered through to more than 1×10^5 for a remote crude tank where the chance of ground penetration and subsequent simulation of migration of dissolved phase constituents was assessed as being unlikely to result in detectable contamination at the sensitive down gradient receptor.

In addition to the numerical assessment there was also consideration of the bunding type, presence of tertiary containment, product toxicity/mobility, etc as part of the mitigation approach. Those bunds which were already constructed to good

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

practice with concrete walls and floors were given further mitigation adjustments whilst those with earth floors were not. Furthermore, bunds with automated valve systems to control rain water discharge were given a mitigation adjustment whilst manually operated valves were not.

For the tank floor release scenario a range of additional calculations were completed to help understand how the failure might evolve and the resultant flux of product which could go undetected through the base of the tank. As with the assessment of release to secondary containment this assessment made use of site specific parameters which could be used to calculate penetration rates through the unsaturated zone which could be compared with tank inspection schedules to assess whether a leak could be identified and remediated prior to the product reaching groundwater. Where the product could reach the groundwater the extent of spreading was assessed and used as a source term for fate and transport modelling in a similar way as the release into secondary containment described above. In some instances where the flux rate was greater than the ground's capacity to absorb the product the calculations indicated that breakthrough at the ground surface might occur – facilitating the chance to apply remedial work much more quickly than where product movement from the tank would potentially go unnoticed for a long period of time. This assessment was only completed in areas of the site where there was unlikely to be short-circuiting pathways, such as faults in the bedrock which could increase the migration rates.

For each of the remaining scenarios a similar approach was adopted – making use of environmental modelling where appropriate to assess the likelihood of a significant concentration of a contaminant reaching the receptors around the site. At this stage in the assessment there was no need to consider the extent of an impact at the receptor (or change the receptor) as the mitigation resulted in sufficient reduction in risk to make this step unnecessary. If required though, it would be possible to use the model outputs to estimate aspects such as time to impact, width of plumes affecting surface waters, mass flux, etc which could then be used to calculate an environmental harm index (EHI). This in turn would assist in generating an evaluation of the level of impact or help support an assessment of area/length of impact in-line with the CDOIF guidance. In many instances at the case study site this may have resulted in the accident scenarios being considered to have an implausible potential to result in a major accident hazard to the environment. This type of receptor focussed assessment was considered to fit better with a demonstration of TifALARP rather than being used to reduce the calculated risk to the lowest possible numerical value and was kept as a negotiating tool during discussions with the regulator.

For scenarios resulting in a release of liquid which could flow over the land surface – for instance following a bund failure – a digital elevation model (DEM) of the site was used together with oil spill modelling tools to estimate the flow direction and ultimate end point of the liquid. Analysis of the flow route was then used to assess whether additional bunds were intersected which could provide further containment, whether the tertiary drainage system was intersected and whether, in any case, the product would end up at a location where product recovery could be effective, thereby reducing the potential for a significant environmental impact. Mitigation adjustment factors were then derived qualitatively based on the information generated.

Fire water addition followed a similar process but took due account of the flammability of the product and therefore the likelihood that fire water/quench water would be added following a release.

Once each scenario had been assessed to an appropriate level the effect of all the mitigation elements were factored in to the unmitigated risk frequencies and a mitigated risk contribution figure was generated as shown in **Figure 12**.

In the case study example the application of a wide range of environmental mitigation assessments resulted in a reduction in assessed risk from intolerable at the site to tifALARP, thus providing the basis for demonstrating a case to the site's regulator that sufficient measures are already in place to manage the risk of a major accident to the environment.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

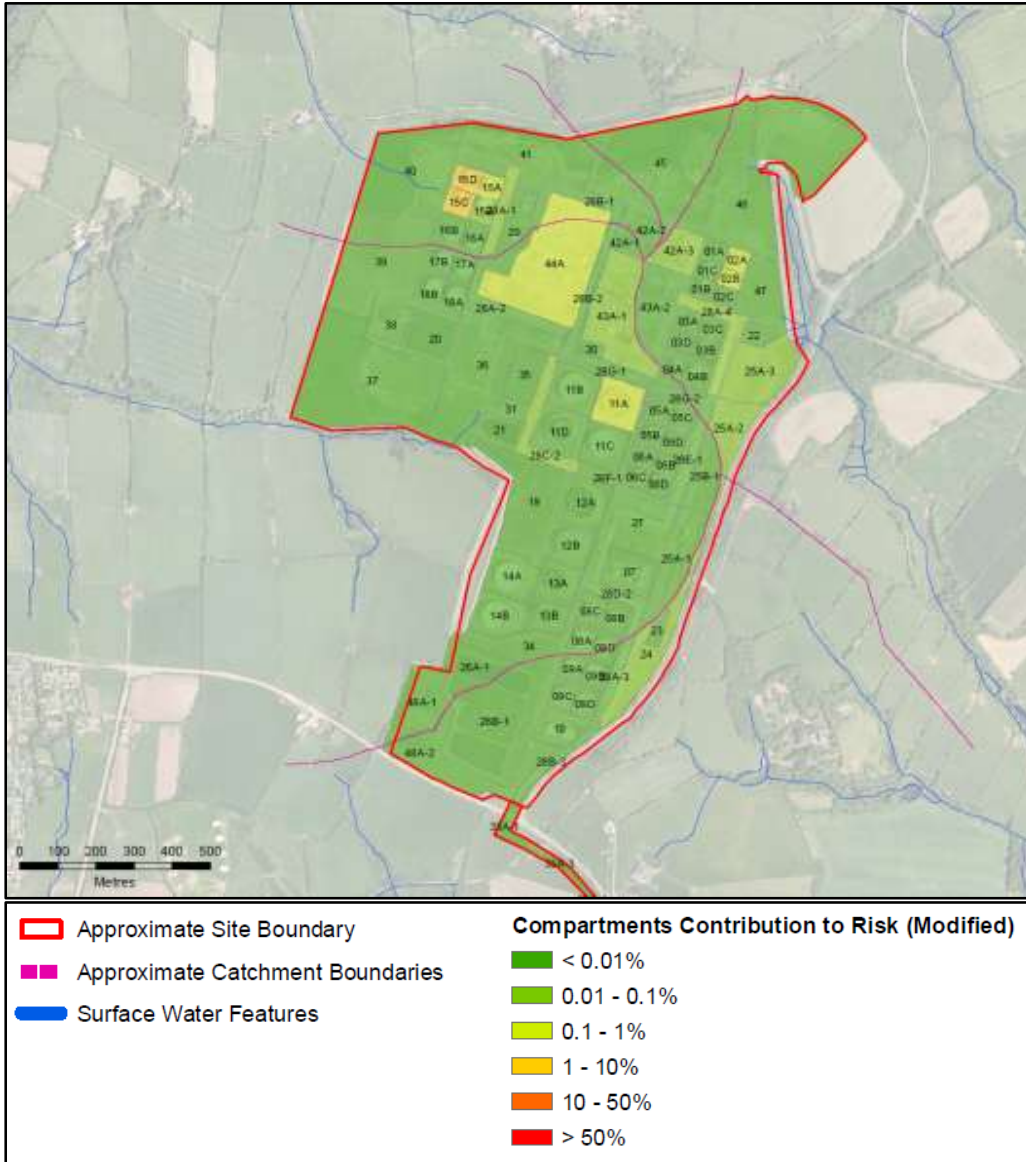


Figure 12 – Mitigated Risk Contribution as a proportion of the intolerable risk frequency.

As well as the graphical representation of the final risk contribution from each compartment a tabular summary of the risk driving scenarios was developed from the accompanying spreadsheet which provided a simple numerical summary of the results for each MAS at both the unmitigated and mitigated assessment stages.

An illustration of this is provided below which assumes all MAS in each of the compartments across all of the catchments could potentially impact the same receptor– a conservative assumption which can be refined further during Stage 2 where necessary.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table A illustrates the summing of each risk for each consequence level within each Catchment for both unmitigated and mitigated assessment stages. As there is the potential for each of the catchments to drain to the same ultimate receptor these may also be added to provide the overall establishment risk as indicated in the grand total row. The site has been split like this for ease of analysis and to help identify both the highest risk driving catchments at the site and the individual MAS which may need further consideration.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table A – Summary MAS by Catchment (and overall Establishment) risk levels and assumed unmitigated and mitigated risk levels.

Catchment	Compartment Type	Failure Type	CDOIF MATTE Consequence Level - Unmitigated	CDOIF MATTE Consequence Level - Mitigated	Sum of Event Frequency (per year)	Sum of Mitigated Event Frequency (per year)	Overall Mitigation Factor (summed)
A	Process	Overflow, CTF and PF to Secondary Containment	A	A	3.87E-03	4.02E-06	962
	Storage	Bund Failure	B	A	8.37E-05	1.63E-06	51
	Storage	Fire	B	A	2.08E-06	3.93E-09	527
	Storage	Fire Water resulting in Release to Ground	B	A	8.37E-05	5.77E-07	145
	Storage	Overflow, CTF and PF to Secondary Containment	B	A	8.37E-05	4.97E-08	1684
	Storage	Tank Floor Failure	B	A	6.00E-03	9.02E-05	67
	Transfer	Overflow, CTF and PF to Secondary Containment	A	A	3.61E-03	1.35E-05	266
	A Total				1.37E-02	1.10E-04	125
C	Process	Overflow, CTF and PF to Secondary Containment	A	A	4.74E-03	4.93E-08	96154
	Storage	Bund Failure	B	A	4.16E-05	1.38E-06	30
	Storage	Fire	B	A	7.98E-07	2.40E-08	33
	Storage	Fire Water resulting in Release to Ground	B	A	4.16E-05	8.53E-07	49
	Storage	Overflow, CTF and PF to Secondary Containment	B	A	4.16E-05	1.08E-06	38
	Storage	Tank Floor Failure	B	A	3.00E-03	5.27E-04	6
	C Total				7.86E-03	5.30E-04	15
D	Process	H2S Release	A	A	2.43E-04	1.22E-06	200
	Process	HF Release	A	A	7.80E-05	3.90E-07	200
	Process	Overflow, CTF and PF to Secondary Containment	A	A	1.65E-02	2.49E-05	661
	Storage	Bund Failure	B	A	1.78E-04	4.61E-07	387
	Storage	Fire	B	A	1.30E-06	7.03E-10	1845
	Storage	Fire Water resulting in Release to Ground	B	A	1.78E-04	6.77E-08	2632
	Storage	Overflow, CTF and PF to Secondary Containment	B	A	1.78E-04	1.83E-07	974
	Storage	Tank Floor Failure	B	A	1.30E-02	1.48E-05	877
	Transfer	Overflow, CTF and PF to Secondary Containment	A	A	1.09E-01	1.03E-05	10534
	D Total				1.39E-01	5.24E-05	2654
E	Storage	Bund Failure	B	A	4.10E-05	1.43E-09	28571
	Storage	Fire	B	A	1.50E-07	7.76E-12	19334
	Storage	Fire Water resulting in Release to Ground	B	A	4.10E-05	3.55E-10	115385
	Storage	Overflow, CTF and PF to Secondary Containment	B	A	4.10E-05	2.12E-09	19334
	Storage	Tank Floor Failure	B	A	3.00E-03	3.08E-06	976
	Transfer	Overflow, CTF and PF to Secondary Containment	A	A	2.23E-03	8.03E-06	277
E Total				5.35E-03	1.11E-05	482	
F	Transfer	Handarm Failure	B	B	1.22E-02	3.05E-03	4
	Transfer	Overflow, CTF and PF to Secondary Containment	A	A	8.40E-06	4.20E-06	2
F Total				1.22E-02	3.06E-03	4	
Grand Total				1.78E-01	3.76E-03	47	

Table B below is a summary of the information in the above table and provides summed risk levels for each catchment by consequence level.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table B – Summary of MAS risk levels by Catchment

Catchment	CDOIF MATTE Consequence Level - Unmitigated	CDOIF MATTE Consequence Level - Mitigated	Sum of Unmitigated Event Frequency (per year)	Sum of Mitigated Event Frequency (per year)
A	A+B	A	1.37E-02	1.10E-04
	B	-	6.25E-03	-
C	A+B	A	7.86E-03	5.30E-04
	B	-	3.13E-03	-
D	A+B	A	1.39E-01	5.24E-05
	B	-	1.35E-02	-
E	A+B	A	5.35E-03	1.11E-05
	B	-	3.12E-03	-
F	A+B	A+B	1.22E-02	3.06E-03
	B	B	1.22E-02	3.06E-03
Grand Total			1.78E-01	3.76E-03

Note: Catchment B is administration only with no significant MAS with MATTE potential identified

Table C below has then been used to plot the results for each compartment and for the establishment as a whole in line with the CDOIF guidance. These results are also represented graphically in the GIS figures provided earlier. The results in this format clearly indicate those catchments which drive the overall establishment risk and which will require further consideration (i.e. the jetty).

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table C - Results plotted on Unmitigated and Mitigated Matrix for individual Catchments (Grouped by MAS) and Establishment as a whole (X)

	Frequency per establishment per receptor per year (Unmitigated)						
Frequency at which CDOIF Consequence Level is equalled or exceeded	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D - MATTE							
C - MATTE							
B - MATTE						A, C, E	D, F, X
A - MATTE						C, E	A, D, F, X
Sub MATTE	Tolerability not considered by CDOIF						

	Frequency per establishment per receptor per year (Mitigated)						
Frequency at which CDOIF Consequence Level is equalled or exceeded	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D - MATTE							
C - MATTE							
B - MATTE						F, X	
A - MATTE				D, E	A, C	F, X	
Sub MATTE	Tolerability not considered by CDOIF						

Letters denote risks for catchments

X indicates overall Establishment risk assuming the same ultimate receptor for the Surface Water environment

	Broadly Acceptable
	TifALARP
	Intolerable

CDOIF

Chemical and Downstream Oil Industries Forum

Supplement to Guideline – ‘Environmental Risk
Tolerability for COMAH Establishments’

Frequently Asked Questions

CDOIF

**Chemical and Downstream
Oil Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Frequently Asked Questions (FAQs)

In completing environmental risk assessments for the establishment, it is important to consider how the CDOIF publication should be applied. The CDOIF methodology provides a high level first pass screening exercise which we have called Phase 1. A further more comprehensive Risk Assessment(s) may be required – this is called Phase 2:

Phase 1: As set out in the CDOIF guidance. Phase 1 screening comprises of two parts, see FAQ's below.

Phase 2: Not covered by the CDOIF guidance. Phase 2 assessments should only be completed if deemed necessary following the Phase 1 screening (for example if Phase 1 screening indicates there is no MATTE potential then detailed Phase 2 work will not be required). Phase 2 work should be carried out in conjunction with the local CA site inspection teams, and where necessary specialist consultants

The following commentary provides answers to commonly asked questions relating to the Phase 1 screening.

FAQ's General

What is the status of the CDOIF Guidance?

The status of the guidance is described in the Foreword.

How will CDOIF guidance work in conjunction with the containment policy score card?

For existing sites, the scorecard is a measure of compliance with the Containment Policy (CP). It is possible that the site can be compliant with the Containment Policy, without a measure being in place, if assessment shows it is not reasonably practicable to upgrade (see scorecard column L) – i.e. an ALARP demonstration. The Phase 1 screening and subsequent Phase 2 risk assessment (where necessary) determines what additional measures may be necessary to meet the CP (So Far As Is Reasonably Practicable). In other words, the screening and subsequent risk assessment will help to clarify the 'yellow' on the scorecard.

How long will the guidance remain 'live', allowing changes to it to be made as appropriate?

The guidance will remain open for the foreseeable future to allow for calibration as necessary. Note that CDOIF guidance can be updated at any point through its lifecycle.

Does this guidance help clarify duty holder responsibility under the environmental liability directive?

No, you will need to talk to your relevant trade body and discuss this separately with relevant government departments and agencies. See also <https://www.gov.uk/government/publications/environmental-damage-prevention-and-remediation-regulations-2009-guidance-for-england-and-wales>

Does the guidance provide any qualification or guidance on what constitutes harm or adverse effect?

Refer to L111 and DETR 1999 for more information as to what constitutes harm. Additional information is also provided in section 3.2.1 of the CDOIF Guidance.

What level of detail is the CA expecting for the Phase 1 Screening?

Worked examples for both simple and complex sites will be provided. Refer also to the FAQ's for Part 1 and Part 2 below. Many sites may already have much of the information required in order to complete the screening.

Reference should also be made to Appendix 5 of the CDOIF guidance which provides a template to assist in grouping substances to determine MATTE potential.

Can you use representative scenarios to simplify the screening process?

Yes, refer to the CDOIF guidance section 4.2.2 and to the Safety Report Assessment Guides (SRAG, <http://www.hse.gov.uk/comah/srag.htm>) for further information (please also note the expectation to include a scenario/scenarios exploring a multi-tank/multi-bund fire following explosion where this is credible).

How will the agencies ensure consistency across regulator training such that a national approach is taken to establishment risk assessment?

This will be achieved through training of regulatory teams. Inspection teams are kept apprised of the developing guidance and other relevant publications. The Better Regulation Review (BRR) challenge mechanism provides a process to query or challenge application of CP at a site level. The CA in agreeing a deadline for completion for Phase 1 screening has in its resourcing an approach to collectively review phase 1 results on a sector basis

FAQ's Part 1: Defining the types of environmental harm

What types of products should you consider in the Phase 1 screening?

If you are a COMAH establishment, any incident that can credibly cause a MATTE where a COMAH dangerous substance is involved should be included in the Phase 1 assessment. Table 4 in Appendix 5 provides some guidance to help you do this.

Can you 'group' similar products to reduce the number of screening assessments required?

Yes, this is a valid mechanism for simplifying the screening process. Reference should also be made to Appendix 5 of the CDOIF guidance which provides a template to assist in grouping substances to determine MATTE potential.

Do you need to complete an event tree for every scenario?

This would be considered a level of detail not required for phase 1 screening; however a simple event tree may be appropriate to demonstrate multiple pathways to single or separate receptors. The purpose of the phase 1 screening is to help determine the level of detail and nature of the assessment at phase 2 (refer to CDOIF guidance section 2.2 for further information).

How do you consider escalation in the risk assessment?

Only credible scenarios should be considered in the Phase 1 screening – i.e. what volume of product could credibly be lost to the receptor? (Refer to the Safety Report

Assessment Manual [SRAM] section 13 for help on determining credibility). It is important to understand what factors of an incident could affect the pathways to the receptor (for example a controlled burn may mean less product reaching a receptor, but tackling a fire may cause pollution from firewater/foam).

What is meant by 'mitigated' and 'unmitigated' when applied to the screening process?

The first step of the Phase 1 screening process is to determine the types of environmental harm that could occur, and whether these have MATTE potential – in the guidance this is referred to as the '*unmitigated* consequence', section 4.1 provides more information on this term.

For example: It is assumed that a storage tank fails. Primary containment (pipes, vessels, control systems) has been lost and the contents of the tank is free to migrate via the pathway to the receptor, unhindered by the existing secondary or tertiary containment, interceptors, pollution controls, spill response etc. No credit is taken at this stage for good design practices, inspection and maintenance regimes etc. This enables the 'worst case' source-pathway-receptor scenarios to be understood, and may indicate that - without any mitigation - the establishment presents an intolerable risk to the receptor/s.

The second step of the Phase 1 screening process is to complete the risk assessment by aggregating failure frequencies – these may be mitigated or unmitigated risk frequencies, section 6.2 provides more information.

For example: The same source-pathway-receptor scenarios examined in the first step are re-evaluated taking credit for the existing mitigation, such as good design measures, inspection and maintenance regimes, secondary and tertiary containment, monitoring systems, fire suppression systems, pollution detectors, human factors, emergency and spill response etc.

In summary, the whole screening process can be broken down into:

STEP 1 – Determine if you have a MATTE potential based on the products and volumes that you store (Appendix 5 can help to map this out). The scale of the unmitigated consequence can now be determined, which tells you what your target frequencies are (i.e. what is Intolerable/TifALARP/Broadly Acceptable).

STEP 2 – now you have the target frequencies, use section 6.2 to help aggregate the failure frequencies (these frequencies may be either mitigated or unmitigated) to determine what further risk reduction mechanisms may be required. The CA will as necessary query the origin of the claimed failure frequencies used, and any layers of protection that are claimed.

The worked examples provided to assist in the application of the guidance provides a practical example as to how to complete these two steps.

How can I determine the duration of environmental damage?

The Energy Institute have been commissioned to develop a report on environmental recovery periods based on incident reviews – this is due for release at the end of 2014.

In the interim, relevant publically available resources can be used to look for similar incidents involving similar products to provide a best estimate of duration. Resources include:

- EMARS: <https://emars.jrc.ec.europa.eu/>
- Aria: <http://www.aria.developpement-durable.gouv.fr/?lang=en>
- ITOPF Reports: <http://www.itopf.co.uk/information-services/publications/technical-reports/>

Where can I get more detail relating to underlying environmental information for consequence assessment, for example soil permeability?

Resources are identified in Appendix 3 of the CDOIF guidance; it is also recommend that a discussion is held with local agency inspection teams.

Can small streams which don't qualify as a receptor in terms of their length be considered as a pathway to further receptors?

Yes, this forms part of the source/pathway/receptor analysis.

In addition, if surface water does not have a WFD classification then it should be considered whether it could be a receptor as per 3.2.2 – Widespread Habitat (land/Water) – see threshold for non-designated water, p.13.

How do you assess land that is already contaminated within the site boundary?

Section 3.2.4 provides additional information on how to treat contaminated land on site. The Phase 2 assessment may provide further evidence as to why a MATTE is not credible based on a detailed assessment of the contaminated land within the site boundary (see environmental damage regulations guidance).

How do you consider non-productive groundwater, for example if the groundwater is on (or under) site but not going anywhere, or has no foreseeable use?

Non-productive groundwater is not considered a receptor, but may be a pathway. For Phase 1 screening, the EA mapping evidence (refer to appendix 3 and section 3.2.3 of the guidance) may be utilised to demonstrate that the body of water is not shown as a groundwater body. If this is not the case then more detailed analysis may be required during the Phase 2 assessment to demonstrate why the body of water is not considered as a receptor with MATTE potential – it is recommended that this should involve a dialogue with the relevant agency before detailed work is commenced.

Do the area thresholds quoted in the guidance include the area within the site boundary?

Yes

The Water Framework Directive guidance establishes area of impact criteria for a change in groundwater body status which differs from the CDOIF guidance. What area of impact should reflect a MATTE?

CDOIF has adopted the minimum area of impact of 1ha from the reporting requirements of the Seveso Directive and has established tolerability criteria on this basis. Thus, for COMAH risk assessment of groundwater impacts, severity of harm should use WFD chemical classification parameters BUT in terms of extent WFD area rules do not apply and the CDOIF agreed areas should be used. These have been developed to reflect the differing value of different types of groundwater (e.g. drinking water vs non-drinking water).

Considering multiple 'pathways' to a receptor following loss of containment can be difficult, particularly for large complex sites, is there a more efficient approach?

Developing conceptual site model may be a more efficient appropriate for Phase 1 screening. Greenleaves 3, Chapter 2, section 2.3 provides information on how to develop a conceptual model, refer to https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69450/pb13670-green-leaves-iii-1111071.pdf

Is it necessary to calibrate the tolerability requirements to help identify where the greatest risks exist?

Calibration is important to ensure that all relevant factors have been accounted for – for example realistic failure frequencies, and credit for mitigation measures that have been applied – what is important is to identify gaps and potential improvements that can be applied to reduce the risk. Refer also to section 4.3 of the CDOIF guidance for additional information.

What boundaries should be applied to help define where the highest risk lies?

CDOIF

**Chemical and Downstream
Oil Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

It is appropriate to set boundaries to help with phase 1 screening - simple boundaries should be defined such as minor release rate and major release rate. Data sources such as FRED (see below) already define these.

FAQ's Part 2: Risk criteria and evaluating risks

Where can I get failure rate data to enable me to complete the high level risk assessment?

Generic failure rate data is available from several sources, for example:

- HSE's Failure Rate and Event Data (FRED), see <http://www.hse.gov.uk/landuseplanning/failure-rates.pdf>
- The EA, SEPA and NRW 'All Measures Necessary' Guidance
- Company specific data that you may have (though this would need to be substantiated as part of any demonstration to the CA)

When completing risk assessments, mitigated failure rates can be used so long as they are clearly defined.

It is recommended that for phase 1 screening FRED data is used for simplicity, but company data is equally acceptable subject to the caveat above.

What boundaries should be applied to help define where the highest risk lies?

It is appropriate to set boundaries to help with phase 1 screening - simple boundaries should be defined such as minor release rate and major release rate. Data sources such as FRED already define these.

How far back do you need to go for unmitigated risk, for example double skinned tanks, bund liners?

Any appropriate measures that reduce the risk to the receptor can be adopted when completing a risk assessment – refer to the FAQ below on failure rates

For multiple receptors affected by one area of site, do you need to consider all of those receptors, or just that which has the most sensitive threshold?

The expectation is that all consequences should be assessed for each receptor. However, where the source/pathway and products/volumes are the same, risk aggregation need only be completed for the most sensitive threshold.

Do you need to add up all failure data for each tank, pipeline and valves etc. to determine the risk from the establishment?

Yes, but for the Phase 1 screening assessment the FRED data (or company data) used could already aggregate individual failure modes into a failure rate (for example the different ways in which a single tank can lose containment) in which case it does not need to be aggregated again. It is recommended that you check your source data, its

CDOIF

**Chemical and Downstream
Oil Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

origins and whether or not it includes aggregated failure modes. Also note that you only need to aggregate *independent* failure rates (e.g. independent tanks within a bund that can harm the same receptor).

Is a LOPA required as part of the Phase 1 screening?

No, this is not a requirement for Phase 1 screening - qualitative assessments are sufficient. Larger higher risk sites may require QRA/Semi-Quantitative assessment at Phase 2.

What measures can be used to reduce the risk of a MATTE?

There are many different measures that could be employed to reduce the risk of a MATTE. These could be either preventative or mitigatory measures, for example, primary, secondary or tertiary containment or planned responses to reduce the risk of pollution following a loss of containment.

How will assessments be judged if outcomes are 'intolerable' for receptors on-site or those already contaminated, or receptors that are not significant?

A discussion with the CA will determine if the risk is intolerable – further phase 2 assessments may be required to more accurately represent the risk. It is not the intent of the CA to issue prohibition notices as an immediate response to screening results since these might be based on overly conservative assumptions, or credit might not have been taken for all risk reduction measures in place. A Phase 1 intolerable risk would trigger further dialogue on risk reduction measures and more detailed QRA as appropriate. (N.B.: L111 para 352 – 359 discusses Serious deficiency and Prohibition of use)

CDOIF

Chemical and Downstream Oil Industries Forum

Supplement to Guideline – ‘Environmental Risk Tolerability for COMAH Establishments’

Storage Terminal Example

Whilst the CA cannot comment on the accuracy of any site specific data or assumptions, the worked example provided does demonstrate an appropriate interpretation and application of the CDOIF guidance, with a sufficient level of detail to allow the screening process to be complete

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Contents

1	Introduction	1
1.1	Limitations	1
2	Part 1: MATTE Definition and Thresholds	2
2.1	Establishment Overview	2
2.2	Establishment Location	2
2.3	Credible Release Scenarios	3
2.4	Environmental Receptors	4
2.5	Identification of Migration Pathways	5
2.6	MATTE Severity Thresholds	6
2.7	MATTE Consequence Levels	7
3	Part 2: Establishment Risk Frequencies	9
3.1	Failure Frequencies	9
3.2	Aggregating Failure Frequencies per Receptor	10
3.3	Worked Example of Tolerability Matrices	15
3.4	Outcome of Phase I Screening	16
4	Phase 2 Assessment	17

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

1 Introduction

This case study is an example of how a Phase I screening assessment would be carried out in accordance with the Guideline on Environmental Risk Tolerability for COMAH Establishments, Version 1.0 (the 'CDOIF Guidance'), published by the Chemical and Downstream Oil Industries Forum (CDOIF).

1.1 Limitations

This case study presents a simplified example of a fictional establishment to illustrate the approach to undertaking a Phase I screening assessment. The case study is not intended to be a complete description of the steps that would be undertaken when carrying out an assessment. It should be noted that a full Phase I assessment of environmental risk tolerability would include a detailed description of the environmental baseline at, and surrounding the establishment, a conceptual site model describing plausible source-pathway-receptor relationships, evaluation of credible scenarios and major accidents to the environment (MATTE) and justification of failure frequencies used in the tolerability assessment. For the purpose of this case study these elements have been summarised at a high level.

The reader should familiarise themselves with the detailed requirements of the CDOIF Guidance and it is likely that environmental specialists will need to be involved in the identification of MATTE and assessment of severity and duration of harm.

The focus of this case study is Phase I screening, as set out in the CDOIF Guidance; Phase 2 assessment is not covered in this example.

2 Part 1: MATTE Definition and Thresholds

2.1 Establishment Overview

The establishment is a fuel storage depot located on the shore of an estuary. Activities at the establishment include:

- Diesel storage in two large semi-buried storage tanks, T1 and T2, both with a maximum capacity of 10,000m³. The tanks are constructed of a welded steel liner surrounded by a concrete jacket. The tanks have been terraced into a steep hillside and are covered with soil.
- Diesel is delivered to the establishment by vessel. The vessel moors at a jetty which is within the establishment boundary. Diesel pipelines are present on a 75m long pipe bridge which lies directly above the estuary.
- Diesel is transferred from the vessel to the jetty pipelines by loading arms. The onshore pipelines which transfer the diesel to the tanks are above ground. The pipelines run across open ground and do not have cathodic protection or leak detection systems installed.
- Diesel is also exported from the establishment by commercial road tankers. The 35m³ capacity road tankers fill up at the road tanker loading bay. Approximately 10 tankers are filled each week.
- Mixed waste oils and water are stored in four above ground tanks:
 - Tank T3 with a capacity of 750m³;
 - Tank T4 with a capacity of 20m³; and
 - Tanks T7 and T8 both with capacities of 500m³.
- The waste oils and water are transferred by above ground pipelines and are loaded onto 35m³ commercial road tankers at the road loading bay for off-site removal. This activity takes place once a year, which involves approximately 20 tankers.
- Diesel fuel additive is stored in two above ground tanks T5 and T6, both with 53m³ capacity. The additive is delivered to the establishment by road tanker at the road loading bay. Additive is injected into the diesel during loading of the commercial road tankers.
- A redundant tank farm is located to the north east and east of the active diesel tanks. These redundant tanks have been cleaned and degassed; as such they do not require assessment at present. However, if these tanks were to be brought back into service the assessment would be updated.

2.2 Establishment Location

The establishment covers approximately 15 hectares and slopes steeply down towards the estuary. The majority of the site is unpaved, although the road loading bay and the foreshore area are surfaced in concrete. An industrial estate is located to the south and a small number of residential properties lie outside the establishment boundary.

A stream is located adjacent to the eastern boundary of the establishment; this accepts the outfall from the tank farm interceptor. The stream is then culverted under the adjacent industrial estate

and discharges into the estuary. The establishment has a second interceptor serving a separate drainage system. This interceptor is located on the foreshore and discharges directly into the estuary.

The geology comprises fractured rock and groundwater seepages can be seen in the exposed foreshore next to the estuary. A previous site investigation at the establishment has also identified a thin layer of permeable gravelly soil above the bedrock, which is likely to allow liquids at the surface to penetrate into the fractures within the bedrock.

2.3 Credible Release Scenarios

The existing Safety Report has identified a number of credible release scenarios, including releases of diesel, waste oils and water, mixed waste oils and water, and fire water. This case study has selected four of these credible scenarios as follows:

- release of diesel from tanks T1 and T2 (hazard reference 'H01'). This includes acute releases (e.g. catastrophic tank failure) and chronic releases from the tank bases;
- acute release of diesel during vessel unloading at the jetty (H02);
- acute release of diesel fuel additive during road tanker delivery to above ground tanks T5 and T6 (H03); and
- acute release of fire-water containing fire-fighting foam and entrained hydrocarbons during operations to combat a major fire (H04).

The existing hazard and effects register has identified a number of factors which make up each credible scenario, including:

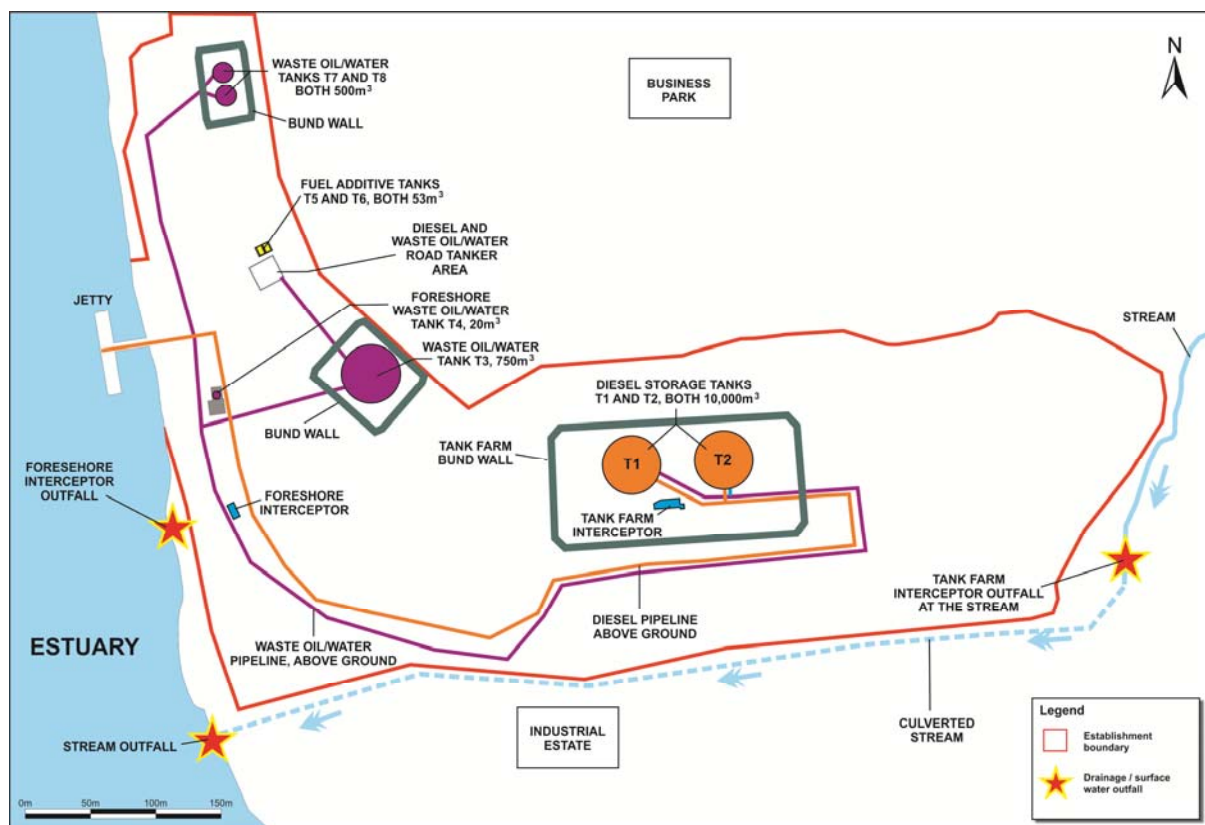
- source and maximum (worst case) release volume;
- causes of loss of containment;
- preventative controls; and
- mitigation controls.

It should be noted that a full Phase I assessment report would identify and describe each credible release scenario at the establishment in detail.

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits



2.4 Environmental Receptors

Section 3.1 Environmental Receptors, Appendix 2 and Appendix 3 provide information on the types of environmental receptors which need to be considered in the assessment. In this case study, a number of these types of environmental receptors are present within 10km of the establishment. For the purpose of this case study, four receptors have been selected to demonstrate how the unmitigated source – pathway – receptor linkages are identified.

- the adjacent estuary is classified as Receptor Type 6 – ‘widespread habitat – non designated water’ and Receptor Type 15 – ‘fresh and estuarine water habitats’;
- a fish farm within the estuary is also classified under Receptor Type 6 – ‘widespread habitat – non designated water’;
- a protected bird species, the Godwit, resides in the estuary. The Godwit occurs at nationally significant numbers in the estuary (i.e. in excess of 1% of the UK population), at 5.6% of the UK population. The Godwit is classified under Receptor Type 13 – ‘particular species’; and

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

- groundwater is present in the fractured bedrock underlying the establishment and is classified as a Receptor Type 8 – ‘groundwater body non-drinking water source’.

Detailed descriptions of the environmental and ecological baseline would be included in a full Phase I assessment report.

2.5 Identification of Migration Pathways

A conceptual site model has been developed to identify the ‘unmitigated’ migration pathways between credible release scenarios and the environmental receptors. The conceptual site model has identified a number of plausible source-pathway-receptor linkages, but also confirmed that some linkages are not plausible due to the absence of migration pathways. For the purposes of this case study an example plausible linkage is:

Source	Migration Pathway	Receptor
10,000m ³ release of diesel from storage in T1 and T2 (H01)	Drainage infrastructure	<ul style="list-style-type: none">• Estuary• Godwit living within the estuary• Fish farm in the estuary

In a full Phase I assessment report each plausible source-pathway-receptor linkage would be described.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

2.6 MATTE Severity Thresholds

Now that the plausible pollutant linkages have been identified, the scale of the unmitigated impact for each of the receptors has been evaluated and 'sub-MATTE' level impacts have been excluded from further assessment. Section 3.2 MATTE Thresholds and Table 1 in Appendix 4 provides the thresholds used to determine whether an impact is 'sub-MATTE' or 'MATTE'.

An example of the MATTE severity comparison for release scenario H01 is presented below. A ✘ indicates the impact is unlikely to exceed the MATTE severity thresholds. A ✓ denotes the linkages which are likely to exceed the MATTE severity thresholds. These will be taken forward to assess the MATTE Consequence Level.

Receptor Type	MATTE Threshold (effects below this are considered sub-MATTE)	Credible release scenario and migration pathway		
		H01: 10,000m ³ release of diesel from storage in T1 and T2		
		Drainage infrastructure	Overland flow	In-ground migration
6 - Widespread habitat – non designated water	Contamination of aquatic habitat which prevents fishing or aquaculture or renders it inaccessible to the public.	✓	✓	✘
8 - Groundwater body (non-drinking water source)	1-100ha of groundwater body where the Water Framework Directive (WFD) status has been lowered	✘	N/A	✓
13 - Particular species (Godwit within the estuary)	Loss of 1-10% of animal or 5-50% of plant ground cover (based on national population levels)	✓	✓	✘
15 - Fresh and estuarine water habitats	WFD chemical or ecological status lowered by one class for 2-10km of watercourse or 2-20ha or 10-50% area of estuaries or ponds. Plus interruption of drinking water supplies.	✓	✓	✘

In a full Phase I assessment report justification for the decisions made in the evaluation of MATTE would be included.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

2.7 MATTE Consequence Levels

As the final part of the MATTE definition, the Consequence Level (A to D) of each MATTE is assessed by determining the severity and duration of the harm using Table 1 (severity/harm criteria), Table 2 (duration/recovery criteria) and Table 3 (method and matrix for deriving receptor tolerability for MATTE) in Appendix 4 of the Guidance.

For the purpose of this case study an example of a consequence level assessment for two receptor types is presented below:

Receptor Type	Credible scenarios	Migration pathways	Severity of Harm Category	Duration of Harm Category	Consequence Level
6 - Widespread habitat – non designated water (estuary)	H01: Acute release from a semi-buried diesel tank (up to 10,000m ³) H02: Acute release during receipt of diesel from a vessel (up to 10,000m ³) H04: Release of firewater containing AFFF and entrained hydrocarbons (up to 15,000m ³)	Drainage infrastructure (H01 and H04) Overland flow (H01 and H04) Direct release to surface water (H02)	Severe (2): Contamination of aquatic habitat which prevents fishing or aquaculture or renders it inaccessible to the public.	Medium term (2): greater than 1 year but less than 10 years	Consequence Level A
13 - Particular species (Godwit within the estuary)	H01: Acute release from a semi-buried diesel tank (up to 10,000m ³) H02: Acute release during receipt of diesel from a vessel (up to 10,000m ³) H04: Release of firewater containing AFFF and entrained hydrocarbons (up to 15,000m ³)	Drainage infrastructure (H01 and H04) Overland flow (H01 and H04) Direct release to surface water (H02)	Severe (2): loss of 1 – 10% of animal or 5-50% of ground cover	Very long term (4): >20 years	Consequence Level C

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Receptor Type	Credible scenarios	Migration pathways	Severity of Harm Category	Duration of Harm Category	Consequence Level
	15,000m ³)				

In a full Phase I assessment report, justification would be given for the severity and duration of harm for each MATTE.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

3 Part 2: Establishment Risk Frequencies

Part 2 of the screening process involves aggregating the failure frequencies for each MATTE, per receptor, per year to define the 'total' risk tolerability for each environmental receptor, per year. This number will either lie in the 'Intolerable', 'TifALARP' or 'Broadly Acceptable' tolerability ranges.

The aggregated frequencies are plotted on the matrix below; initially for unmitigated scenarios and then for the mitigated scenarios, where credit is taken for existing preventative and mitigation controls. Unmitigated risk is denoted by 'UnMi', mitigated risk is denoted by 'Mi':

Tolerability Ranges							
	Frequency per establishment <u>per receptor per year</u>						
MATTE Consequence Level	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D - MATTE	Broadly Acceptable		TifALARP		Intolerable		
C - MATTE					Intolerable		
B - MATTE	Broadly Acceptable		TifALARP		Mi		UnMi
A - MATTE					Mi		
Sub MATTE	Tolerability not considered under the CDOIF environmental risk tolerability methodology						

It should be noted that the frequencies should be aggregated per receptor. Some receptors have the potential to be impacted by more MATTE scenarios than others; therefore, for these receptors the overall 'risk' is likely to be higher.

This approach allows the most vulnerable receptors to be identified, along with the highest risk release scenarios and migration pathways.

Details of the control measures being considered, release frequencies and failure rates of individual protection layers would be provided within the full Phase I assessment report, or cross reference made to relevant sections of the Safety Report.

3.1 Failure Frequencies

3.1.1 Unmitigated Failure Frequencies

In many cases the existing Safety Report will have identified frequencies for the causes of a release for each credible release scenario. The unmitigated failure frequencies may be based on generic failure rate data, for example:

- Health & Safety Executive's (HSE's) Failure Rate and Event Data (FRED), see <http://www.hse.gov.uk/landuseplanning/failure-rates.pdf>; and
- The Environment Agency (EA), Scottish Environment Protection Agency (SEPA) and Natural Resources Wales (NRW) 'All Measures Necessary' Guidance.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

3.1.2 Mitigated Failure Frequencies

For the purpose of this case study, examples of control measures which can be taken into account when deriving the mitigated frequencies include (but are not limited to):

- site operational procedures and controls which minimise the likelihood of a release occurring from primary containment e.g.:
 - the high level alarm on the tanks which reduces the likelihood of overfilling; and
 - routine site patrols along the pipeline routes;
- secondary containment which mitigates the impact on environmental receptors from a loss of primary containment e.g.:
 - the earth bund around the storage tank farm preventing overland flow;
- tertiary containment which mitigates the impact on environmental receptors from a loss of secondary containment e.g.:
 - the drainage infrastructure which includes pollution probes and automatic shut-off valves.

A probability of failure of demand (PFD) factor can be applied for each of the control measures. However, it should also be noted that for some release scenarios there may be more than one migration pathway to the same receptor; for example, via the establishment's drainage system and by overland flow. One migration pathway may be afforded a greater level of protection from the available control measures than the other(s). This needs to be taken into account when aggregating the overall mitigated release frequencies per receptor.

3.2 Aggregating Failure Frequencies per Receptor

The following table presents the total unmitigated and mitigated failure frequencies for each of the MATTE level credible release scenarios in the case study.

Unmitigated and Mitigated Failure Frequencies			
Credible release scenario	Failure types covered	Total Unmitigated Failure Frequency per Scenario	Total Mitigated Failure Frequency per Scenario
H01: Diesel storage in T1 and T2; 2 x 10,000m ³ semi-buried tanks – non pressure vessels. Maximum acute release volume: 10,000m ³ from a catastrophic failure	Failure rates for pipework 304.8mm diameter: 4mm diameter, 25mm diameter, 1/3 pipework diameter and guillotine release sizes.	2.76x10⁻⁰¹ years	1.46x10⁻⁰³ years

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Unmitigated and Mitigated Failure Frequencies			
Credible release scenario	Failure types covered	Total Unmitigated Failure Frequency per Scenario	Total Mitigated Failure Frequency per Scenario
Chronic releases from the tank bases can go undetected for some time. 1,000m ³ .	Overfill of storage tank during refuelling operations (based on two semi-buried tanks)		
	Major and minor release frequencies rate for AST > 450m ³ (includes chronic release and catastrophic failure).		
H02: Receipt of diesel by vessel. Receipts of fuel from vessels are pumped to T1 and T2 via on-board vessel pumps and a foreshore pump house. Maximum release volume 10,000m ³ .	Loading arm failure during transfer	6.57x10⁻⁰³ years	3.57x10⁻⁰⁵ years
	Jetty pipeline failure		
	Release from jetty equipment		
	Vessel impact with jetty structure		
H04: Release of fire-water containing aqueous film forming foam (AFFF) and entrained hydrocarbons during operations to combat a major fire. Maximum release volume 15,000m ³ based on current fire water requirement assessments. AFFF in 3% solution in water.	Ignition of releases following loss of containment	1.48x10⁻⁰³ years	7.40x10⁻⁰⁴ years

The following table then presents the total release frequencies for each credible scenario, aggregated for each receptor, per year, and also taking into account the different MATTE consequence levels.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Aggregate Unmitigated and Mitigated Failure Frequencies per Receptor

Receptor Type	H01: Diesel storage in T1 and T2; 2 x 10,000m ³ semi-buried tanks – non pressure vessels. Maximum acute release volume: 10,000m ³ from a catastrophic failure Chronic releases from the tank bases can go undetected for some time. 1,000m ³	H02: Receipt of diesel by vessel. Receipts of fuel from vessels are pumped to T1 and T2 via on-board vessel pumps and a foreshore pump house. Maximum release volume 10,000m ³ .	H04: Release of fire-water containing aqueous film forming foam (AFFF) and entrained hydrocarbons during operations to combat a major fire. Maximum release volume 15,000m ³ , based on current fire water requirement
Unmitigated total failure frequency per scenario	2.76x10 ⁻¹ years	6.57x10 ⁻⁰³ years	1.48x10 ⁻⁰³ years
Mitigated total failure frequency per scenario	1.46x10 ⁻⁰³ years	3.57x10 ⁻⁰⁵ years	7.40x10 ⁻⁰⁴ years
6 – widespread habitat – non designated water (adjacent estuary) Scenarios H01, H02 and H04 result in a Consequence Level A	Aggregate unmitigated failure frequency for the establishment	2.84x10⁻⁰¹ years	
	Aggregate mitigated failure frequency for the establishment	2.24x10⁻⁰³ years	
8 – groundwater body (non-drinking water source) (groundwater within the fractured bedrock) Scenarios (H01, H02 and H04) result in a Consequence Level A	Aggregate unmitigated failure frequency for the establishment	2.77x10⁻⁰¹ years	
	Aggregate mitigated failure	2.20x10⁻⁰³ years	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Aggregate Unmitigated and Mitigated Failure Frequencies per Receptor

Receptor Type	H01: Diesel storage in T1 and T2; 2 x 10,000m ³ semi-buried tanks – non pressure vessels. Maximum acute release volume: 10,000m ³ from a catastrophic failure Chronic releases from the tank bases can go undetected for some time. 1,000m ³	H02: Receipt of diesel by vessel. Receipts of fuel from vessels are pumped to T1 and T2 via on-board vessel pumps and a foreshore pump house. Maximum release volume 10,000m ³ .	H04: Release of fire-water containing aqueous film forming foam (AFFF) and entrained hydrocarbons during operations to combat a major fire. Maximum release volume 15,000m ³ , based on current fire water requirement
Unmitigated total failure frequency per scenario	2.76x10 ⁻¹ years	6.57x10 ⁻⁰³ years	1.48x10 ⁻⁰³ years
Mitigated total failure frequency per scenario	1.46x10 ⁻⁰³ years	3.57x10 ⁻⁰⁵ years	7.40x10 ⁻⁰⁴ years
	frequency for the establishment		
13 – particular species (Godwit within the estuary) Scenarios H01, H02 and H04 are Consequence Level C	Aggregate unmitigated failure frequency for the establishment	2.84x10⁻⁰¹ years	
	Aggregate mitigated failure frequency for the establishment	2.24x10⁻⁰³ years	
15 – fresh and estuarine water habitats (adjacent estuary)	Aggregate unmitigated failure frequency for the	2.84x10⁻⁰¹ years	

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Aggregate Unmitigated and Mitigated Failure Frequencies per Receptor

Receptor Type		H01: Diesel storage in T1 and T2; 2 x 10,000m ³ semi-buried tanks – non pressure vessels. Maximum acute release volume: 10,000m ³ from a catastrophic failure Chronic releases from the tank bases can go undetected for some time. 1,000m ³	H02: Receipt of diesel by vessel. Receipts of fuel from vessels are pumped to T1 and T2 via on-board vessel pumps and a foreshore pump house. Maximum release volume 10,000m ³ .	H04: Release of fire-water containing aqueous film forming foam (AFFF) and entrained hydrocarbons during operations to combat a major fire. Maximum release volume 15,000m ³ , based on current fire water requirement
Unmitigated total failure frequency per scenario		2.76x10 ⁻¹ years	6.57x10 ⁻⁰³ years	1.48x10 ⁻⁰³ years
Mitigated total failure frequency per scenario		1.46x10 ⁻⁰³ years	3.57x10 ⁻⁰⁵ years	7.40x10 ⁻⁰⁴ years
Scenarios H01, H02 and H04 result in a Consequence Level A	establishment			
	Aggregate mitigated failure frequency for the establishment	2.24x10⁻⁰³ years		
15 – fresh and estuarine water habitats (adjacent estuary) Impact from the jetty and fire water releases (H02 and H04) can also impact at Consequence Level B	Aggregate unmitigated failure frequency for the establishment	8.05x10⁻⁰³ years		
	Aggregate mitigated failure frequency for the establishment	7.76x10⁻⁰⁴ years		

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

3.3 Worked Example of Tolerability Matrices

Examples of the resulting unmitigated and mitigated risk tolerability matrices for selected receptor types are presented below. Unmitigated risk is denoted by 'UnMi', mitigated risk is denoted by 'Mi':

Receptor Type 6 – widespread habitat – non designated water (adjacent estuary)							
	Frequency per establishment per receptor per year						
MATTE Consequence Level	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D – MATTE	Broadly Acceptable			TifALARP		Intolerable	
C - MATTE				TifALARP		Intolerable	
B - MATTE	Broadly Acceptable			TifALARP		Intolerable	
A - MATTE	Broadly Acceptable			TifALARP		Mi	UnMi
Sub MATTE	Tolerability not considered under the CDOIF environmental risk tolerability methodology						

Receptor Type 8 – groundwater body non drinking water source (groundwater within the fractured bedrock)							
	Frequency per establishment per receptor per year						
MATTE Consequence Level	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D – MATTE	Broadly Acceptable			TifALARP		Intolerable	
C - MATTE				TifALARP		Intolerable	
B - MATTE	Broadly Acceptable			TifALARP		Intolerable	
A - MATTE	Broadly Acceptable			TifALARP		Mi	UnMi
Sub MATTE	Tolerability not considered under the CDOIF environmental risk tolerability methodology						

Receptor Type 13 - particular species (Godwit within the estuary)							
	Frequency per establishment per receptor per year						
MATTE Consequence Level	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D – MATTE	Broadly Acceptable			TifALARP		Intolerable	
C - MATTE				TifALARP		Mi	UnMi
B - MATTE	Broadly Acceptable			TifALARP		Intolerable	
A - MATTE	Broadly Acceptable			TifALARP		Intolerable	
Sub MATTE	Tolerability not considered under the CDOIF environmental risk tolerability methodology						

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits

Receptor Type 15 – fresh and estuarine water habitats (adjacent estuary)							
	Frequency per establishment per receptor per year						
MATTE Consequence Level	$10^{-8} - 10^{-7}$	$10^{-7} - 10^{-6}$	$10^{-6} - 10^{-5}$	$10^{-5} - 10^{-4}$	$10^{-4} - 10^{-3}$	$10^{-3} - 10^{-2}$	$>10^{-2}$
D – MATTE	Broadly Acceptable		TifALARP		Intolerable		
C - MATTE			Intolerable				
B - MATTE	Broadly Acceptable		TifALARP		Mi	UnMi	UnMi
A - MATTE			TifALARP		Mi	UnMi	
Sub MATTE	Tolerability not considered under the CDOIF environmental risk tolerability methodology						

In a full Phase I assessment the unmitigated and mitigated risk tolerability would be defined for each relevant environmental receptor.

3.4 Outcome of Phase I Screening

From these matrices, it can be seen that all of the unmitigated risks to all receptors are in the ‘intolerable’ range. When the protection provided by the preventative and mitigation controls are accounted for, the mitigated risk to most receptors is reduced to within the TifALARP range. However, one environmental receptor, the Godwit living in the estuary (receptor type 13 – particular species), remains in the ‘intolerable’ range. This is primarily driven by the higher consequence level (C) of a MATTE harming this receptor.

The outcome of this screening level assessment is that the Godwit residing in the estuary are one of the most vulnerable receptors in the event of an acute release, primarily from scenarios H01 (release from a semi-buried tank), H02 (acute release of diesel during vessel unloading at the jetty) and H04 (release of fire water containing foam and entrained hydrocarbons). The pathways by which the Godwit population could be impacted are migration within the drainage network and overland flow (scenarios H01 and H04) and by direct release into surface water (scenario H04).

4 Phase 2 Assessment

The outcome of this case study is that the risk to the Godwit population in the estuary, taking into account mitigation, is in the 'intolerable' range. At this establishment two options would be considered:

- Option 1: Provide additional mitigation to reduce the risk to an acceptable level; or
- Option 2: Undertake more detailed assessment of the risk to this receptor.

In this instance the more detailed assessments could include obtaining additional data on the population and residency of the species in the vicinity of the establishment, natural variability in the population baseline, the ecotoxicity and fate of the substances released to the habitat and/or further assessment of the natural recovery of the species following a MATTE.

The outcome of the Phase 2 assessments may also support cost benefit analysis in the demonstration of ALARP.

CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Environmental Risk Tolerability for COMAH
Establishments

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members this guideline on environmental risk tolerability for COMAH establishments.

The intent of this document is to provide a reference for those organisations completing environmental risk assessments.

This guidance (or equivalent) should be used from the date of publication to carry out environmental risk assessments required by COMAH. The document will remain open for comment and revision until end 2014 to allow industry to use the process and provide feedback on any significant issues that may arise from its implementation.

It is not the intention of this guidance to replace the existing DETR 1999 publication 'Guidance on the Interpretation of Major Accident to the Environment for the Purposes of the COMAH Regulations', but provide a framework and screening methodology by which regulators and duty holders can apply it.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to environmental risk assessment, and determining risk tolerability.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Environmental Risk Tolerability for COMAH sites".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

This guidance is not intended to be an authoritative interpretation of the law; however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach. Reference should also be made to the CA's 'All Measures Necessary Guidance' to local inspection teams.

It should be understood however that this document does not explore all possible options for determining environmental risk tolerability or environmental risk assessment, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

FOREWORD	2
CONTENTS	3
1. EXECUTIVE SUMMARY	5
2. SCOPE	6
2.1 Competency requirements.....	6
2.2 Proportionality in Risk Assessment.....	6
2.3 Using this guidance.....	7
3. DEFINITION OF THE TYPES OF ENVIRONMENTAL HARM	10
3.1 Environmental Receptors.....	10
3.2 MATTE Thresholds	11
3.2.1 Designated area.....	11
3.2.2 Widespread habitat (land/Water)	12
3.2.3 Groundwater	13
3.2.4 Soil or Sediment (Land/Water).....	15
3.2.5 Built environment (Land, man-made).....	16
3.2.6 Various receptors, as defined (Water)	17
3.2.7 Particular species (Land, Water, Air)	17
3.2.8 Marine (Water).....	17
3.2.9 Freshwater and estuarine habitats (Water).....	18
4. RISK CRITERIA AND EVALUATING RISKS.....	20
4.1 Assessing the risk of potential harm	20
4.1.1 Terms used in risk assessment	22
4.2 MATTE potential matrix	23
4.2.1 Grouping and compartmentalisation	23
4.2.2 Tables to assess MATTE potential	24
4.3 Aggregating risk and risk frequencies.....	25
4.3.1 Aggregating risk option 1 - Summation of risks	25
4.3.2 Aggregating risk option 2 – Developing scenario based risk criteria	25
4.3.3 Impacts from adjacent sites	26
4.3.4 Determining risk frequencies	27
4.3.5 Determining risk reduction of prevention and mitigation layers	28
5. COST BENEFIT ANALYSIS	29
5.1 Disproportion Factor (DF)	29

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

5.2	Benefits	29
5.3	Costs	29
5.4	Discounting Rates.....	29
5.5	Evaluation of Environmental Remediation	29
6.	COMPLETING THE RISK ASSESSMENT	31
6.1	Part 1 - MATTE definition and thresholds	31
6.1.1	Identifying the major accident scenarios.....	32
6.1.2	Determining the level of severity.....	32
6.1.3	Assigning a duration/recovery category.....	32
6.1.4	Determining tolerability boundaries.....	33
6.2	Part 2 calculating the establishment risk frequencies	34
6.2.1	Aggregating risk - Examples	34
6.2.1.1	Single substance stored in a single tank.....	36
6.2.1.2	Tank farm or group of tanks containing similar substances.....	37
6.2.1.3	Groups (e.g. tank farms) with dissimilar substances/incident consequences.....	38
6.2.1.4	Comparison with tolerability criteria	39
6.2.1.5	Interdependent scenarios	41
7.	ABBREVIATIONS	42
	REVISION HISTORY.....	43
	APPENDIX 1 - KEY GUIDANCE	44
	APPENDIX 2 – DETR 1999 TABLE REFERENCES.....	47
	APPENDIX 3 – INFORMATION SOURCES.....	57
	APPENDIX 4 – MATTE TOLERABILITY TABLES	67
	APPENDIX 5 – TABLES TO ASSESS MATTE POTENTIAL	78

1. Executive Summary

COMAH requires all Top Tier site operators to submit site safety reports to the Competent Authority (CA) that demonstrate that the environmental risk for the whole COMAH establishment has been reduced to a tolerable level. Lower Tier operators must prepare risk assessments making a demonstration proportionate and appropriate to the environmental risk, and whilst these are not required to be submitted to the CA these need to be available during CA inspection.

The purpose of this guidance is to provide a common methodology by which this risk assessment can be carried out. The methodology can be used by both duty holders and the Competent Authority when preparing or reviewing risk assessments.

The guidance will also help identify scenarios and areas of installations which are subject to COMAH vs. those that might be subject to other environmental legislation (e.g. EPR, PPC etc.). Where measures (physical or procedural) are necessary for prevention and mitigation of MATTE, then COMAH will be used to regulate those measures; conversely for potential environmental impacts below MATTE thresholds COMAH will not be used but other environmental legislation might apply (e.g. EPR, PPC etc.). If there is a potential for a Major Accident to people, but no MATTE potential then COMAH will apply to the measures, which might require measures related to environmental protection (e.g. those required by COMAH regarding emergency preparedness). In these circumstances HSE will carry out regulation of such activities under COMAH, whilst the Agencies will have limited involvement under COMAH (e.g. as their role as statutory consultees to emergency planning) and the Agencies will carry out regulation as required by other environmental legislation.

It is not the intention of this guidance to provide a detailed assessment process, but to provide a screening mechanism by which risks to environmental receptors can be reviewed. Depending on the result of this screening, further more detailed analysis may be required.

In summary, this publication provides:

- A clear definition of the types of harm that should be considered in an environmental risk assessment, and how the harm should be characterised for the assessment
- A definition of the risk criteria to be used in assessing the tolerability of the environmental risk from an establishment and, where appropriate, individual scenarios
- Guidance on how the risks may be evaluated
- Guidance on how to include the cost of environmental harm in a COMAH cost benefit analysis

2. Scope

This document provides a screening methodology to help Duty Holders and the Competent Authority in determining environmental risk tolerability from an establishment.

2.1 Competency requirements

When completing an environmental risk assessment there is a need to ensure that relevant competent resources are used throughout the process. In the context of this guidance, it is likely that environmental specialists will be involved with the identification of potential Major Accidents to the Environment (MATTE's), and in determining the thresholds that should apply to those receptors around the site. Similarly, it is likely that the skills of process safety specialists will be needed to evaluate the un-mitigated risk frequencies to these receptors, and to determine the mitigation and prevention measures already in place to reduce the risk.

In some circumstances it might be necessary to consult experts outside of the operator's organisation. For example, where a designated site could be impacted then discussions with the relevant conservation bodies might be required to ensure the assessment includes current information on the designated site status and vulnerability. Similarly, the Agencies (NRW, SEPA and EA) hold much information on water resources.

Caution should be taken when completing the screening process to ensure that over-simplification does not take place – there will often be a need for expert opinion and professional judgment.

2.2 Proportionality in Risk Assessment

For COMAH, environmental risk can be assessed within the established “As low as reasonably practicable” (ALARP) framework and evaluated to be either Intolerable, Tolerable if ALARP (TifALARP) or Broadly Acceptable. These terms have broadly the same meaning as used in relation to risks to people. Further guidance on their meaning and application can be found in the CA guidance on All Measures Necessary for environmental risk and other HSE ALARP guidance (see Appendix 1).

The level of environmental risk can be used to guide the type and depth of assessment that would be expected by the CA. For screening purposes, a qualitative or semi-quantitative approach (using this guidance), combined with conservative assumptions is appropriate.

There are no specific rules regarding the depth of further analysis, but generally, if risk is in the lower half of the TifALARP zone, then the semi-quantitative methods described in this document should be appropriate. If risk falls in the upper half of the TifALARP or in the intolerable zone then a greater depth of demonstration may be necessary to demonstrate adequate risk control. The level of risk assessment will also be influenced by data availability. If data is not available then a qualitative or semi-quantitative approach may need to be adopted, but as with screening this should be combined with conservative assumptions.

Further discussion of types and proportionality of assessment can be found in the references in Appendix 1, in particular paragraph 292 of HSG (190) and section 2.5 of Green Leaves III.

2.3 Using this guidance

As discussed above, this guideline provides a screening methodology for carrying out a COMAH Environmental Risk Assessment (ERA). It does not provide detailed guidance on all aspects of ERA and for this reference should be made to Appendix 1, which signposts other available key guidance.

The process of ERA involves:

- Identification and evaluation of source – pathway – receptor linkages for different credible accident scenarios. This includes demonstrating an understanding of the hazards of the establishment, and the sensitivities of the environment.
- Identification of tolerability criteria for relevant receptors, dependent on the receptor type and potential level of consequence to the receptor.
- Evaluation of risks to the receptor, through examination of accident scenarios (their consequences and frequency) and comparing this to the tolerability criteria derived above.

Following completion of the ERA, determine what (if any) additional measures are required to demonstrate that the risk has been reduced to ALARP.

This guidance provides further information on specific elements of this process:

- Section 3 – How to quantify consequence to different receptor types, in terms of extent, severity and duration of harm. In particular to identify accident scenarios where the level of consequence exceeds thresholds for MATTE.
- Section 4 – Evaluating risk and making judgements against tolerability criteria. This process includes screening out of further assessment any scenarios where it can be demonstrated that the nature and quantity of material present do not have MATTE potential. Sub-sections include discussion of domino sites, failure rate data and the credit that can be claimed for mitigation.
- Section 5 – How environmental matters can be dealt with in CBA, if this is required
- Section 6 – An outline of the assessment process, by reference to the concepts introduced in previous sections, with examples.
- The appendixes provide links to a wealth of important information, much of which will be necessary to support an assessment of environmental risk. However, above all, Appendix 4 is most important since it provides the agreed tolerability thresholds for various differing consequence scales of MATTE.

Figure 1 below depicts how aspects of this approach are covered in the relevant sections within this guidance.

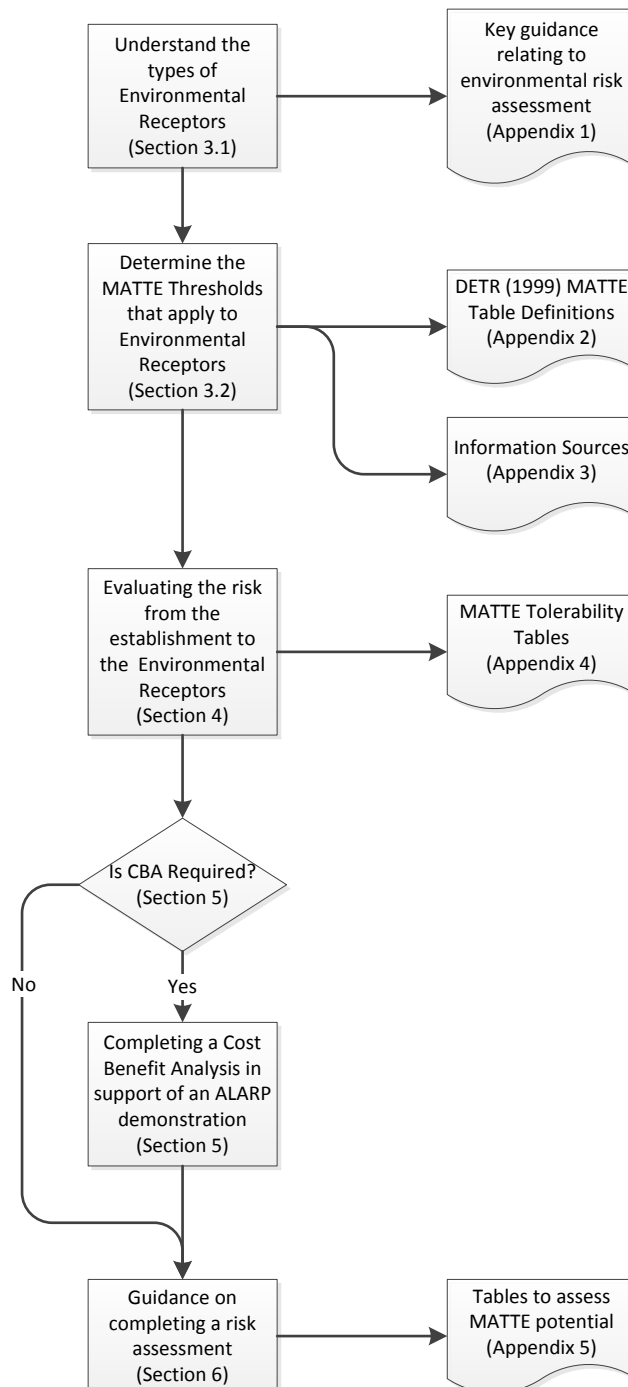


Figure 1 – Using this guidance

When preparing environmental risk assessments, operators of both Top and Lower Tier sites can usefully refer to Section 13 of the Safety Report Assessment Manual. This provides the structured approach the CA uses to assess and inspect environmental risk assessment for the purpose of demonstrating All Measures Necessary. It thus provides

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

a strong indication of CA expectations regarding risk based demonstrations and how they should be presented.

3. Definition of the types of environmental harm

The definition of major accident in the COMAH regulations requires serious danger (to people or the environment). Serious danger to the environment is considered to occur where there is potential for a Major Accident to the Environment (MATTE). A MATTE would be taken to require harm or damage to the environment above the described thresholds (refer to section 3.2 for extent, severity and duration thresholds).

In preparing this guidance, the following key technical documents have been referenced:

- DETR 1999, Guidance on the interpretation of Major Accident to the Environment for the purposes of COMAH regulations
- EA, 2004, Guidance identifying COMAH Major Accidents to the Environment (MATTEs)
- EA, 2010, Incidents and their classification: the Common Incident Classification Scheme (CICS)

Reference should also be made to Appendix 1, Key Guidance.

Appendix 2 provides a reference to the relevant tables from the DETR 1999 guidance on the interpretation of Major Accident to the Environment for the purposes of COMAH regulations.

3.1 Environmental Receptors

The types of environmental receptors that should be considered are as follows:

- Terrestrial habitats
- Freshwater habitats
- Marine habitats
- Groundwater bodies

When reviewing habitats the following points should be considered:

- Small areas within the larger overall area of a receptor may be significant, depending on the flora / fauna that inhabits them, reference should be made to the DETR 1999 guidance table 10 and Appendix 4 for further details.
- Any review of receptors should include migratory species which could be transient in the habitat
- Individual species (where appropriate) should be considered in the assessment, regardless of the pathway to the receptor.

Links to sources of information on environmental receptors are provided for each receptor in Appendix 3.

3.2 MATTE Thresholds

The following thresholds should be used when determining the potential for a MATTE to each of the receptors described in section 3.1.

These thresholds have been developed with regard to the Major Accident EC reporting thresholds in the Seveso Directive (Sch. 7 of the COMAH regulations) and the DETR 1999 Guidance on MATTE.

Thresholds are presented in two dimensions

- (i) Extent and Severity; and
- (ii) Duration of harm

The thresholds for both dimensions must be exceeded for the scenario to be considered to be a potential MATTE.

The thresholds referring to extent and severity are presented below and should be read in conjunction with Table 1 of Appendix 4. To avoid disproportionate application of percentage criteria in the MATTE thresholds on small receptors, for small sites, the percentage criteria will not reduce the threshold to lower than **half the area/distance criteria**.

With respect to Duration of Harm, impacts with short term natural recovery (other than those to people) would not be considered MATTE – Appendix 4 table 2 provides natural recovery times for differing receptors that would or would not be considered MATTE.

3.2.1 Designated area

NOTE: The DETR 1999 guidance refers to 'Designated Land'. The CDOIF working group have agreed to refer to 'designated Area' as this also encompasses water.

Nationally important: SSSI and National Nature Reserves (NNR) [Refer to DETR 1999 table 1]:

The level of harm that would constitute a MATTE is defined as follows:

- a) Greater than 0.5 ha or 10% of the area of the site adversely affected (whichever is the lesser, subject to a lower limit of 0.25ha); or,
- b) Greater than 10% of a designated linear feature of the site adversely affected; or,
- c) Greater than 10% of a particular habitat or population of individual species adversely affected (Population refers to the known or estimated population at the site, and individual species named in the designation, not the national population. For other species refer to table 10 of the DETR guidance)

Internationally important: SACs, SPAs & Ramsar sites [Refer to DETR 1999 table 2]

The level of harm that would constitute a MATTE is defined as follows:

- a) Greater than 0.5 ha or 5% of the area of the site adversely affected (whichever is the lesser, subject to a lower limit of 0.25ha); or,
- b) Greater than 5% of a designated linear feature of the site adversely affected; or,
- c) Greater than 5% of a particular habitat or population of individual species adversely affected (Population refers to the known or estimated population at the site not the national population and individual species named in the designation, for other species refer to table 10 of the DETR guidance)

Other designated land (ESA's, AONB's LNRs, NSA's etc [Refer to DETR 1999 table 3])

The level of harm that would constitute a MATTE is defined as follows:

- a) Greater than 10% or 10 ha seriously damaged, whichever is the lesser (seriously damaged is defined in 'EA, 2004, Guidance identifying COMAH Major Accidents to the Environment (MATTEs)', table 3

Scarce habitat [Refer to DETR 1999 table 4]

The level of harm that would constitute a MATTE is defined as follows:

- a) Damage to 10% of the area of the habitat or 2 ha, whichever is the lesser. Refer to DETR 1999, table 4 for a definition of 'scarce habitats'. Note that 10% refers to the site area.

NOTE: Definition of 'Adversely Affected'

Means that the part of the site affected loses at least one of its reasons for designation, or favourable conservation status, and would not naturally recover (i.e. regain its designated status) within 3 years for terrestrial habitats and a single season for marine/freshwater.

Marine implies everything below the high water mark, for example mud flats, estuary.

Due consideration should be given to features such as estuaries and sea lochs. Further information on the definition of 'Adversely affected' can be found in the DETR 1999 guidance, tables 1 – 4.

3.2.2 Widespread habitat (land/Water)

Non-designated land [Refer to DETR 1999 table 5]

The level of harm that would constitute a MATTE is defined as follows:

- a) Contamination of 10 ha or more of land which, for two growing seasons or more, prevents growing of crops or the grazing of domestic animals or renders the area inaccessible to the public because of possible skin contact with dangerous substances;

NB. The health effect above covers the impact on amenity

or,

- b) Contamination of 10 ha or more of vacant land for three years or more. (Refer to Appendix 3, Table 1)

NOTE: Definition of 'Non-Designated Land'

Land means all non-designated land, not just agricultural land.

Non-designated water [Refer to DETR 1999 Table 5]

The level of harm that would constitute a MATTE is defined as follows:

- a) Contamination of aquatic habitat (freshwater or marine) which prevents fishing or aquaculture or renders it inaccessible to the public

Where there is no potential to contaminate an aquatic habitat, the non-designated water will not have MATTE potential, and should therefore not be considered as part of the screening process.

3.2.3 Groundwater

[Refer to DETR 1999 table 6]

Because of the diverse nature of groundwater, it is not possible to attribute a single threshold to determine whether a MATTE has occurred. The following definition provides the basis against which a MATTE to groundwater can be determined:

1. Pollution could happen to any groundwater (as defined by the Water Framework Directive); however, any pollution to groundwater is not necessarily a MATTE. It is necessary to determine whether the groundwater is acting as a pathway, or is itself a receptor.
2. The EC reporting criteria for groundwater is 1ha or more of significant damage to an aquifer or underground water. CDOIF proposes that damage is only considered to be significant if the groundwater in the aquifer meets the definition of a groundwater body (Water Framework Directive). Groundwater bodies are therefore environmental receptors. Pollution of other groundwater (falling outside of the groundwater body definition) would not be considered a MATTE (unless the groundwater acted as a pollutant pathway to a separate receptor).
3. Groundwater bodies, in accordance with the Water Framework Directive and associated guidance, are those productive ground-waters which are used (or could be used in the future) as sources of public or private drinking water (minimum production of 10m³ per day), or which support ecosystems or recharge surface waters. Moreover, the EA Groundwater protection: Principles and practice (GP3) (2012) states that: "All groundwater bodies in England and Wales have been designated Drinking Water Protection Areas." Further detail on assessing groundwater is available on the Agencies' websites (for England, GP3 in particular).

4. For the purpose of application of this guidance, CDOIF has developed 3 categories of groundwater (as described below). Consequence thresholds have been assigned based on the relative value of these 3 categories (note the third category of groundwater, "Other groundwater outside of groundwater bodies" is of least value and impact here would be sub-MATTE with this category of groundwater being a potential pathway only.)
5. For screening purposes, Groundwater bodies can be identified by reference to aquifer maps (see Appendix 3). In accordance with Seveso reporting thresholds, the area threshold strictly relates to the aquifer (rock type) and not the area of groundwater within it. In England and Wales, all Principle and Secondary aquifers (coloured areas on mapping) are groundwater bodies, whilst unproductive strata (un-coloured areas) are not groundwater bodies. Scotland also has an equivalent aquifer map.
6. The resolution of mapping is such that at specific locations, the groundwater in an aquifer that is depicted on the map at that location might not actually meet the formal definitions for groundwater body, i.e. detailed assessment of local groundwater might show the groundwater is not a groundwater body and thus not a receptor for the purposes of MATTEs. This circumstance is expected to be exceptional and the level of demonstration would be resource intensive and beyond the level of work envisaged for screening.

This guidance sets out a MATTE definition, based on different areas/values dependent on the type of groundwater.

Groundwater body – Source of Public or Private Drinking Water

The level of harm that would constitute a MATTE is defined as follows:

- a) For England and Wales only, 1 ha or more of an SPZ where public drinking water standards are breached; or,
- b) Interruption of public or private drinking water supplied from a ground or surface water source, where: (persons affected x duration in hours {at least two hours}) > 1,000

Groundwater body – non Drinking Water Source

The level of harm that would constitute a MATTE is defined as follows:

- a) 1 ha or more of a groundwater body where the Water Framework Directive (WFD) status has been lowered

Other Groundwater (outside of groundwater bodies)

Not applicable. Where the groundwater does not meet the definition of a groundwater body it is considered as a *pathway* to another receptor, and assessment should be against the criteria defined for that receptor (for example marine, fresh or estuarine water habitats)

3.2.4 Soil or Sediment (Land/Water)

[Refer to DETR 1999 Table 7]

For sediment, the DETR guidance refers to a change in overlying water quality - thus sediment should be considered a pathway and the MATTE threshold to consider is the one for the relevant overlying water or particular species.

For Soil, the level of harm that would constitute a MATTE is defined as follows:

- a) Contamination of 10 ha or more of land which, for two growing seasons or more, prevents growing of crops or the grazing of domestic animals or renders the area inaccessible to the public because of possible skin contact with dangerous substances;

Note The health effect above covers the impact on amenity

or,

- b) Contamination of 10 ha or more of land by substances, preparations, organisms or micro-organisms that results in a significant risk of adverse effects on human health.

Note This definition is taken from DEFRA publication "The Environmental Damage (Prevention and Remediation) Regulations 2009 Guidance for England and Wales" and this also covers the impact on amenity.

NOTE: Land that is already contaminated

Refer to figure 2 below.

Where soil is already contaminated, a site-specific analysis of the potential impact of a MATTE scenario may be required as this could have the potential to cause additional contamination or suspend or reverse any existing recovery.

When completing this analysis, the following factors should be considered;

- The pollutant from the MATTE scenario may not have the same chemical nature/characteristics as any pre-existing pollutants, which may aggravate the current contamination effects (e.g. solubilisation).
- The pollutant from the MATTE scenario may suspend or reverse any existing recovery (Reference: Environmental Damage Regulations).

In concluding the analysis;

- If the potential MATTE scenario could exceed the MATTE thresholds in the absence of any existing contamination, the receptor would be deemed as having MATTE potential.
- If the potential MATTE scenario does not alter the existing contamination management (i.e. the existing pollution management system would not need to

be updated following further pollution of the soil or sediment), then credit can be claimed in the risk assessment that the current remedial approach reduces the risk to ALARP.

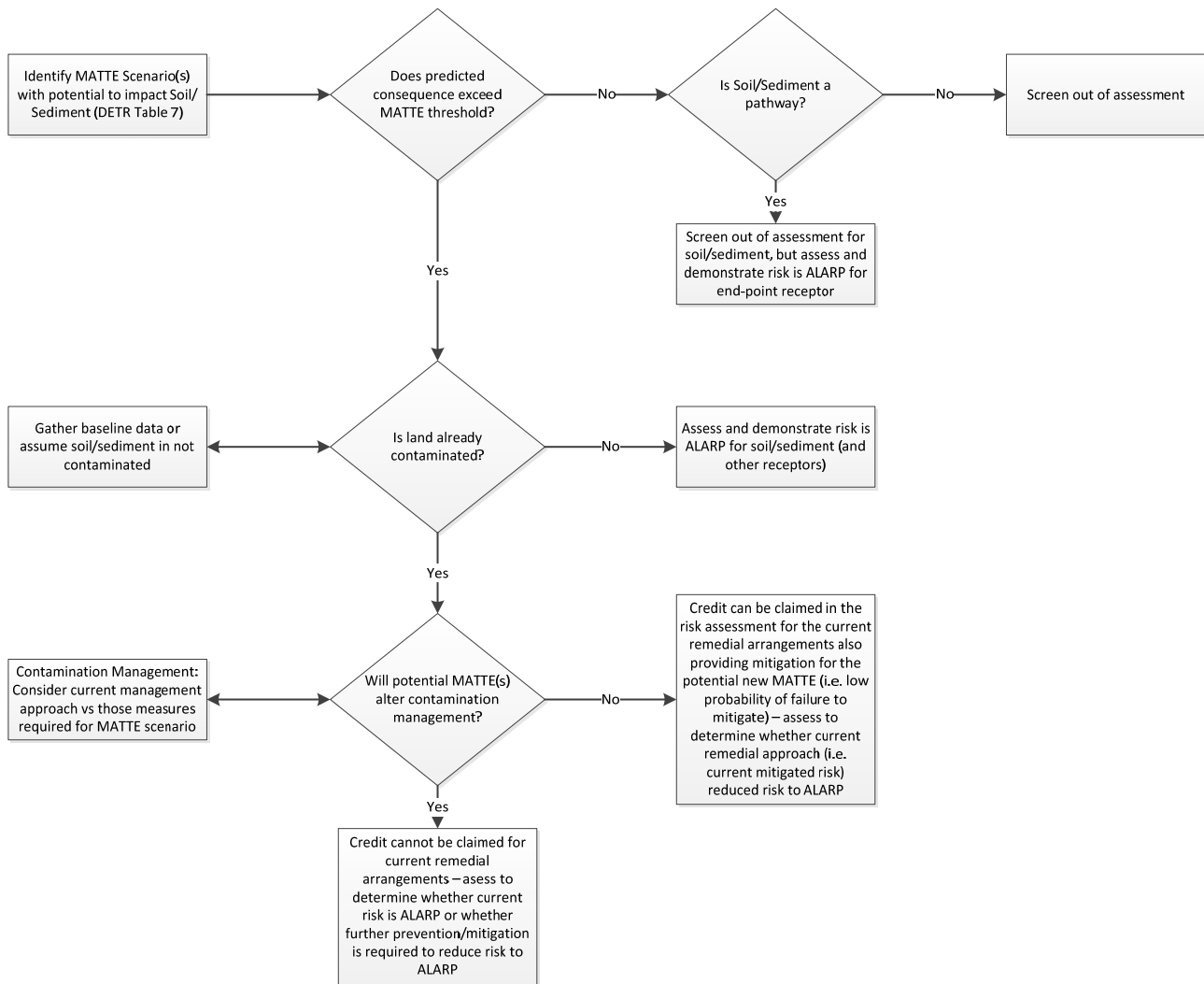


Figure 2 – Assessing contaminated land

3.2.5 Built environment (Land, man-made)

[Refer to DETR 1999 Table 8]

The level of harm that would constitute a MATTE is defined as follows:

- a) Damage to the built environment (e.g. Grade 1/Category A listed buildings, scheduled ancient monuments, conservation areas) such that its designation of importance is withdrawn.

For other built heritage types (e.g. Grade 2 listed buildings), the MATTE definitions for widespread habitats (land, water) apply, refer to section 3.2.2.

3.2.6 Various receptors, as defined (Water)

[Refer to DETR 1999 Table 9]

Not applicable, the definition (based on standards applicable to continuous emissions which fall under other EU legislation) is not used to identify and assess a MATTE.

3.2.7 Particular species (Land, Water, Air)

[Refer to DETR 1999 Table 10]

The level of harm that would constitute a MATTE is defined as follows:

- a) 1% or more of the population; or,
- b) 5% or more of the plant ground cover

Note: the 1% and 5% above refer to national populations of England, Wales or Scotland. Note that for particular high value or special protection species, consult the relevant conservation organisation to determine the appropriate threshold.

3.2.8 Marine (Water)

[Refer to DETR 1999 Table 11]

The level of harm that would constitute a MATTE is defined as follows:

- a) 2 ha or more of contamination to the littoral or sub-littoral zone; or,
- b) 100 ha or more of open sea benthic community; or,
- c) 100 or more dead sea birds (500 or more gulls); or,
- d) 5 or more dead/significantly impaired sea mammals

Note: Further definition of these areas is defined below and in Figure 3.

- Supralittoral: area just above high water mark, only submerged during storms; otherwise ocean spray
- Benthic: benthic zone is the ecological region at the lowest level of a body of water such as an ocean or a lake, including the sediment surface and some sub-surface layers
- Littoral: intertidal zone between low and high water marks (e.g. from the Mean High Water Springs to the Mean Low Water Springs on the OS map)

- Sublittoral: subtidal zone below low water mark (e.g. from the Mean Low Water Springs on the OS map), permanently submerged; extends down to the continental shelf break (~200 m)

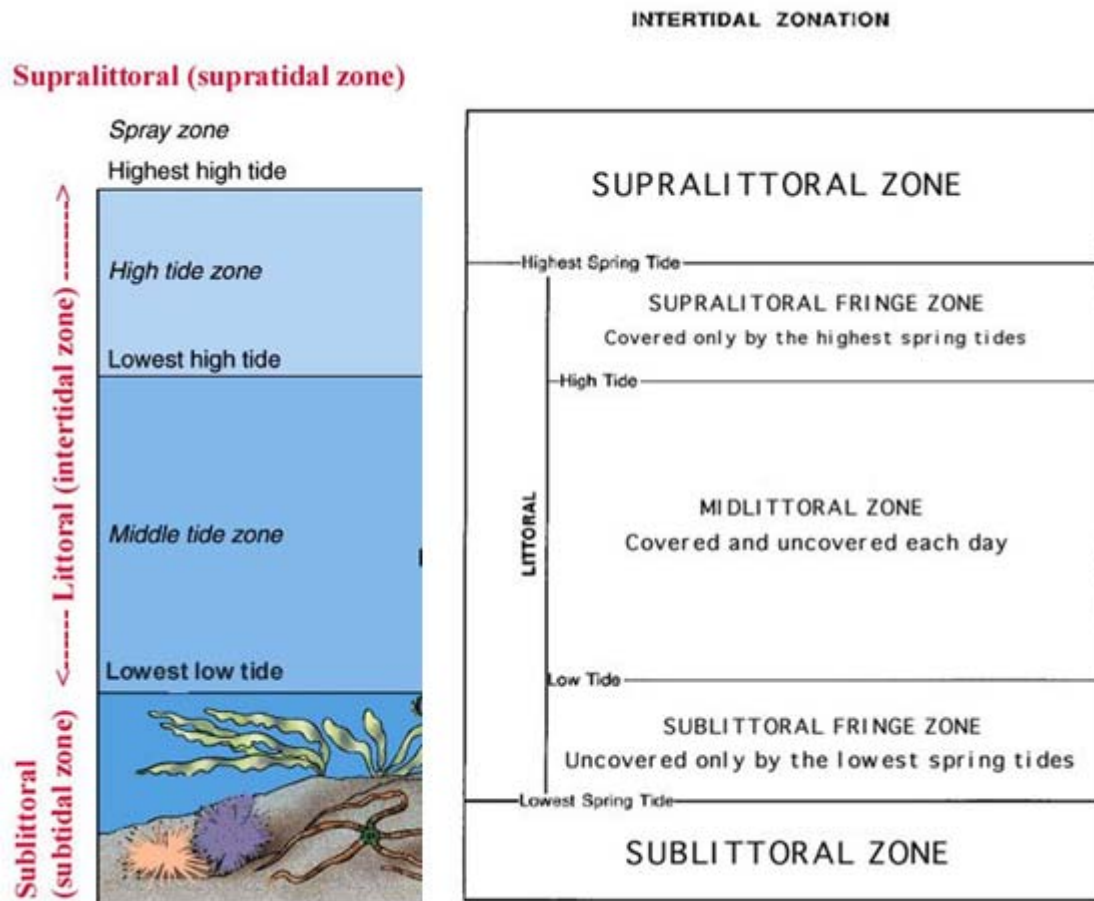


Figure 3 – Marine (Water) zones

3.2.9 Freshwater and estuarine habitats (Water)

[Refer to DETR 1999 Table 12]

The level of harm that would constitute a MATTE is defined as follows:

- a) The chemical or ecological status given by the Water Framework Directive (WFD) has been lowered by one class for more than 2 km of a watercourse; or,
- b) 10% or greater of the area (for estuaries and ponds, reservoirs and lakes); or,
- c) 2 ha or more of the area for estuaries or ponds, reservoirs and lakes, or
- d) Interruption of public or private drinking water supply, where: (persons affected x duration in hours {at least two hours}) > 1,000

Note (criteria a): In DETR guidance, the minimum length of watercourse for MATTE is stated as 10km or 10% of the length (whichever is lesser). In practice, for a large number of watercourses the 10% threshold will dominate, and for many a very short distance would be derived. To avoid very short distances (<2 km, where a watercourse is <20km), CDOIF have agreed the minimum length of watercourse where serious harm could occur is taken here as a fixed value of 2km. This aligns to the EA Common Incident Classification System (CICS) category 1.

Note (criteria d): interruption of public or private drinking supplies is included here to take account of where abstraction points exist in rivers, reservoirs and lakes. Risk thresholds based on potential severity and duration are the same as for interruption of groundwater drinking water supplies (Refer to Appendix 4, MATTE Tolerability Tables, Table 1 row 7).

4. Risk criteria and Evaluating Risks

4.1 Assessing the risk of potential harm

Following the identification of possible environmental receptors around a site, it is necessary to evaluate whether the substance stored on site (or other substance which could be present, such as firewater or reaction by-products) has the potential to cause a MATTE to those receptors. Where this potential could be realised, a risk assessment is necessary to determine if any further prevention or mitigation (or both) techniques are required to reduce the risk to Broadly Acceptable or As Low as Reasonably Practicable (ALARP). The depth of assessment required is discussed in section 2.2.

To complete this assessment, it is necessary to understand the following:

- For each receptor
 - Is there a potential for a MATTE based on the quantities and types of substance stored on site? (Note: include substances that might credibly be produced/introduced in an emergency, such as firewater). This screening step can also be used to rule out from further assessment areas of larger sites where there is no MATTE potential if they will have no involvement in other areas that do have MATTE potential. A site plan may be a useful tool to highlight those areas which have or do not have MATTE potential.
- If there is potential
 - Determine unmitigated consequences from credible accident scenarios and use this to establish the tolerability thresholds per receptor per establishment per year (this is from the Appendix 4 risk matrix)
 - Determine the unmitigated aggregated risk to the receptor from all credible scenarios (i.e. risk with no mitigation measures in place)
 - Determine the mitigated risk (with existing measures in place) from all credible scenarios
 - Determine if further measures are required to reduce the risk to Broadly Acceptable or TifALARP (If mitigated risk remains in TifALARP then the CA will require an ALARP justification to demonstrate why further risk reduction is not reasonably practicable).

The methodology for assessing risk within this guidance begins with determining the *unmitigated* consequence (see definitions below figure 4). The unmitigated consequence could be sub-MATTE (enabling screening out from further assessment) or MATTE level A-D. Each MATTE level A-D has associated tolerability thresholds - the greater the consequence the lower the tolerable frequencies for a MATTE (Appendix 4).

The tolerability thresholds are then compared to the unmitigated risk to the receptor from the establishment. This approach may well indicate an intolerable risk from the outset. However once the total unmitigated risk has been calculated, the process then requires the analysis of mitigated risk by inclusion of all existing mitigation layers – this includes such elements as good design practices, inspection and maintenance, secondary and tertiary containment and emergency response procedures. It is important to recognise

the risk gap between unmitigated and mitigated risk since this is an evaluation of the amount of risk reduction provided by existing mitigatory measures and will illustrate the importance of maintaining these safety critical measures.

An overview of the process is given in Figure 4.

Note that the risk assessment process should consider only credible scenarios.

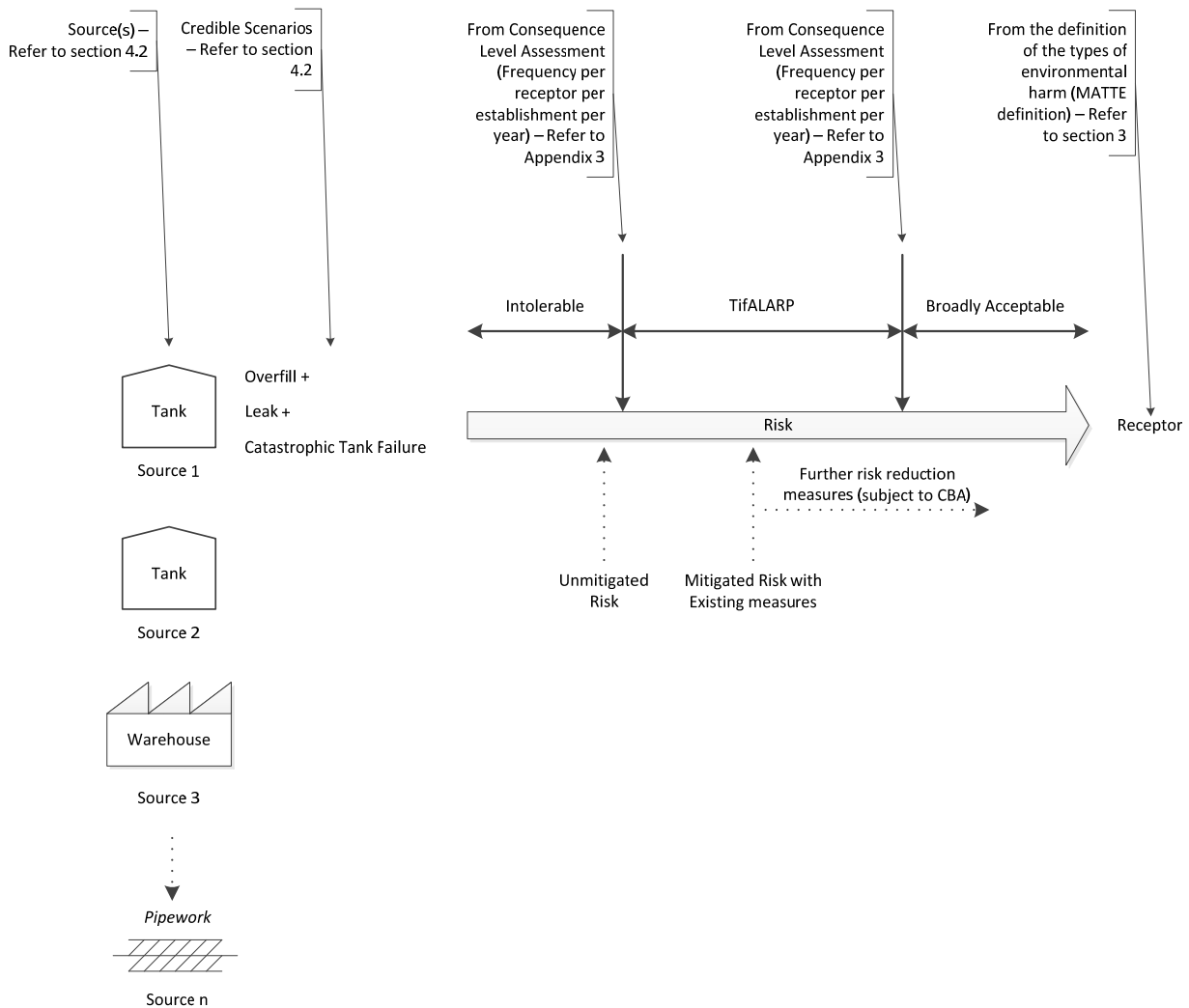


Figure 4 – Overview of the risk assessment process

4.1.1 Terms used in risk assessment

Sources

The sources of pollution which could give rise to a MATTE, (for example tanks, pipework, warehousing, process units, reactors, etc.) refer to section 4.2 'MATTE potential matrix'. Note that pipelines outside of the site boundary are not covered by COMAH when covered by the Pipeline Safety Regulations, and should therefore be excluded from this analysis.

Credible scenarios

The scenarios under which a source could credibly pollute a receptor (for example spills, fire, explosion), refer to section 4.2 'MATTE potential matrix'.

Consequence

A combination of the following:

- the extent, severity and duration of harm to the receptor.

Refer to section 3 'Definition of the types of Environmental Harm'

Risk

A combination of

- consequence and
- frequency of occurrence (per receptor per establishment per year)

Receptor

The receptor that could be polluted by the source, refer to section 3 'Definition of the types of Environmental Harm'.

Protection Layers

Risk reduction measures - either preventive layers (i.e. reduce the frequency of a hazardous event from occurring) or mitigatory layers (i.e. reduce the consequences of a hazardous event after it has occurred). Preventive layers typically include the primary containment (pipes, vessels and control systems) whilst mitigatory layers include secondary and tertiary containment or fire suppression systems.

Unmitigated consequence

The potential consequence from credible scenarios before any mitigation measures are employed, refer to section 4.3 'Aggregating Risk and Risk Frequencies'. This is essentially the worst credible consequence associated with the credible scenario, (with no protection layers in place) and is used to establish tolerability thresholds.

Unmitigated risk

The aggregated risk from credible scenarios, before any mitigation measures are employed, refer to section 4.3 'Aggregating Risk and Risk Frequencies'. This is the risk (consequence and frequency) associated with all credible scenarios given failure of prevention layers, escalation and no mitigation.

Mitigated risk

The level of risk that remains from all credible scenarios once existing protection layers (mitigation and/or prevention measures) are employed, refer to section 4.3 'Aggregating Risk and Risk Frequencies'.

Further risk reduction measures

Further risk reduction measures which could be employed to reduce the risk further to TifALARP or Broadly Acceptable. An ALARP demonstration, which might include Cost Benefit Analysis, may be required to further justify a claim of TifALARP.

4.2 MATTE potential matrix

The sources, or more importantly the substances which could give rise to a MATTE should be screened for each relevant receptor to determine their potential.

In order to screen for potential credible MATTE scenarios, it is important to understand the following:

- The types or groups of substances present on the site which could cause a MATTE
- The receptor itself, and how it could be polluted (or otherwise harmed) to the extent of causing a MATTE
- The site specific scenarios that could cause the receptor to be polluted (or otherwise harmed) to the extent of causing a MATTE

4.2.1 Grouping and compartmentalisation

To simplify the process of risk assessment, duty holders may consider grouping different product categories (or substances with similar risk phrases) which have a similar nature, and can damage the receptor in a similar way, for example:

- Petroleum products
- Dense non-aqueous phase liquid

Grouping of similar products can also be considered based on geographical location, for example, all products stored in a tank farm(s) have similar properties and all have the potential to pollute a nearby receptor(s).

On this basis it may not be necessary for sites to complete risk assessments for individual tanks and individual products but instead to group similar substances and 'compartments' of tanks within the site boundary.

4.2.2 Tables to assess MATTE potential

The tables defined in Appendix 5 provide a methodology for how to begin to assess the potential for substances (and cocktails of substances) to cause a MATTE if released to the receptor unmitigated. The tables are provided as guidance on the information that needs to be presented and provide a suggested format; however the information may be presented in another format.

Table 1 – MATTE Potential Summary Matrix

Table 1 can be used to summarise which substances or groups of substances could give rise to a MATTE if unmitigated (i.e. no prevention or mitigation measures are in place). The table should be completed for each receptor that is relevant to the site.

A tick (✓) can be used in each box to indicate that a MATTE could occur if the credible scenario (as defined in table 3) occurred.

A cross (x) can be used in each box to indicate that a MATTE could not be caused by the substance.

Further footnotes could be referenced with each tick or cross to justify the prediction.

Note that it is important that this summary table is used to cover the potential consequence of all dangerous substances, both single releases and multi-release (for example from a tank farm or warehouse) and firewater – the substance groupings defined can be used to achieve this.

Table 2 – Receptor Detail

Table 2 can be used to provide further definition of each relevant receptor and the environmental vulnerabilities which they present. Reference should be made to section 3 of this guidance document for further definition of the receptor type, and to Appendix 2 for the original DETR 1999 tables.

Please note, for designated sites it is expected that information will be sought from the conservation bodies.

Table 3 – MATTE Scenarios

Table 3 can be used to provide a description of the consequences to the receptor from the credible scenarios under which a MATTE may occur to each of the receptors. Typical scenarios may be:

- Tank Overfill
- Catastrophic Tank Failure
- Leak from tank base
- Pipework failure
- Warehouse / Chemical plant fire.
- Escalation of the above or any other incidents.

The majority of MATTEs seen across Europe have been harm to surface waters from direct releases or runoff from fires, but toxic gas and aerial deposition impacts (e.g. Seveso) should not be discounted.

Further guidance on typical Major Accident scenarios can be found in the Safety Report Assessment Guides (see <http://www.hse.gov.uk/comah/srag.htm>), and in H1 Environmental Risk Assessment, Annex A, (see <http://www.environment-agency.gov.uk/business/topics/permitting/36414.aspx>)

Table 4 – Dangerous Substances with Environmental Risk

Table 4 can be used to provide further definition of the substances or groups of substances which have the potential to cause environmental damage. The final column can be used to include a reference to link to a fuller description (e.g. a section of the Safety Report or MSDS reference).

Where substances share similar properties, grouping can be performed on the basis of risk phrases.

N.B. a group of chemicals could be “contents of warehouse A, loss of containment during fire” or “chemicals in bund B (tanks 1-5) and firewater”

4.3 Aggregating risk and risk frequencies

When analysing the MATTE potential for each receptor from the establishment, several potential credible scenarios may be identified which could cause harm to that receptor. Moreover, if there are several tanks, warehouses, process units, etc., the frequency of a MATTE occurring from the credible scenarios associated with each of these, above the specified consequence level, needs to be summed (independent events only) since the establishment risk to a receptor is from all credible MATTE scenarios from all sources (multiple sources will increase the risk). In practice, assurance that the total risk is reduced below a specified target can be done in a number of ways.

4.3.1 Aggregating risk option 1 - Summation of risks

Add all independent risks from all sources affecting a single receptor and compare these (both unmitigated and mitigated risk) to the receptor's establishment risk targets (e.g. Appendix 4 tolerability criteria) – this approach may suit small sites with a smaller number of Major Accident Scenarios.

4.3.2 Aggregating risk option 2 – Developing scenario based risk criteria

Once the consequence and frequency of an identified major accident scenario have been evaluated it is necessary to consider whether the risk from this scenario is 'Intolerable', 'TifALARP' or 'Broadly Acceptable'.

However the tolerability criteria are established for the frequency of ALL major accident scenarios from the establishment impacting on an environmental receptor. For larger sites this requires the summation of frequencies from a number of scenarios - which may be followed by identification of which scenario results in the 'Intolerable' or 'TifALARP' conclusion, and consequently requires risk reduction and/or ALARP assessment.

This approach can make it difficult for individual plant management teams to judge the tolerability of their own area scenarios and drive risk management processes. It is often more convenient, simpler and more empowering for plant management teams to 'allocate' a proportion of the 'Intolerable' risk criteria to each scenario, or each part of the site, against which the risks can be assessed.

The simplest way to achieve this is to estimate the total number of scenarios on the establishment which could result in specific MATTE severity level consequence to a receptor and divide the 'Intolerable' risk frequency criteria for this severity level by that number to define a scenario based risk criteria. If the receptor chosen for this calculation is the one most at risk from the site, the resultant criteria will be conservatively low for all other receptors. Therefore a 'scenario based' tolerability of risk matrix can be defined for use in scenario based risk assessments.

At the conclusion of the establishment risk assessment, it is clearly necessary to check the validity of the 'number of scenarios' assumption. If a specific scenario risk is found to be 'Intolerable' against the scenario specific criteria, further consideration of the total establishment risk to the scenario will be required - it may be that other risks to the receptor are sufficiently low that a greater proportion of the establishment criteria can be allocated to that scenario and that the overall risk remains 'TifALARP' i.e. the site may allocate different risk criteria to different scenarios within the overall establishment risk.

4.3.3 Impacts from adjacent sites

If the site is not currently designated as a domino site, then the site should consider only its own source/pathway/receptor analysis, and not that of other neighbours – the risk analysis will apply only to the one establishment.

For Domino sites:

- If the site is designated as a domino site, then the site operator is legally required to consult with their neighbours (who will also be designated as an upstream or downstream domino site). In these circumstances the increased risk of a neighbouring domino site creating an increased risk of a MATTE from your site needs to be included in the establishment risk aggregation and may increase the whole establishment risk to environmental receptors.
- For domino events risk can be increased in two ways. 1) The neighbouring domino site could increase the frequency at which a Major Accident could occur on your site – i.e. be an additional off-site initiator. 2) The consequences of the domino event could increase as the scale of a domino-type incident from both sites could be greater. Both possibilities need to be reflected in assessment.
- Scenarios from a domino site that do not increase risk of a MATTE (scale of consequence or frequency) at your site should not be included in the aggregation of risk to a receptor for your site. i.e. even though events at a neighbouring domino site might be MATTEs in their own right, if they do not affect your site these do not need to be included in your aggregation.

Domino example

Two COMAH domino sites, fuel terminal A and chemical warehouse B.

- Fuel terminal A – MATTE scenarios: Leaks, Fires (including running pool fires) and Explosion.
- Warehouse B – MATTE scenario: Fire.

The domino scenario is a fuel terminal running pool fire, which could initiate a warehouse fire causing a combined consequence greater than any other scenarios. For the purpose of this example, no other scenarios at site A or B would impact on each other.

The MATTE risk for fuel terminal A is as follows: To aggregate the risk for fuel terminal A on a receptor, take the scenarios for fuel terminal A which could affect the receptor. Because the running fuel fire could also initiate a fire at the warehouse, the consequences of both events happening at the same time needs to be included. Hence the overall consequences could be greater than from the running pool fire alone. However, frequency should not increase, as the frequency of pool fire initiating a warehouse fire should not be greater than the frequency of the running pool fire. Indeed the frequency of this domino scenario might be lower than the running pool fire frequency, if the running pool fire does not always lead to a fire at the warehouse.

The MATTE risk at warehouse B is the risk of fire, and this risk would be increased by the domino scenario. The risk would not include the scenarios of leaks at the fuel terminal which cannot impact site B. Thus the implication for site B being domino (as opposed to not domino) is a potential increase in consequence and frequency of MATTE.

Note 1: This example is based on one domino scenario. This circumstance would need review on a site by site, scenario by scenario basis. If there were multiple potential domino scenarios then the aggregate establishment risk could increase – either due to increased consequences or increased frequency of a specific consequence level or a combination of both.

Note 2: The Habitats Directive does require the assessment to consider a combination of risks from multiple sites. The view of the CA is that so long as individual sites routinely review the condition of Habitat sites which they can potentially impact upon and can demonstrate use of all measures necessary (i.e. ALARP) for their own risks, this would be seen as being sufficient, and would not require consideration of risk of simultaneous Major Accidents from other neighbouring COMAH sites (except for those domino sites noted above). If a Major Accident to a Habitats Directive site does occur, then other operators will be expected to review the implications of that accident for their own sites after the event has occurred.

4.3.4 Determining risk frequencies

Company specific failure rate data (for the identified credible scenarios) could be used when completing environmental risk assessments. However the CA would require justification (for example hours of operation, circumstance of failures etc.) as to the figures used where they were significantly different to published industry figures. In the majority of cases it is anticipated that failure rate data will be the same for safety and the environment (i.e. the initiating event frequency should be the same).

Where company specific failure rate data is not available, duty holders can make reference to the table of typical failure rates and the Environmental QRA data and MATTE case studies available in the CA's 'All Measures Necessary Guidance'.

Note that when completing environmental risk assessments, consideration should be given to escalation of a scenario, which could give rise to a greater consequence.

4.3.5 Determining risk reduction of prevention and mitigation layers

Reference should be made to the CA's 'All Measures Necessary Guidance' for information relating to the risk reduction provided by different prevention and mitigation layers. Other sources may also be of use, for example insurance company databases may provide failure rate data for fire prevention systems.

5. Cost Benefit Analysis

This section provides advice on how to include the cost of environmental harm in COMAH Cost Benefit Analysis (CBA). Existing guidance on CBA within an ALARP demonstration is relevant to environmental CBAs and the general framework for carrying out the CBA is the same for risks to persons and risks to the environment. Relevant guidance includes application of CBA for decisions within the TifALARP zone, as outlined by HSE guidance on ALARP (including SPC/perm/37 & 39) and general principles associated with CBA, as outlined in the wider HSE CBA principles and CBA checklist.

5.1 Disproportion Factor (DF)

Disproportion Factors should be used in environmental CBAs in the same way as for Health and Safety CBAs, within the range 1 to 10, (10 at the intolerable border, and 1 at the broadly acceptable border). The operator needs to justify why a specific DF has been applied. A Major Accident Hazard (MAH) could possibly result in several consequences to both persons and the environment and that each consequence could have a different DF. The CBA summation would be the last task following the application of each DF.

5.2 Benefits

Health, safety and environmental benefits should be included in the CBA where these relate directly to a MAH. Business related benefits such as avoided loss of production, higher insurance premiums, damage to an operators own assets, insurance costs etc. should not be included as a benefit. These business related benefits may be considered by the operator when considering investment, but this is not required to be included as part of a CBA supporting an ALARP demonstration to the CA.

5.3 Costs

Only those costs incurred solely from the implementation of the measure should be included.

5.4 Discounting Rates

It is recommended that the same discounting rate is used for costs and benefits for health, safety and the environment. Refer to <http://www.hse.gov.uk/risk/theory/alarpcba.htm> for further information.

5.5 Evaluation of Environmental Remediation

Where available, company specific costs should be used as this will often provide the most accurate information as it is based on the company's own experience of dealing with environmental incidents. If no company data is available, generic cost information can be found from a number of sources, including:

- i. Worldwide Analysis of Marine Oil Spill Clean-up Cost Factors
- ii. Cost Analyses for Selected Groundwater Clean-up Projects
- iii. Assessing the Value of Groundwater

iv. Assessing fish kills

Refer to Appendix 1 for further details regarding these sources of information.

The following checklist may be helpful when considering activities to be included in the costing exercise:

- i. Reference to pre - accident baseline data set of the ecological condition of the impacted area
- ii. Establishment of post - accident data set for ecological condition of the impacted area, e.g. monitor, sample, test and analyse watercourses, groundwater, soil etc.
- iii. Identification of the scope of remedial work
- iv. Establishment of temporary facilities and utilities
- v. Excavation and removal / storage / treatment of contaminated material
- vi. Import and consolidation of fill material
- vii. Pump out and removal / treatment of contaminated groundwater
- viii. Mitigation / clean-up of surface waters (river / estuarine / coastal)
- ix. Restoring the natural environment e.g. fish stocking
- x. Restoring the built environment
- xi. Clean-up of pollution to third party property
- xii. Civil liability claims e.g. loss of fisheries / impact on tourism / loss of abstraction
- xiii. Environmental fines

6. Completing the risk assessment

Risk assessments can be completed in two parts:

- Part 1 – MATTE Definition and Thresholds, refer to section 6.1
- Part 2 – Risk assessment process, refer to section 6.2

When considering receptors with MATTE potential, note that the Safety Report Assessment Manual (SRAM) indicates that it is reasonable to screen within 10km of the site. However, for linear pathways (such as rivers) this distance may be longer.

6.1 Part 1 - MATTE definition and thresholds

With reference to sections 3 and 4, the Source-Pathway-Receptor approach described in the flowchart below can be used to identify those scenarios from the establishment which could harm each environmental receptor:

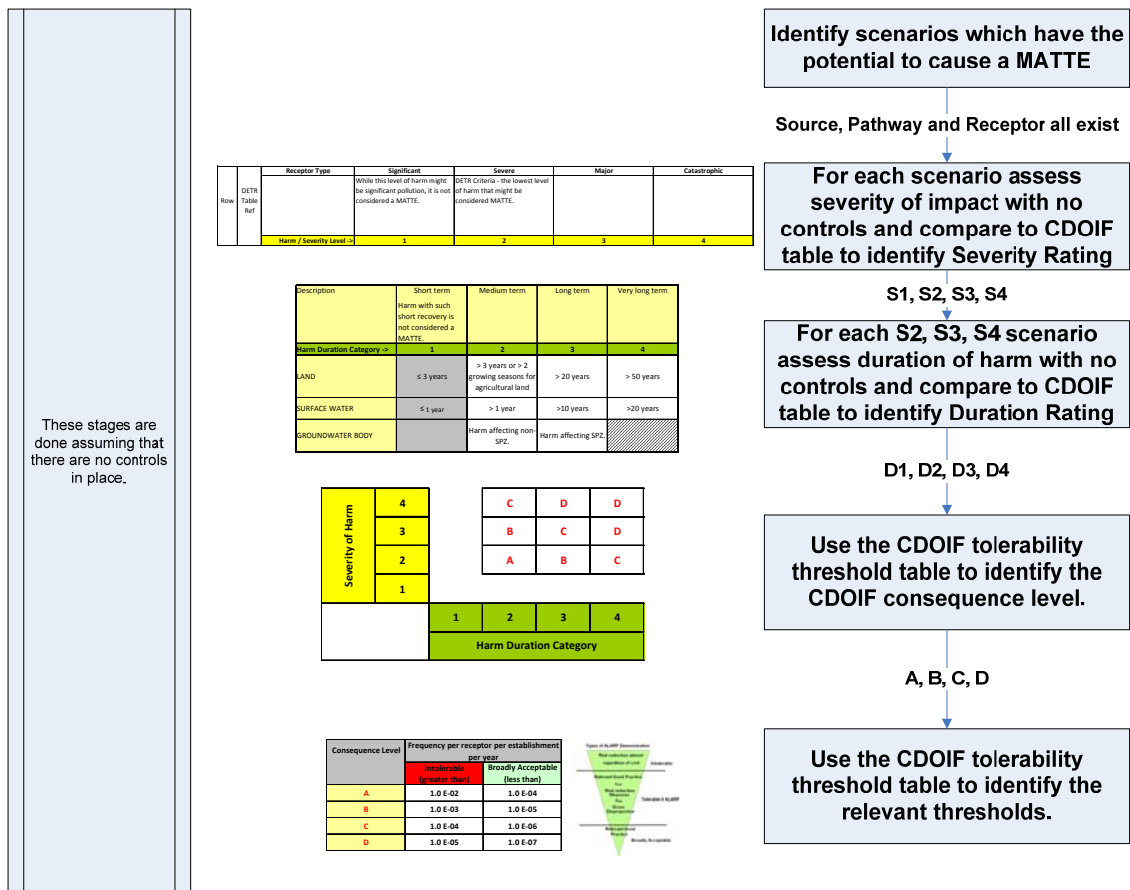


Figure 5 – Summary of MATTE Tolerability Tables (Refer to Appendix 4)

6.1.1 Identifying the major accident scenarios

When considering which credible major accident scenarios to consider as part of the risk assessment, two options are available:

- Evaluate all credible scenarios which could have a MATTE potential on the identified receptor, or
- Select a representative set of credible major accident scenarios, in line with the HSE guidance 'Risk analysis or 'predictive' aspects of COMAH safety reports guidance for explosive sites',
<http://www.hse.gov.uk/comah/assessexplosives/index.htm>

Note that when using a representative set of credible major accident scenarios, it is likely that aggregation of risk will be based on developing scenario based risk criteria as described in section 4.3.2.

6.1.2 Determining the level of severity

For each credible major accident scenario (or representative set of credible major accident scenarios) and receptor affected, assign the Level of Severity that would be associated with the unmitigated consequences (see 4.1):

- Table 1 (Severity/Harm criteria for consideration as a major accident) in Appendix 4 contains consequence descriptions – the “severe” column represents the lowest level MATTE descriptor (as taken from the DETR 1999 guidance). Consequences lower than this, although pollution incidents are not regarded as MATTE or covered by COMAH. Consequences greater than this level may trigger the higher threshold categories in the table.
- Each column in the table has a number assigned to it: 1-4. This is the harm/severity level.

6.1.3 Assigning a duration/recovery category

For each credible major accident scenario (or representative set of credible major accident scenarios), assign a duration/recovery category that would be associated with the unmitigated consequences.

It has been recognised that environmental incidents differ in ultimate consequence depending on the (natural) recovery time of the environment. Longer term harm will produce a less tolerable consequence than one of only short duration.

For many scenarios there will be opportunities for clean-up and remediation as a post-incident measure which will reduce environmental harm. However, these should be disregarded at this stage, but discussed as “mitigation” measures within the ALARP demonstration.

To assign a duration/recovery category:

- Using Table 2 (Duration/Recovery criteria) in Appendix 4, select a duration descriptor for the relevant receptor category. These should be unaided recovery times, without restoration and clean-up activity (though natural attenuation can be taken into account). These are broad-brush categories, and as part of the screening process, estimates can be used.
- Each duration column has a category level assigned to it: 1-4. This is the harm/duration category.

6.1.4 Determining tolerability boundaries

Determine Tolerability boundaries from the Tolerability Assessment Matrix (Appendix 4 Table 3 - MATTE tolerability assessment matrix)

- Using the harm/severity level (1-4) and the harm/duration category (1-4), determine the overall unmitigated Consequence Level (A-D) from the matrix.
- Each consequence level (A-D) has been assigned tolerability thresholds to define the ALARP band. i.e. Intolerable and Broadly Acceptable frequencies per receptor, per establishment, per year.

The level of risk posed by the establishment, to each receptor, is then compared with these respective tolerability criteria, as explained in section 6.2 below.

6.2 Part 2 calculating the establishment risk frequencies

Part 1 of the risk assessment process has identified the ALARP band. Part 2 sets out how to assess the risk from the establishment to the receptor:

- Determine the risk from the establishment to a receptor
 - Determine the frequency of occurrence of all scenarios based on available failure rate and/or event data (which may include preventative or mitigatory layers and if so these should be clearly identified in the assessments).
 - Total the frequency of all scenarios from the establishment that result in each Consequence level (A-D) to the receptor.
 - The total frequency of events which meet or exceed each consequence level of harm should then be compared with the tolerability thresholds established in Part 1 (section 6.1). When comparing the establishment frequency of lower consequence levels (e.g. B) with the assigned ALARP bands, note that the total frequency to be considered is the total of that and higher consequence levels (i.e. B + C + D). An example of how aggregation is completed can be found in section 6.2.1.
- If the risk is still not Tolerable if ALARP (TifALARP) then assess other potential control measures, accept/dismiss these within an ALARP demonstration and integrate into site improvement plan as appropriate

6.2.1 Aggregating risk - Examples

Completing the initial screening (as described in section 6.1) will have discounted potential receptors from the risk assessment process as the screening will have determined that a MATTE is not credible.

For those substances and scenarios which do have MATTE potential, their risks to the relevant receptor must now be determined. As it is the total risk to the receptor that is required, i.e. from all substances, and credible scenarios, these risks must be aggregated. Examples of how this can be achieved for each receptor are provided in the following sections.

- 6.2.1.1 – Single substance stored in a single tank
- 6.2.1.2 – Tank farm or group of tanks containing similar substances
- 6.2.1.3 – Groups (e.g. tank farms) with dissimilar substances/incident consequences

In each of the examples below, the first step is to identify the credible scenarios that could cause a MATTE to the receptor being assessed (note that this could be credible scenarios from a single tank, multiple tank or facility based on the grouping of substances and compartmentalisation).

Once the credible scenarios have been identified, these should then each be categorised using the MATTE tolerability matrix (refer to Appendix 4) to give a consequence level of either A, B, C or D - this in turn provides the frequency per receptor per establishment per year and thus the thresholds for broadly acceptable and intolerable.

When aggregating the risk to a receptor from all credible scenarios, the following text can be used as a guide:

Tolerability of risk to the receptor, from the establishment as a whole, will depend on the aggregate predicted frequency of all independent accident scenarios which could impact a given receptor at or above the respective consequence level. Thus to confirm tolerability at level D then all independent level D predicted incident frequencies should be aggregated. To confirm tolerability at level A, all independent level A, B, C and D predicted incident frequencies should be aggregated.

Refer also to section 6.2.1.5 on interdependent scenarios.

6.2.1.1 Single substance stored in a single tank



If we assume that credible scenarios, consequence levels of those scenarios and event frequencies are as follows:

Scenario (Tank Farm Tank 1)	Consequence Level*	Event frequency*
Catastrophic tank failure	B	F1, 1×10^{-6}
Large hole	A	F2, 1×10^{-5}
Small leak from tank base	A	F3, 1×10^{-4}

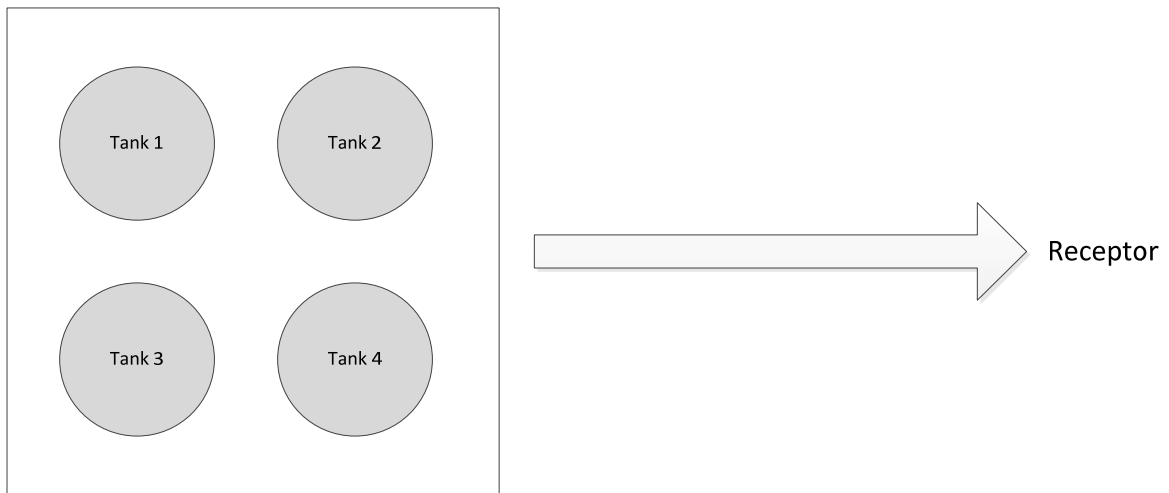
*Provided for illustrative purposes only, and at this stage does not include mitigation. For event frequencies refer to section 'Determining unmitigated risk frequencies' which is a sub-section of 6.2. For consequence level, refer to 'MATTE thresholds', section 3.2.

The aggregated risk to the receptor for all credible scenarios can be calculated as follows:

$$\text{Category B incident frequency} = F1 = 1 \times 10^{-6}$$

$$\text{Category A incident frequency} = F1 + F2 + F3 = 1 \times 10^{-6} + 1 \times 10^{-5} + 1 \times 10^{-4} = 1.11 \times 10^{-4}$$

6.2.1.2 Tank farm or group of tanks containing similar substances



If we assume that credible scenarios, consequence levels of those scenarios and event frequencies for each of the tanks are the same (because of substance grouping/compartimentalisation), and can be defined as follows:

Scenario (Tank Farm Tanks 1-4)	Consequence Level*	Event frequency*
Catastrophic tank failure	B	F1, 1×10^{-6}
Large hole	A	F2, 1×10^{-5}
Small leak from tank base	A	F3, 1×10^{-4}

* Provided for illustrative purposes only, and at this stage does not include mitigation. For event frequencies refer to section 'Determining unmitigated risk frequencies' which is a sub-section of 6.2. For consequence level, refer to 'MATTE thresholds', section 3.2

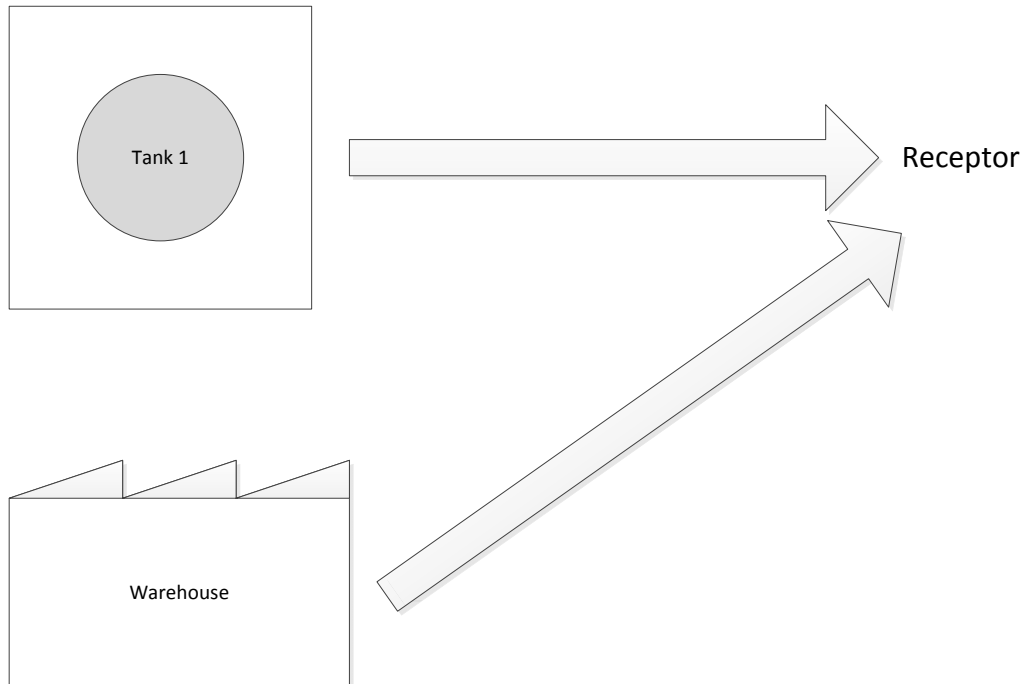
On the basis that there are now 4 tanks, the aggregated risk to the receptor for all credible scenarios (i.e. the frequency of any one of the scenarios at or above the relevant consequence level occurring from any one of the tanks) can be calculated as follows:

$$\text{Category B incident frequency} = 4 * (F1) = 4 \times 10^{-6}$$

$$\text{Category A incident frequency} = 4 * (F1 + F2 + F3) = 4 * (1 \times 10^{-6} + 1 \times 10^{-5} + 1 \times 10^{-4}) = 4.44 \times 10^{-4}$$

6.2.1.3 Groups (e.g. tank farms) with dissimilar substances/incident consequences

It is likely, particularly on chemical sites, that substances/scenarios will not be sufficiently similar to group together. However, the Category A, B, C or D incidents can be aggregated in the same way as indicated in the earlier examples.



If we assume that credible scenarios, consequence levels of those scenarios and event frequencies for each of the tanks are the same (because of substance grouping/compartimentalisation), and can be defined as follows:

Scenario (Tank Farm Tank 1)	Consequence Level*	Event frequency*
Catastrophic tank failure	B	F1, 1×10^{-6}
Large hole	A	F2, 1×10^{-5}
Small leak from tank base	A	F3, 1×10^{-4}

Scenario (Warehouse)	Consequence Level*	Event frequency*
Warehouse fire	B	F4, 1×10^{-3}

* Provided for illustrative purposes only, and at this stage does not include mitigation. For event frequencies refer to section 'Determining unmitigated risk frequencies' which is a sub-section of 6.2. For consequence level, refer to 'MATTE thresholds', section 3.2

The aggregated risk to the receptor for all credible scenarios can be calculated as follows:

$$\text{Category B incident frequency} = F1 + F4 = 1 \times 10^{-6} + 1 \times 10^{-3} = 1.001 \times 10^{-3}$$

$$\text{Category A incident frequency} = F1 + F2 + F3 + F4 = 1 \times 10^{-6} + 1 \times 10^{-5} + 1 \times 10^{-4} + 1 \times 10^{-3} = 1.111 \times 10^{-3}$$

It can be seen that in this example that the warehouse fire is by far the biggest contributor to the risk frequency, and hence this indicates where best to look at additional control measures.

6.2.1.4 Comparison with tolerability criteria

For the single tank and warehouse example above it was determined

Category B incident frequency = 1.001×10^{-3}

Category A incident frequency = 1.111×10^{-3}

These can then be compared to the tolerability criteria as follows:

Frequency at which CDOIF Consequence Level is equalled or exceeded	Frequency per establishment per receptor per year (unmitigated)						
	10^{-8} – 10^{-7}	10^{-7} – 10^{-6}	10^{-6} – 10^{-5}	10^{-5} – 10^{-4}	10^{-4} – 10^{-3}	10^{-3} – 10^{-2}	$>10^{-2}$
D - MATTE						Intolerable	
C - MATTE				TifALARP			
B - MATTE	Broadly Acceptable					X	
A - MATTE						X	
Sub MATTE	Tolerability not considered by CDOIF						

The unmitigated risk is depicted above by **X**.

Up to this point in the assessment, no mitigation has been considered. It is now necessary to consider what forms of mitigation are in place to further reduce risk. The calculations above need to be repeated to include the Probability of Failure on Demand (PFD) of any protection layers present (e.g. safety instrumented systems, secondary or tertiary containment, emergency arrangements) to estimate the mitigated risk to each receptor, for each consequence category and thus whether mitigated risk is tolerable.

So, for example, if the tank is bunded (PFD = 0.1) and the bunded tank and warehouse surrounded by site-wide tertiary containment designed to contain fire runoff (PFD = 0.1) then the mitigated risk to each receptor would be calculated by multiplying the event frequency with the relevant mitigation layer PFD(s) as follows:

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Scenario (Tank Farm T1)	Consequence Level ¹	Event frequency ¹	Independent mitigation layers (PFD) ¹	Outcome frequency (mitigated)
Catastrophic tank failure	B	F1, 1×10^{-6}	0.1 * 0.1	F5, 1×10^{-8}
Large hole	A	F2, 1×10^{-5}	0.1 * 0.1	F6, 1×10^{-7}
Small leak from tank base	A	F3, 1×10^{-4}	0.1 * 0.1	F7, 1×10^{-6}

Scenario (Warehouse)	Consequence Level ¹	Event frequency ¹	Independent mitigation layer (PFD) ¹	Outcome frequency (mitigated)
Warehouse fire	B	F4, 1×10^{-3}	0.1	F8, 1×10^{-4}

Note 1: Provided for illustrative purposes only. For event frequencies refer to section 4.3.4 'Determining risk frequencies'. For consequence level, refer to 'MATTE thresholds', section 3.2.

The aggregated mitigated risk to the receptor for all credible scenarios can be calculated as follows:

$$\text{Category B mitigated frequency} = F5 + F8 = 1 \times 10^{-8} + 1 \times 10^{-4} = 1.0001 \times 10^{-4}$$

$$\text{Category A mitigated frequency} = \text{Category A frequencies} + \text{Category B frequencies}$$

$$= (F6 + F7) + (F5 + F8)$$

$$= 1 \times 10^{-7} + 1 \times 10^{-6} + 1 \times 10^{-8} + 1 \times 10^{-4} = 1.0111 \times 10^{-4}$$

These can then be compared to the tolerability criteria as follows:

Frequency at which CDOIF Consequence Level is equalled or exceeded	Frequency per establishment per receptor per year (mitigated)						
	$10^{-8}-10^{-7}$	$10^{-7}-10^{-6}$	$10^{-6}-10^{-5}$	$10^{-5}-10^{-4}$	$10^{-4}-10^{-3}$	$10^{-3}-10^{-2}$	$>10^{-2}$
D - MATTE						Intolerable	
C - MATTE				TifALARP			
B - MATTE	Broadly Acceptable				X		
A - MATTE					X		
Sub MATTE	Tolerability not considered by CDOIF						

The mitigated risk is depicted above by **X**.

It can now be seen that the mitigated risk is TifALARP. Further risk reduction needs to be considered and implemented so far as is reasonably practicable (but an ALARP demonstration may show the cost of further risk reduction is grossly disproportionate).

6.2.1.5 Interdependent scenarios

When summing frequencies it is important that this should only be done for independent events.

For example, from the four tank example above (6.2.1.2), consider a further possible level C scenario of a multi-tank fire arising from a spill followed by escalation. The overall escalated scenario frequency would be made up from the chance of any of the other events occurring (spills) and then escalating (ignition). The frequency of the escalation scenario would need to be compared to the level C tolerability criteria.

However, when considering the frequencies for A and B tolerability (all events with outcomes at or exceeding level A or B), the risk assessor would not in this case sum the A and B spill frequencies with the escalated event (level C) frequency. This is because the level C event is not independent from the level A and B initiating events. The escalated scenario frequency is derived from the frequencies of the lesser events and their probabilities of escalation (the spill frequency includes the frequency of both un-ignited and ignited events). Summing the spill events and the escalated fire events would result in double counting of the same initiating events.

Conversely, if the level C scenario was caused by an event independent to the level A and B events (e.g. explosion from adjacent site) then the frequencies would be summed when examining level A or B tolerability.

Consideration of bowtie diagrams often helps to avoid errors in logic.

7. Abbreviations

Abbreviation	Description
ALARP	As Low As Reasonably Practicable
AONB	Areas of Outstanding Natural Beauty
CA	Competent Authority
CBA	Cost Benefit Analysis
CDOIF	Chemical and Downstream Oil Industry Forum
CICS	Common Incident Classification Scheme
COMAH	Control of Major Accident Hazards
DETR	Department of the Environment, Transport and the Regions
DF	Disproportion Factor
EA	Environment Agency
EPR	Environmental Permitting Regulations
ESA	Environmentally Sensitive Areas
EU	European Union
LNR	Local Nature Reserves (may be referred to as Local Wildlife Site)
MAH	Major Accident Hazard
MATTE	Major Accident to the Environment
MNR	Marine Nature Reserves
NNR	National Nature Reserves
NSA	Nitrate Sensitive Areas
OS	Ordnance Survey
PFD	Probability of Failure on Demand
PPC	Pollution Prevention and Control (Regulations)
SAC	Special Areas of Conservation
SEPA	Scottish Environment Protection Agency
SPA	Special Protection Areas
SPZ	Source Protection Zone
SRAM	Safety Report Assessment Manual
SSSI	Site of Special Scientific Interest
TifALARP	Tolerable if As Low As Reasonably Practicable
WFD	Water Framework Directive

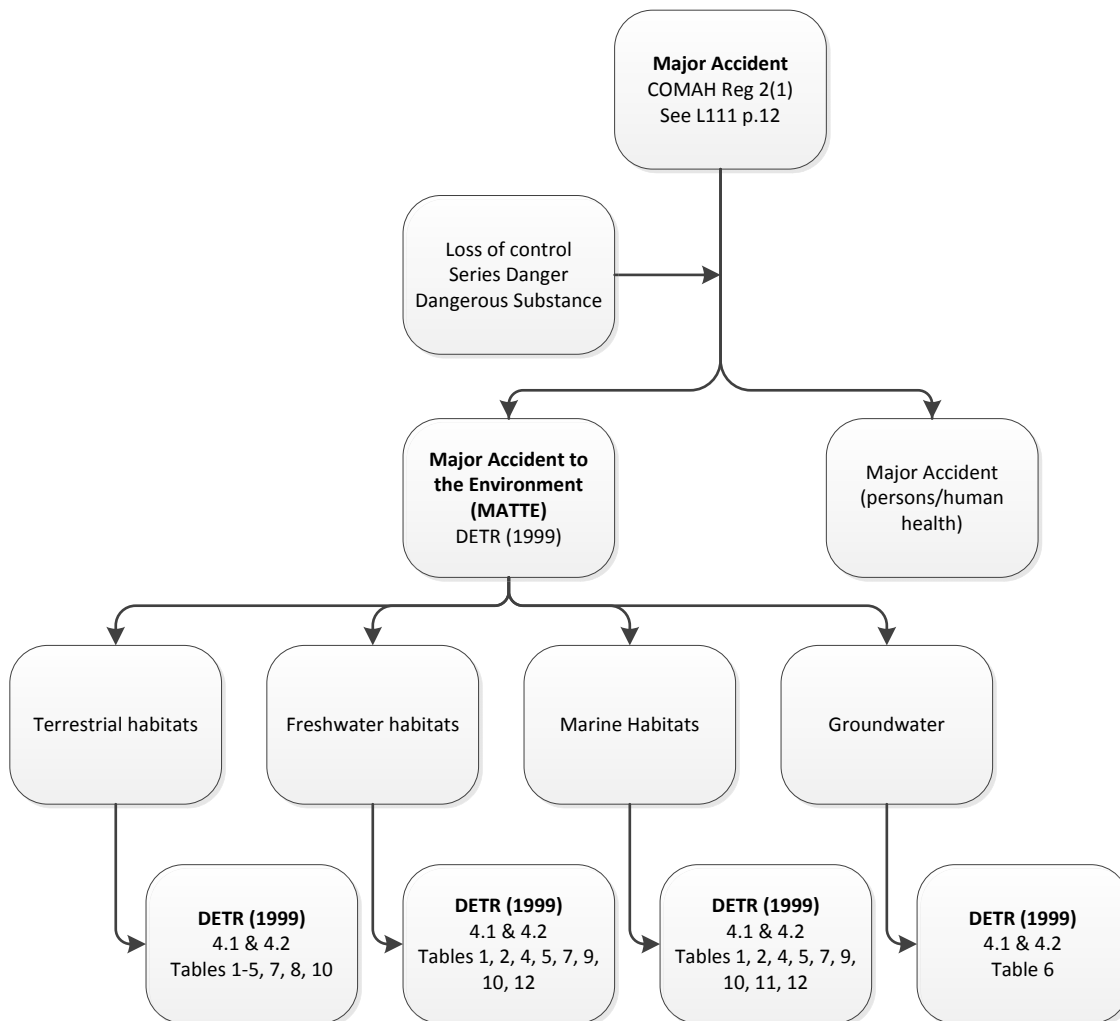
Revision History

Rev.	Section	Description	Date	Changed By
0.0	All	First Issue	23-Jan-2012	Peter Davidson
0.1	3	Updated with WP2 definitions	27-Jul-2012	Peter Davidson
0.2	3	Corrected WP2 definition	01-Aug-2012	Peter Davidson
0.3	3	Updated to include TA comments	08-Aug-2012	Peter Davidson
0.4	All	Updated following WP 3 Meeting 13/08/12	23-Aug-2012	Peter Davidson
0.5	All	Updated following road testing	24-Jan-2013	Peter Davidson
0.6	All	Updated to final draft – for stakeholder review	08-Feb-2013	Hugh Bray Ian Brocklebank Jackie Coates Mike Nicholas Peter Davidson
0.7	All	Stakeholder review comments incorporated	23-Jul-2013	Hugh Bray Ian Brocklebank Jackie Coates Mike Nicholas Peter Davidson
0.8	All	Final stakeholder review comments incorporated	19-Aug-2013	Hugh Bray Ian Brocklebank Jackie Coates Mike Nicholas Peter Davidson
1.0	All	First publication	18-Sep-2013	Hugh Bray Ian Brocklebank Jackie Coates Mike Nicholas Peter Davidson

Appendix 1 - Key Guidance

The following provides reference to the key guidance relating to environmental risk assessment, and how that guidance inter-relates.

Reference should also be made to the table on the following page which provides links to access both L111 and DETR 1999 and other related guidance and legislation.



CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Topic	Guidance	Web reference
General COMAH	A guide to the Control of Major Accident Hazards Regulations 1999 (as amended) (L111) (HSE, 2006)	www.hse.gov.uk/pubns/books/l111.htm
	Guidance on the Interpretation of Major Accident to the Environment for the Purposes of the COMAH Regulations (DETR, 1999)	http://archive.defra.gov.uk/environment/quality/chemicals/accident/index.htm
	CA procedures and strategic topics (signposting CA expectations on necessary measures)	http://www.hse.gov.uk/comah/ca-guides.htm
	HSE ALARP suite of guidance	http://www.hse.gov.uk/risk/expert.htm
	Guidance Identifying COMAH Major Accidents to the Environment (MATTE) Table 3 EA, 2004	N/A
Risk Assessment for COMAH (guidance applicable to Safety Reports and LT risk assessment)	Safety Report Assessment Manual – Section 13 (remodelled for use with all Safety Reports)	http://www.hse.gov.uk/comah/guidance/sram.pdf
	Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports, COMAH CA, Dec 1999	http://www.environment-agency.gov.uk/default.aspx (search for COMAH safety report – document filed as comah_1785585)
	HSG 190 Preparing Safety reports (HSE, 1999)	http://www.hse.gov.uk/pubns/books/hsg190.htm
Historic incident data	eMARS (European accident database)	https://emars.jrc.ec.europa.eu/
	ARIA	http://www.aria.developpement-durable.gouv.fr/index_en.html

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Topic	Guidance	Web reference
General Risk Assessment	Guidelines for Environmental Risk Assessment and Management – Green Leaves III (DEFRA, 2011)	http://www.defra.gov.uk/publications/2011/11/07/green-leaves-iii-pb13670/
Related legislation (see also regulator and DEFRA websites)	Water Framework Directive	http://ec.europa.eu/environment/water/water-framework/index_en.html and http://www.wfduk.org/
	Habitats Directive	http://ec.europa.eu/environment/nature/legislation/habitatsdirective/index_en.htm
	Environmental Liability Directive	http://ec.europa.eu/environment/legal/liability/index.htm
General good practice	EA Pollution Prevention Guidance (PPGs)	http://www.environment-agency.gov.uk/business/topics/pollution/39083.aspx
	HSE Health and Safety Guidance (HSGs)	http://www.hse.gov.uk/pubns/books/index-hsg-ref.htm
Other useful references	My Environment Website	http://www.myenvironment.org.uk/

Appendix 2 – DETR 1999 Table References

The following provides reference to the relevant definition tables in the DETR 1999 Guidance on the interpretation of Major Accident to the Environment for the purposes of COMAH regulations.

Table 1 National Nature Reserves, Sites of Special Scientific Interest, Marine Nature Reserves (Land/Water)

<p>Medium: Land/Water (inter-tidal/near-shore sub-tidal)</p> <p>Receptor: NNRs, SSSIs, MNRs</p> <p>Definition of receptor: National Nature Reserves (NNRs) Sites of Special Scientific Interest (SSSIs), both biological (terrestrial and water-based) and geological Marine Nature Reserves (MNRs)</p> <p>Threshold: The following thresholds apply:</p> <ul style="list-style-type: none"> • Greater than 0.5 ha adversely affected, or greater than 10% of the area of the site affected (whichever is the lesser), or • Greater than 10% of an associated linear feature adversely affected, or • Greater than 10% of a particular habitat or population of individual species adversely affected. 	<p>Explanation/justification:</p> <p>Sites of Special Scientific Interest (SSSIs) represent areas judged to be special on the basis of their plant or animal communities, geological features or landforms. They represent the basic minimum area of habitat that should be conserved to maintain the current range and distribution of native plants and animals. SSSIs can be terrestrial (biological or geological), freshwater or marine. In practice, the seaward limit of an SSSI depends upon the definition of 'land', but generally can extend to mean low water (inter-tidal).</p> <p>SSSIs are notified under Section 28 of the Wildlife & Countryside Act 1981.</p> <p>National Nature Reserves (NNRs) are a key selection of nationally important SSSIs. NNRs have been established to protect the most important national areas of wildlife habitat and geological formation. They are among the best examples of particular habitat types, and therefore represent a nationally important resource. The selection of NNRs is based on criteria including fragility of, and threats to, habitats and species, size, lack of disturbance, presence of species-rich communities and rare species, and the degree of 'naturalness' of the site.</p> <p>NNRs are designated under Section 19 of the National Parks and Access to the Countryside Act 1949.</p> <p>Marine Nature Reserves (MNRs) are designated under Section 36 of the Wildlife & Countryside Act 1981 in areas between the high water mark and the territorial limit.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 2 Natura 2000 sites, Ramsar sites (Land/Water)

<p>Medium: Land/Water</p> <p>Receptor: Natura 2000 sites (SPAs, SACs), Ramsar sites</p> <p>Definition of receptor: Special Areas of Conservation (SACs) Special Protection Areas (SPAs) Ramsar sites</p> <p>[Note that these receptors are often also SSSIs]</p> <p>Threshold: Lower thresholds than for SSSIs.</p> <p>For SACs, SPAs, and Ramsar sites, the thresholds are:</p> <ul style="list-style-type: none"> • Greater than 0.5 ha or 5% of the area of the site adversely affected (whichever is the lesser), or • Greater than 5% of an associated linear feature adversely affected, or • Greater than 5% of a particular habitat or population of individual species adversely affected. 	<p>Explanation/justification: Central to the European Union's policy of protecting and conserving wildlife and habitats is the creation of an ecological network of protected areas – Natura 2000. Natura 2000 sites are SACs and SPAs.</p> <p>SPAs are aimed at conserving bird species listed in Annex I of Council Directive 79/409/EEC on the conservation of wild birds (the 'Birds Directive'), and also migratory birds. This is primarily through designation of bird habitats, and particularly wetlands.</p> <p>SACs conserve the habitat types, animals and plant species listed under Council Directive 92/43/EEC on the conservation of natural habitats and of wild flora and fauna (the 'Habitats Directive'), and thus contribute towards maintenance of favourable conservation status of selected habitats and species. Marine habitats and species are included.</p> <p>The Habitats Directive (Article 6) sets out a legal framework for protecting these sites. Article 6(2) outlines a general duty for Member States to avoid habitat deterioration and significant species disturbance within a site.</p> <p>Ramsar sites are wetlands of international importance (arising from the Convention on Wetlands of International Importance especially as Waterfowl Habitat).</p> <p>As a matter of policy the Government wishes sites listed as potential SPAs and candidate SACs to be treated as if they are already designated.</p> <p>Further details may be found in Appendix 2.</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 3 Other designated land (Land)

Medium:
Land

Receptor:
Other designated land

Definition of receptor:
Environmentally Sensitive Areas (ESAs)
Areas of Outstanding Natural Beauty (AONBs)
Greenbelt land
National Parks
Local Nature Reserves (LNRs), Wildlife Trust sites
National Trust land
Common land/country parks

Threshold:
• Greater than 10% or 10 ha of land damaged, whichever is the lesser.

Explanation/justification:

Nature conservation values are covered by designations such as SSSI and NNR. However, there are many more land designations that aim to conserve areas purely for amenity and aesthetic reasons.

Such areas may (or may not) have associated wildlife value, but are valued for landscape, aesthetic (outstanding natural beauty), historic and archaeological, geological amenity or recreational features.

Table 4 Scarce habitat (Land/Water)

Medium:
Land/Water

Receptor:
Scarce habitat

Definition of receptor:
Biodiversity Action Plan habitats
Geological features: caves, fossil beds, mineral veins, moraines, etc.

Threshold:
• Damage to 10% of the area of the habitat or 2 ha, whichever is the lesser, would be considered a major accident.

Explanation/justification:

Scarce/key habitats are awarded protection principally on the basis of the declines in distribution and extent of such habitats within the recent past. Those habitat types which have undergone major or rapid declines, or which are rare, are considered to be 'at risk'. Additionally, certain areas, particularly marine/coastal/estuarine, are extremely important in terms of their functioning, and are thus 'key' in this respect. Other habitats, whilst not necessarily of great intrinsic value in themselves, are worthy of consideration/protection because of the particular species that they may support.

The local English Nature/Scottish Natural Heritage/Countryside Council for Wales office should be consulted to identify these receptors locally.

Table 5 Widespread habitat (Land/Water)

Medium:
Land/Water

Receptor:
Widespread habitat

Definition of receptor:
More widespread habitat, including agricultural land, that has not been otherwise classified, i.e. is not designated or scarce

Forestry

Threshold:

- Contamination of 10 ha or more of land which, for one year or more, prevents the growing of crops or the grazing of domestic animals or renders the area inaccessible to the public because of possible skin contact with dangerous substances, or
- Contamination of any aquatic habitat which prevents fishing or aquaculture or which similarly renders it inaccessible to the public.

Explanation/justification:

The size criteria of 10 ha of land can relate either to the total area contaminated or the total land taken out of production as a result of a smaller area being contaminated. It is assumed that contamination of a proportion of a field will result in the whole field being unusable due to the difficulties associated with determination of 'safe' and 'unsafe' areas of the same field.

It should be remembered that there may still be areas within the wider countryside of high conservation value, and that the lack of current designation does not necessarily imply that an area is of no ecological worth.

Table 6 Aquifers or groundwater (Water)

Medium:
Water

Receptor:
Aquifers or groundwater

Definition of receptor:
Water resources in or under the soil

Threshold:
A major accident would be:

- Any incident likely to require large-scale and long-term remedial measures, or
- Any incident of contamination/pollution (by persistent compounds) occurring within groundwater protection zone 1 (the most vulnerable groundwater resources).

Explanation/justification:

Groundwater is water that is held underground, mainly within rock formations. Approximately 75% of the groundwater that is abstracted in England and Wales is used for drinking water. Because groundwater is inaccessible, it is difficult to remediate contamination incidents. Therefore, any incident likely to result in pollution of groundwater should be considered to be serious.

The Environment Agency has published a groundwater protection policy for England and Wales, classifying groundwater vulnerability to pollution on the basis of the nature of the overlying soils, the presence and nature of unconsolidated deposits overlying solid rock formations, the nature of the rock strata, and the depth to the water-table. Vulnerability maps have been produced which identify areas in which groundwater requires protection. Similarly, the Scottish Environment Protection Agency (SEPA) has produced a Groundwater Protection Policy for Scotland.

This information should be used to identify the presence of vulnerable groundwaters locally.

The Directive on the protection of groundwater against pollution caused by certain dangerous substances (80/68/EEC) will be integrated into the forthcoming Water Framework Directive. The current Directive aims to control the direct and indirect discharge of certain substances into groundwater: List 1 substances, which should be prevented from entering groundwater; and List 2 substances, which could have a harmful effect on groundwater.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 7 Soil or sediment (Land/Water)

Medium:
Land/Water

Receptor:
Soil or sediment

Definition of receptor:
Material at the earth's surface or the base of the water column to a depth of 1 metre (soil samples to be obtained from the top 10 cm for chemical analysis)

Threshold:
Contamination or pollution of the receptor such that

- Soil would be regarded as contaminated land by relevant authorities (i.e. contamination such that planned present or future uses could be compromised), or
- Sediment would become loaded with sufficient material to compromise the chemical or biological quality of overlying waters for any period in excess of a few days.

Deterioration of the biological quality of soil or sediment such that

- Common organisms of these ecosystems (e.g. earthworms) were absent, the structure of the biological community altered for periods in excess of a season, or normal ecosystem function was severely impaired for a period in excess of one year.

Explanation/justification:

There are no existing numerical criteria for soil quality that are thought adequate for indicating what might constitute a major accident to the environment in relation to soils and sediments. Thus, thresholds have been set in non-numerical terms. As a guide, long-term 'capping' or other forms of physical amendment of soil or sediment are likely to lead to loss of soil biodiversity, as will high levels of chemical contamination with a range of individual substances (such as metals and persistent organic compounds) and mixtures of substances.

Operators' attention is drawn (a) to earlier work by the Interdepartmental Committee on the Redevelopment of Contaminated Land (ICRCL 59/83) that lists trigger thresholds for different contaminants according to future uses of the land, and (b) to work from the Netherlands that sets optimum and action levels for a range of contaminants in soil (the so-called 'Dutch list'). These documents provide particular perspectives on soil contamination that mean they cannot be used to meet the requirements of Seveso II/COMAH. Similar documents available from North America have similar limitations.

CDOIF

Chemical and Downstream Oil
Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 8 Built heritage (Land – man-made)

Medium:
Land – man-made

Receptor:
Built heritage

Definition of receptor:
Buildings
Listed buildings

Threshold:

- Damage to a Grade I listed building (England and Wales) or a category A building (Scotland) or a scheduled ancient monument such that it no longer possesses its architectural, historic or archaeological importance, and which would result in it being de-listed or de-scheduled if no remedial/restorative work was undertaken, or
- Sediment would become loaded with sufficient material to damage to an area of archaeological importance or to a conservation area similarly resulting in loss of importance.

Explanation/justification:

Buildings of architectural or historic interest (England and Wales) are listed in accordance with the Planning (Listed Buildings and Conservation Areas) Act 1990. The list includes most buildings constructed before 1840, together with others depending on quality, character and/or architect. Grade I buildings are of 'exceptional importance'.

Buildings of special architectural or historic interest (Scotland) are listed under the terms of the Town and Country Planning (Scotland) Act 1972, using similar criteria to those used in England. Category A buildings are those of national architectural or historic importance.

Ancient monuments of national importance (England and Wales) are scheduled under the Ancient Monuments and Archaeological Areas Act 1979.

Similar documents available from North America have similar limitations.

Table 9 Various receptors, as defined (Water)

<p>Medium: Water</p> <p>Receptor: Various, as defined</p> <p>Definition of receptor: Groundwater Drinking water Fish and shellfish water Bathing waters</p> <p>Threshold: Standards relating to continuous emissions and contained within the relevant European legislation (listed here) should not be adopted to define a major accident. However, the specific level of exceedence of these standards should be considered in the post-accident remediation and restoration works.</p>	<p>Explanation/justification: Groundwater Directive (80/68/EEC) on the protection of groundwater pollution caused by certain dangerous substances aims to control the direct and indirect discharge of these substances into groundwater.</p> <p>The Drinking Water Directive (80/778/EEC) relates to the quality of water for human consumption, and establishes standards for quality of drinking water designed to safeguard human health.</p> <p>The Surface Water for Drinking Water Abstraction Directive (75/440/EEC) lays down requirements to ensure that surface water intended for the abstraction of drinking water meets certain minimum specified standards.</p> <p>The Dangerous Substances Discharges Directive (76/464/EEC) on pollution caused by certain dangerous substances discharged into waters requires control of emissions.</p> <p>Directive 78/659/EEC on fish water quality seeks to protect fresh waters identified as fish waters and sets water quality standards for salmonid and cyprinid waters. Where the water quality in such waters does not comply with the standards, pollution reduction is required. Directive 79/923/EEC on shellfish water quality similarly seeks to protect those coastal and brackish water bodies identified as shellfish waters.</p> <p>The Bathing Water Directive (76/160/EEC) seeks to ensure the quality of bathing waters, both freshwater and coastal. Nineteen physical, chemical and microbiological parameters are set, and monitoring of bathing waters is required.</p> <p>The Integrated Pollution Prevention and Control Directive (96/61/EEC) deals with emissions to air and soil as well as to water, and will have a central role in the control of point source pollution.</p> <p>The proposed Water Framework Directive will establish a common approach to environmental objectives for all ground and surface waters. The target of 'good water status' would have to be achieved within a specified period of the Directive coming into force.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 10 Particular species (Land/Water/Air)

Medium:
Land/Water/Air

Receptor:
Particular species

Definition of receptor:
'Common' species
Species listed under European legislation
Species listed in the Wildlife & Countryside Act
Red Data Book species

Threshold:

- For common species, where reliable estimates of population numbers exist, the death of, or serious sub-lethal effects within, 1% of any species would be significant.
- For common plant species, the death of, or serious sub-lethal effects within, 5% of the ground cover would be considered a major accident.
- For species listed in Appendix 4, the threshold may be lower than 1% or 5%, and liaison with the appropriate statutory conservation organisations should be used to determine the appropriate threshold.

Moreover, for all species, where reliable estimates of population numbers do not exist, liaison with the statutory authority will be necessary to determine appropriate thresholds.

Any loss of a Red Data Book species (or a Red Data Book species site) would be considered a major accident.

Explanation/justification:

Damage to individuals (sub-lethal effects and death) within populations may not only have implications for the survival of that species, but may also have knock-on consequences for other species, the habitat or the ecosystem. Thus major accidents to species need to be considered not only in terms of the sustainability of the affected species, but also in terms of other species that may be wholly or partly dependent upon that species.

For species listed in Appendix 4 (threatened and rare species), a major accident will generally be deemed to have occurred at lower thresholds than for common species, i.e. the definition of a major accident will depend upon the commonness or rarity of that species.

Furthermore, the mobility and dispersal ability of species could be considered in the context of other suitable habitat in the locality. Certain species may be able to move away from a site following an incident and utilise resources elsewhere, whereas others may be unable to move or be dependent upon that area.

In addition, the effect of the same event at different times of the year should be considered, i.e. between seasons different species may be present at differing population densities; an event coinciding with the breeding season may be more serious than the same event at a different time of year.

Table 11 Marine (Water)

Medium:
Water

Receptor:
Marine

Definition of receptor:
Non-estuarine marine waters
Littoral, sub-littoral zone
Benthic community adjacent to coast
Fish spawning grounds

Threshold:
Permanent or long-term damage to

- An area of 2 ha or more of the littoral or sub-littoral zone, or the coastal benthic community, or the benthic community of any fish spawning ground, or
- An area of 100 ha or more of the open sea benthic community.

Or a count of

- 100 or more dead sea birds (not gulls), or
- 500 dead sea birds of any species, or
- 5 dead or significantly injured/impaired sea mammals of any species.

Explanation/justification:

Damage is assessed relative to the area impacted, or the number of individuals affected, rather than by contaminant concentrations in the water. Dilution may subsequently reduce the concentration of a released substance to levels difficult to measure (and thus monitor), although initial concentrations may be sufficiently high to damage sub-littoral, littoral and inshore organisms. Moreover, low concentrations of substances may still pose a hazard if they are highly toxic or if they are persistent and bioaccumulate.

The number of animal casualties detected following an accident will depend on local circumstances, such as geographical location, season and whether the incident occurred near a breeding colony. Moreover, the extent of the impact on species will rarely be quantifiable immediately following the accident, and will require long-term monitoring to adequately assess the true extent of the impact.

The number of animals killed in an incident is almost certain to be considerably more than the number of casualties detected. For example, the proportion of casualties recovered may be as low as 10-20% of the total number of animals impacted.

Table 12 Freshwater and estuarine habitats (Water)

<p>Medium: Water</p>	<p>Explanation/justification: A 'significant part' of a river, canal or stream is taken to be a 10 km stretch or 10% of the length of the water course, whichever is the lesser.</p>
<p>Receptor: Freshwater and estuarine habitats</p>	<p>For estuaries and ponds, a significant area is taken to be 2 ha or 10% of the area, whichever is the lesser.</p>
<p>Definition of receptor: Stream, river, canal, reservoir, lake, pond or estuary</p>	<p>Long-term damage will be deemed to have occurred if the system takes longer than 3 years to recover.</p>
<p>Threshold: • Effects on a significant part of any receptor defined above which, when assessed using the Environment Agency General Quality Assessment (GQA) scheme, either lower the chemical water quality by one class for more than one month or lower the biological quality by one class for more than one year or cause long-term damage to the habitat overall (but see explanation).</p>	<p>There are several factors to be taken into consideration when assessing the severity of impacts to fresh waters:</p> <p>The importance of lowering the quality of the water when assessed using the Environment Agency GQA scheme may be considered to be of greater importance in the case of higher quality water courses than already degraded systems.</p> <p>The precise location of the impact relative to the water course may be important, such that an impact affecting the head waters may be more serious than one further down stream, particularly in relation to the potential for recovery. Downstream habitats may be readily recolonised by organisms from further upstream, but upstream areas may take much longer to recover.</p> <p>Increased consideration should be given to the use to which the water is put when assessing the severity of an impact.</p> <p>Evaluation techniques exist to assess not only water quality but also existing vegetation and fauna, i.e. RIVPACS (see Glossary).</p>

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 3 – Information Sources

Note: For Wales, please contact site officer – further guidance to be available after the formation of Natural Resources Wales. The following web links were correct at the time of publication, but are subject to change.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
1	Designated Land/Water Sites (National)	England	www.magic.gov.uk/ http://www.natureonthemap.naturalengland.org.uk/ International sites tab www.jncc.gov.uk/	As per item 2 below but focus on sites of national importance	SSSIs, National Nature Reserves, Marine Conservation Zones	Natural England Environment Agency See also guidance on Environmental Damage (http://www.defra.gov.uk/environment/quality/environmental-liability/) for interpretational guidance on Damage to species and habitats.	see item 2 below	
		Wales Scotland	Scotland's Environmental Web interactive mapping page (SEWeb) "Wildlife" tab Scottish Natural Heritage Website "Protected Areas" tab www.jncc.gov.uk/	On both websites interactive maps can be used to search for and identify designated sites. The Marine Atlas can assist in identifying the location and population of some species which may be of interest.	SSSIs, National Nature Reserves etc. The area of the site can be found on the relevant information sheet or citation for the area this can be accessed via the Joint Nature Conservation Committee (JNCC website). In some cases the qualifying population may also be included.	Scottish Natural Heritage (SNH) http://www.snh.gov.uk/ Relevant Fishery Board List of fisheries boards See also guidance on Environmental Damage (http://www.scotland.gov.uk/Resource/Doc/211199/0087791.doc) for interpretational guidance on Damage to species and habitats.		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
2	Designated Land/Water Sites (International)	England	<p>www.magic.gov.uk/</p> <p>http://www.natureonthemap.naturalengland.org.uk/</p> <p>International sites tab</p> <p>www.jncc.gov.uk/</p>	<p>In magic the interactive map can be used to search "Rural Designations – Statutory" (step 1) around a given location (step 2). This opens a new map with further map tools such as a radius / linear and polygon searches or identify features at specific point.</p> <p>Depending on site location, other layers, such as "Coastal and marine resources atlas" might also be relevant.</p>	<p>SAC, SPA, Ramsar sites and their component SSSIs</p> <p>Use magic to find the sites (e.g. radius search or manually explore map along length of a stream/river) – then follow links to data (e.g. on the JNCC and Natural England websites)</p>	<p>Natural England, http://www.naturalengland.org.uk/</p> <p>Environment Agency</p> <p>See also guidance on Environmental Damage (http://www.defra.gov.uk/environment/quality/environmental-liability/) for interpretational guidance on Damage to species and habitats</p>	<p>https://emars.jrc.ec.europa.eu/</p> <p>http://www.aria.developpement-durable.gouv.fr/index_en.html</p> <p>Accident databases, like the two above can be searched using substance based keywords / CAS / industry type and the impacts from the shortlisted incidents compared to those that might be credible for the installation under assessment.</p>	<p>Once receptors have been identified either assume impact is possible and screen scenario in or gather more detailed data on the vulnerability of those to impact from the chemicals concerned need to be assessed. e.g. data at http://evidence.environment-agency.gov.uk/ChemicalStandards/home.aspx</p> <p>This to be considered along with the site conservation objectives and status.</p>
		Wales	<p>Scotland</p> <p>Scotland's Environmental Web interactive mapping page (SEWeb)</p> <p>"Wildlife" tab</p> <p>Scottish Natural Heritage Website</p> <p>"Protected Areas" tab</p> <p>www.jncc.gov.uk/</p>	<p>On both websites interactive maps can be used to search for and identify designated sites.</p> <p>The Marine Atlas can assist in identifying the location and population of some species which may be of interest.</p>	<p>SAC, SPA, Ramsar sites and their component SSSIs</p> <p>The area of the site can be found on the relevant information sheet or citation for the area this can be accessed via the links on the SNH website or via the Joint Nature Conservation Committee (JNCC website).</p> <p>In some cases the qualifying population may also be included.</p>	<p>Scottish Natural Heritage (SNH) http://www.snh.gov.uk/</p> <p>Relevant Fishery Board List of fisheries boards</p> <p>See also guidance on Environmental Damage (http://www.scotland.gov.uk/Resource/Doc/211199/0087791.doc) for interpretational guidance on Damage to species and habitats.</p>		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
3	Other designated land	England	As per Table 1 row 1 "International sites)			Local Wildlife Trusts Local Authority Local Records Centre		
		Wales						
		Scotland	Useful webpages include: Map of National Scenic Areas National Parks in Scotland webpage SNH Local nature reserves webpage Wildlife Trust Site search			Scottish Natural Heritage Local Wildlife Trusts Local Authority Local Records Centre		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
4	Scarce Habitat	England	www.magic.gov.uk/ http://www.natureonthemap.naturalengland.org.uk/ International sites tab www.jncc.gov.uk/	In magic, lower designations might also be found in other datasets such as "Rural Designations – Other" and "Rural Land-Based Schemes"		Local Wildlife Trusts Local Authority Local Records Centre		
		Wales						
		Scotland	UK BAP species and habitats webpage SNH Bio-diversity webpage Local authority biodiversity action plans SNH Geo-diversity webpage			Local Wildlife Trusts Local Authority Local Records Centre		
5	Widespread Habitat – Non-designated land	England	See table 1.2 of H1 Annex A for data sources e.g. OS mapping	Use data sources to establish main types of land use, and in particular any agricultural or areas of public access	Generally land use can be determined by OS mapping, and if not by local field surveying (walking / driving round to see what land-use is evident.)	For food safety – FSA For risk to people, HSE & HPA		
		Wales						
		Scotland	e.g. OS mapping					

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
5	Widespread Habitat – Non-designated water	England	See table 1.2 of H1 Annex A for data sources e.g. OS mapping Angling trust http://www.anglingtrust.net/	Use data sources to establish main types of land use, and in particular angling trust to find the local angling society, club or fishery.	Generally land use can be determined by OS mapping, and if not by local field surveying (walking / driving round to see what land-use is evident.)	For food safety – FSA For risk to people, HSE & HPA For fishing – local angling society		
		Wales						
		Scotland	e.g. OS mapping					
6	Source of public or private drinking water (groundwater or surface water)	England	See What's in your Backyard - http://www.environment-agency.gov.uk/ For surface water abstraction information discuss with EA site officer or contact 03708 506 506 or enquiries@environment-agency.gov.uk	In WIYBY, enter place or postcode, select the groundwater topic and check the Groundwater Source Protection Zone box (in Map legend on Left Hand side). N.B. you may need zoom in or out – this layer only displays at certain map scales.	SPZs are depicted as a colour overlay	Environment Agency		If drinking water is a relevant receptor the drinking water standards will need to be considered – see http://evidence.environment-agency.gov.uk/ChemicalStandards/home.aspx
		Wales						
		Scotland	Contact SEPA and the relevant local Authority asking for the location of Drinking Water abstraction in the area concerned.			SEPA Private water supplies are the responsibility of owners and users and are regulated by local authorities.		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
6	Groundwater body (non- drinking water source)	England	See What's in your Backyard - http://www.environment-agency.gov.uk/	In WIYBY, enter place or postcode, select the groundwater topic and check the Aquifer Maps (either superficial or bedrock or both). Aquifers will appear as coloured areas. See also the topic "River basin Management Plans – Groundwater" for current and predicted status.	Groundwater bodies are a distinct volume of groundwater within an aquifer or aquifers	Environment Agency See also guidance on Environmental Damage (http://www.defra.gov.uk/environment/quality/environmental-liability/) for interpretational guidance on Damage to water		
		Wales Scotland	SEPA has mapped all bedrock aquifers and selected extensive sand and gravel aquifers as groundwater bodies, and these underlie the whole mainland of Scotland and many islands. These groundwater bodies can be seen on our interactive map .	Open the map and click on the double down arrow next to table of contents. From the menu click the 2008 Classification status box. Groundwater bodies will now be shown on the map. Use the "identify" icon from the menu at the top of the map to identify which groundwater body is under the area being assessed. Other more localised sand and gravel aquifers have not been mapped as groundwater bodies due to their inherent variability and a lack of information. The presence of these more localised aquifers can only be determined using site specific data.		SEPA See also guidance on Environmental Damage (http://www.scotland.gov.uk/Resource/Doc/211199/0087791.doc) for interpretational guidance on damage to water.		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
				SEPA's Position Statement WAT-PS-10-01 , Assigning groundwater assessment criteria for pollutant inputs provides more details on how to make this determination.				
6	Other Groundwater (outside of groundwater bodies)	England	See What's in your Backyard - http://www.environment-agency.gov.uk/	Area outside of SPZs, aquifers (groundwater bodies) would not appear as coloured when the layers are selected as described above.				
		Wales						
		Scotland	See groundwater bodies above.	Groundwater bodies underlie the whole mainland of Scotland and many islands, and therefore in most cases an assessment will be required in order to justify use of this category.		SEPA		
7	Soil or sediment (i.e. as receptor rather than purely a pathway)	England	Further information on Environmental Damage Regulations http://www.defra.gov.uk/environment/quality/environmental-liability/ and see the in depth guide in particular	The definitions of Environmental damage to conservation sites and water is aligned to the MATTE thresholds above and thus covered by the above rows, thus potential environmental damage to land should be the key consideration for this receptor.	Damage to land is: ...contamination of land by substances, preparations, organisms or micro-organisms that results in a significant risk of adverse effects on human health.	Environment Agency or Local Authority	see http://www.defra.gov.uk/environment/quality/environmental-liability/ which includes incident returns detailing previous Environmental Damage cases	
		Wales						
		Scotland	Further information on the application of the Environmental Liability	The Scottish Government ELR Technical Guidance gives definitions and		SEPA or Local Authority		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
			Regulations can be found at the SEPA Environmental Liability Regulations web-page and the Scottish Government Environmental Liability Regulations web-page	examples of "Environmental Damage".				
8	Built environment	England	http://www.english-heritage.org.uk/ www.magic.gov.uk/ "Rural Designations – statutory" for scheduled monuments and world heritage sites	In the English heritage site you can search The National Heritage List for England to search for listed buildings in your area and download copies of individual entries. The site also provides world heritage information	Use English Heritage site advanced search to limit search to Grade I listing in a given location then from the search results see list entry summary for detail	English Heritage, Local planning authority for listed buildings, Institute of historic building conservation (www.ihbc.org.uk), The National Trust, County Archaeologist (local county council)		
		Wales						
		Scotland	Scotland's Environmental Web interactive mapping page "Built Environment" Tab	Marked on the map as: Listed Buildings; Conservation Areas; Scheduled Monuments; or World Heritage sites.		Historic Scotland		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
9	Various receptors							
10	Particular species	England	In addition to magic and JNCC (links above), see the National Biodiversity Network's Gateway http://data.nbn.org.uk/	In NBN gateway search for data by species or site Explore species distributions, whole datasets, protected sites and habitats using the interactive map	See in particular note on appendix 4 where such species might be associated with a designated site (thus proportion of the local population harmed, not national population is used)	Natural England and others species specific bodies such as the Amphibian and Reptile Conservation trust and the British Trust for Ornithology		
		Wales						
		Scotland						
11	Marine	England	www.magic.gov.uk/ Select "Coastal and marine resources atlas" (step 1 of interactive map). OS mapping See also What's in your Backyard - http://www.environment-agency.gov.uk/	For the status of coastal waters - In WIYBY, enter place or postcode, select the River Basin Management Plan (Coastal or estuarine) topic	Water body status depicted as a colour overlay	Environment Agency and Inshore Fishery and Conservation Authorities, See also guidance on Environmental Damage (http://www.defra.gov.uk/environment/quality/environmental-liability/) for interpretational guidance on Damage to water		
		Wales						
		Scotland	Scotland's Environmental Web (SEWeb) interactive mapping webpage	For the status of coastal waters - In SEWeb, enter place or postcode, select "Advanced Maps" then "Water" and the relevant		See also guidance on Environmental Damage (http://www.scotland.gov		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

DETR Table	Receptor Type		How can I decide which receptors I have around my site?	How do I use/interpret the information on the website?	What features are most relevant and where can I find detail of them – for example designation land, categorisation for water	Which agency or body should I contact if I need further information on helping me determine MATTE potential?	What impact have 'similar' incidents had, and where can I find more information about these?	How do I use the information gathered above to help me work out Consequence (Extent, Severity and Duration)?
			The Marine Atlas and the Interactive Marine Planning Tool can assist in identifying the location and population of some species which may be of interest.	classification requirements (Coastal or estuarine). OS Explorer series (1:25 000 scale) shows the position of high and low tide marks.		.uk/Resource/Doc/21119/9/0087791.doc for interpretational guidance on damage to water.		
12	Fresh and estuarine water habitats	England	www.magic.gov.uk/ For estuaries select "Coastal and marine resources atlas" (step 1 of interactive map). OS mapping See also What's in your Backyard - http://www.environment-agency.gov.uk/	For the status of fresh and estuarine waters - In WIYBY, enter place or postcode, select the River Basin Management Plan (Rivers, Lakes, Estuarine) topics	Water body status depicted as a colour overlay	Environment Agency See also guidance on Environmental Damage (http://www.defra.gov.uk/environment/quality/environmental-liability/) for interpretational guidance on Damage to water		
		Wales						
		Scotland	Scotland's Environmental Web (SEWeb) interactive mapping webpage	For the status of fresh and estuarine waters - In SEWeb, enter place or postcode, select "Water" and the relevant classification requirements (Rivers, Lochs, Estuarine)	Water body status can be selected	SEPA See also guidance on Environmental Damage (http://www.scotland.gov.uk/Resource/Doc/21119/9/0087791.doc) for interpretational guidance on damage to water.		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 4 – MATTE tolerability tables

Table 1 - Severity/Harm criteria for consideration as a major accident (based on unmitigated consequence)

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			<i>While this level of harm might be significant pollution, it is not considered a MATTE.</i>	<i>DETR Criteria - the lowest level of harm that might be considered MATTE.</i>			<i>Corresponding Harm/Duration / Recovery row in Table 2</i>	<i>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</i>
		Severity Level →	1	2	3	4		<i>Receptors include:</i>
1	1	Designated Land/Water Sites (Nationally important)	<0.5ha or <10%	>0.5ha or 10-50% of site area, associated linear feature or population	>50% of site area, associated linear feature or population	N/A	Land or Surface Water	NNR, SSSI, MNR
2	2	Designated Land/Water Sites (Internationally important)	<0.5ha or <5% (<5% LF/Pop)	>0.5ha or 5-25% of site area or 5-25% of associated linear feature or population	25-50% of site area, associated linear feature or population	>50% of site area, associated linear feature or population	Land or Surface Water	SAC, SPA, RAMSAR
3	3	Other designated Land	<10ha or <10%	10-100ha or 10-50% of land	>100ha or >50% of land	N/A	Land	ESA, AONB, National Park, etc.
4	4	Scarce Habitat	<2 ha or <10%	2-20ha or 10-50% of habitat	>20ha or >50% of habitat	N/A	Land or Surface Water	BAP habitats, geological features

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			<p><i>While this level of harm might be significant pollution, it is not considered a MATTE.</i></p>	<p><i>DETR Criteria - the lowest level of harm that might be considered MATTE.</i></p>			<p><i>Corresponding Harm/Duration / Recovery row in Table 2</i></p>	<p><i>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</i></p> <p><i>Receptors include:</i></p>
			Severity Level →	1	2	3	4	
5	5	Widespread Habitat - Non-designated Land	<10ha	Contamination of 10-100ha of land, preventing growing of crops, grazing of domestic animals or renders the area inaccessible to the public because of possible skin contact with dangerous substances. Alternatively, contamination of 10ha or more of vacant land.	100-1000ha (applied as per text under 'Severe')	>1000ha (applied as per text under 'Severe')	Land	Land/water used for agriculture, forestry, fishing or aquaculture
6	5	Widespread Habitat - Non-designated Water		Contamination of aquatic habitat which prevents fishing or aquaculture or renders is inaccessible to the public.	N/A	N/A	Surface Water	Land/water used for agriculture, forestry, fishing or aquaculture

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			While this level of harm might be significant pollution, it is not considered a MATTE.	DETR Criteria - the lowest level of harm that might be considered MATTE.				
Severity Level →			1	2	3	4		
7	6	Source of Public or Private Drinking Water (Groundwater or Surface Water)	<p>Interruption of drinking water supply <1000 person-hours or For England & Wales only <1ha SPZ</p>	<p>Interruption of drinking water supplied from a ground or surface source (where persons affected x duration in hours [at least 2] > 1,000) or For England & Wales only 1-10ha of SPZ where drinking water standards are breached</p>	<p>>1 x 10⁷ person-hours interruption of drinking water (a town of ~100,000 people losing supply for month) or For England & Wales only 10-100ha SPZ drinking water standards breached</p>	<p>>1 x 10⁹ person-hours interruption of drinking water (~1 million people losing supply for 1 month) or For England & Wales only >100ha SPZ drinking water standards breached</p>	<p>Corresponding Harm/Duration / Recovery row in Table 2</p> <p>Groundwater body or Surface Water Public Drinking Water Source</p>	<p>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</p> <p>Receptors include:</p> <p>In England the area of groundwater, used for public drinking water, at risk from pollution is mapped using Source Protection Zones (SPZs). In Scotland, there is not an equivalent mapping of SPZs and only the interruption criteria should be used.</p>

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			While this level of harm might be significant pollution, it is not considered a MATTE.	DETR Criteria - the lowest level of harm that might be considered MATTE.				
Severity Level →	1	2	3	4				
8	6	Groundwater Body (non- Drinking Water Source)	<1ha	1-100ha of groundwater body where the WFD status has been lowered	100-10,000ha	>10,000ha	Groundwater body or Surface Water Public Drinking Water Source	UKTAG has determined that to qualify as a body of groundwater, an aquifer must be capable of supplying 10m ³ per day or 50 people (on a continuous basis) and that such aquifers/groundwater bodies have future resource value which must be protected. Groundwater Bodies have been identified and mapped in accordance with guidance under the Water Framework Directive – see 3.2.3 and appendix 3 for further information
9	6	Other Groundwater (outside of groundwater bodies)	Groundwater not a pathway to another receptor.	Where the groundwater is a pathway for another receptor assess against relevant criteria for the receptor.		N/A		

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			<p>While this level of harm might be significant pollution, it is not considered a MATTE.</p>	<p>DETR Criteria - the lowest level of harm that might be considered MATTE.</p>			<p>Corresponding Harm/Duration / Recovery row in Table 2</p>	<p>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</p> <p>Receptors include:</p>
		Severity Level →	1	2	3	4		
10	7	Soil or sediment (i.e. as receptor rather than purely a pathway)	Contamination not leading to environmental damage (as per ELD), or not significantly affecting overlying water quality.	Contamination of 10-100ha of land etc. as per Widespread Habitat; Contamination sufficient to be deemed environmental damage (Environmental Liability Directive)	Contamination of 100-1000ha of land, as per Widespread Habitat; Contamination rendering the soil immediately hazardous to humans (e.g. skin contact) or the living environment, but remediation available.	Contamination of >1000ha of land, as per Widespread Habitat; Contamination rendering the soil immediately hazardous to humans (e.g. skin contact) or the living environment and remediation difficult or impossible.	Land	
11	8	Built environment	Damage below a level at which designation of importance would be withdrawn.	Damage sufficient for designation of importance to be withdrawn.	Feature of built environment subject to designation of importance entirely destroyed.	N/A	Built Environment	This is limited to Grade 1 / Cat A Listed buildings, scheduled ancient monuments, conservation area, etc.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			<i>While this level of harm might be significant pollution, it is not considered a MATTE.</i>	<i>DETR Criteria - the lowest level of harm that might be considered MATTE.</i>			<i>Corresponding Harm/Duration / Recovery row in Table 2</i>	<i>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</i> <i>Receptors include:</i>
		Severity Level →	1	2	3	4		
12	9	Various receptors. Should not be used to identify and assess MATTE.	N/A	N/A	N/A	N/A	N/A	Refer to DETR. Standards relating to continuous emissions, contained in other EU legislation.
13	10	Particular species (Note - these criteria apply nationally - i.e. England, Wales, Scotland)	Loss of <1% of animal or <5% of plant ground cover in a habitat.	Loss of 1-10% of animal or 5-50% of plant ground cover.	Loss of 10-90% of animal or 50-90% of plant ground cover.	Total loss (>90%) of animal or plant ground cover.	Land	
14	11	Marine	<2ha littoral or sub-littoral zone, <100ha of open sea benthic community, <100 dead sea birds (<500 gulls), <5 dead/significantly impaired sea mammals	2-20ha littoral or sub-littoral zone, 100-1000ha of open sea benthic community, 100-1000 dead sea birds (500-5000 gulls), 5-50 dead/significantly impaired sea mammals	20-200ha littoral or sub-littoral zone, 100-10,000ha of open sea benthic community, 1000-10,000 dead sea birds (5,000-50,000 gulls), 50-500 dead/significantly impaired sea mammals	>200ha littoral or sub-littoral zone, >10000ha of open sea benthic community, >10000 dead sea birds (>50000 gulls), >500 dead/significantly impaired sea mammals	Surface Water	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant	Severe	Major	Catastrophic		
			<i>While this level of harm might be significant pollution, it is not considered a MATTE.</i>	<i>DETR Criteria - the lowest level of harm that might be considered MATTE.</i>			<i>Corresponding Harm/Duration / Recovery row in Table 2</i>	<i>The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.</i>
		Severity Level →	1	2	3	4		Receptors include:
15	12	Fresh and estuarine water habitats	Impact below that of Severity level 2	WFD Chemical or ecological status lowered by one class for 2-10km of watercourse or 2-20ha or 10-50% area of estuaries or ponds. Plus interruption of drinking water supplies, as per DETR Table 6	WFD Chemical or ecological status lowered by one class for 10-200km of watercourse or 20-200ha or 50-90% area of estuaries and ponds. Plus interruption of drinking water supplies, as per DETR Table 6	WFD Chemical or ecological status lowered by one class for >200km of watercourse or >200ha or >90% area of estuaries and ponds. Plus interruption of drinking water supplies, as per DETR Table 6	Surface Water	

Notes for Table 1:

In applying the criteria on this sheet, an estimate of the mean population of species will be required, subject to data available. Variability in population might be relevant for later detailed scenario assessments, but a mean is more relevant to the initial selection criteria here.

When applying the criteria above, note that receptors are not mutually exclusive - for example some sites are both Ramsar and SSSI, while the 'widespread habitat' rows might apply irrespective of any specific designations.

To avoid disproportionate application of percentage criteria on small receptors, for small sites, the percentage criteria will not reduce the threshold to lower than half the area/distance criteria.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Glossary of terms for table 1

Littoral: pertaining to the shore of a lake, sea, or ocean.

Sub-littoral zone: from the low water line to the edge of the continental shelf

Benthic community: is made up of organisms that live in and on the bottom of the ocean floor.

WFD: Water Framework Directive

SAC: Special Area of Conservation

SPA: Special Protection Area

RAMSAR: Wetlands of international importance,

NNR: National Nature Reserve

MNR: Marine Nature Reserve

BAP habitat: Biodiversity Action Plan habitat

ESA: Environmentally Sensitive Area

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 2 – Duration/Recovery criteria (based on unmitigated consequence)

Description	Short term	Medium term	Long term	Very long term
	Harm with such short recovery is not considered a MATTE.			
Harm Duration Category →	1	2	3	4
LAND	≤ 3 years	> 3 years or > 2 growing seasons for agricultural land	> 20 years	> 50 years
SURFACE WATER (ALL EXCEPT PUBLIC OR PRIVATE DRINKING WATER SOURCE)	≤ 1 year	> 1 year	>10 years	>20 years
GROUNDWATER BODY OR SURFACE WATER PUBLIC OR PRIVATE DRINKING WATER SOURCE	N/A	Harm affecting non-public drinking water source.	Harm affecting public drinking water source or SPZ.	N/A
BUILT ENVIRONMENT	Can be repaired in < 3 years, such that its designation can be reinstated	Can be repaired in > 3 years, such that its designation can be reinstated	Feature destroyed, cannot be rebuilt, all features except world heritage site	Feature destroyed, cannot be rebuilt, world heritage site

Notes for Table 2:

Separate criteria are provided in Table 2 depending on the nature of the site, be it land, surface water or groundwater - these shall be applied in conjunction with the corresponding harm criteria in Table 1.

These criteria are based on estimating the likely time for the habitat (or species, etc.) has substantially recovered (unaided) from the damage caused. Complete recovery is difficult to judge for the environment, and hence it is suggested that this should be clarified as >80% of the damage.

There are no obvious time criteria to apply to groundwater bodies or drinking water sources. In this case, Table 2 effectively reduces the tolerability of affecting a drinking water source compared with non-drinking water groundwater bodies.

The time specified for long and very long term harm durations are stated as guides to help assess potential recovery time if the impact to the receptor was left to natural recovery alone. Consider the mechanisms that could influence this, such as (weathering, natural bio-remediation or breakdown and replenishment through flushing, dilution etc.) and if these alone could achieve the natural recovery in this specified time.

CDOIF

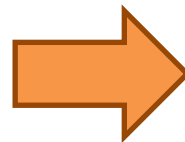
Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 3 - Method and Matrix for Deriving Receptor Tolerability for MATTE (based on unmitigated consequence)

- 1 Identify scenario and receptor affected.
- 2 Select Harm Severity Level (Table 1)
- 3 Select Duration / Recovery Category (Table 2)
- 4 Apply to Tolerability Assessment Matrix to determine tolerability boundaries.

Severity of Harm	4		C	D	D
	3		B	C	D
	2		A	B	C
	1		Sub-MATTE Harm		
		1	2	3	4
		Harm Duration Category			



Frequency at which the CDOIF consequence level is reached or exceeded	Frequency per receptor per establishment per year	
	Intolerable (greater than)	Broadly Acceptable (less than)
A	1.0 E-02	1.0 E-04
B	1.0 E-03	1.0 E-05
C	1.0 E-04	1.0 E-06
D	1.0 E-05	1.0 E-07

Appendix 5 – Tables to assess MATTE potential

Table 1 – MATTE Potential Summary Matrix

Row	DETR Table Ref	Receptor Type	MATTE threshold	Substance / group of substances (see table 4 of Appendix 5 for description of substances or substance groups)										
		See Table 2 of Appendix 5 for receptor detail	See Table 3 of Appendix 5 for description of identified MATTE scenarios	1	2	3	4	5	6	7	Etc.	Etc.		
1	1	Designated Land/Water Sites (Nationally important)	>0.5ha or 10-50%											
2	2	Designated Land/Water Sites (Internationally important)	>0.5ha or 5-25% (5-25% LF/Pop)											
3	3	Other designated Land	10-100ha or 10-50%											
4	4	Scarce Habitat	2-20 ha or 10-50%											
5	5a	Widespread Habitat - Non-designated Land	>10ha											
6	5b	Widespread Habitat - Non-designated Water	Contamination of aquatic habitat which prevents fishing or aquaculture or renders is inaccessible to the public.											

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Substance / group of substances (see table 4 of Appendix 5 for description of substances or substance groups)										
		See Table 2 of Appendix 5 for receptor detail	See Table 3 of Appendix 5 for description of identified MATTE scenarios	1	2	3	4	5	6	7	Etc.	Etc.		
7	6	Groundwater Body - Source Protection Zone (SPZ) for Public Drinking Water Supplies (Note - refer to EA website for SPZ aquifer maps.)	>1ha SPZ or >1000 person-hours interruption											
8	6	Groundwater Body (non-SPZ)	>1ha											
9	6	Groundwater (non-groundwater body wrt Water Framework Directive)	Please indicate if non groundwater body is a pathway to another receptor.											
10	7	Soil or sediment (i.e. as receptor rather than purely a pathway)	>10ha Contamination leading to environmental damage (as per ELD), or significantly affecting overlying water quality.											
11	8	Built environment	Damage above a level at which designation of importance would be withdrawn.											

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Substance / group of substances (see table 4 of Appendix 5 for description of substances or substance groups)									
		See Table 2 of Appendix 5 for receptor detail	See Table 3 of Appendix 5 for description of identified MATTE scenarios	1	2	3	4	5	6	7	Etc.	Etc.	
12	9	Various receptors. Not used to identify and assess MATTE.											
13	10	Particular species (Note - these criteria apply nationally - i.e. England, Wales, Scotland)	Loss of >1% of animal or >5% of plant ground cover in a habitat.										
14	11	Marine	>2ha littoral or sub-littoral zone, >100ha of open sea benthic community, >100 dead sea birds (>500 gulls), >5 dead/significantly impaired sea mammals										
15	12	Fresh and estuarine water habitats	WFD Chemical or ecological status lowered by one class for >2km of watercourse or >10% area (estuaries or ponds) or >2 ha of estuaries and >2ha of ponds. Plus interruption of drinking water supplies, as per DETR Table 6										

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 2 – Receptor Detail

Row	DETR Table Ref	Receptor Type	MATTE threshold	Receptor Detail
1	1	Designated Land/Water Sites (Nationally important)	>0.5ha or 10-50%	
2	2	Designated Land/Water Sites (Internationally important)	>0.5ha or 5-25% (5-25% LF/Pop)	
3	3	Other designated Land	10-100ha or 10-50%	
4	4	Scarce Habitat	2-20ha or 10-50%	
5	5a	Widespread Habitat - Non-designated Land	>10ha	
6	5b	Widespread Habitat - Non-designated Water	>10ha	
7	6	Groundwater Body - Source Protection Zone (SPZ) for Public Drinking Water Supplies (Note - refer to EA website for SPZ aquifer maps.)	>1ha SPZ or >1000 person-hours interruption	
8	6	Groundwater Body (non-SPZ)	>1ha	
9	6	Groundwater (non-groundwater body wrt Water Framework Directive)	Please indicate if non groundwater body is a pathway to another receptor.	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Receptor Detail
10	7	Soil or sediment (i.e. as receptor rather than purely a pathway)	Contamination leading to environmental damage (as per ELD), or significantly affecting overlying water quality.	
11	8	Built environment	Damage above a level at which designation of importance would be withdrawn.	
12	9	Various receptors. Not used to identify and assess MATTE.		
13	10	Particular species (Note - these criteria apply nationally - i.e. England, Wales, Scotland)	Loss of >1% of animal or >5% of plant ground cover in a habitat.	
14	11	Marine	>2ha littoral or sub-littoral zone, >100ha of open sea benthic community, >100 dead sea birds (>500 gulls), >5 dead/significantly impaired sea mammals	

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Receptor Detail
15	12	Fresh and estuarine water habitats	WFD Chemical or ecological status lowered by one class for >2km of watercourse or >10% area (estuaries or ponds) or >2 ha of estuaries and >2ha of ponds. Plus interruption of drinking water supplies, as per DETR Table 6	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 3 – MATTE Scenarios

Row	DETR Table Ref	Receptor Type	MATTE threshold	Credible MATTE Scenarios
1	1	Designated Land/Water Sites (Nationally important)	>0.5ha or 10-50%	
2	2	Designated Land/Water Sites (Internationally important)	>0.5ha or 5-25% (5-25% LF/Pop)	
3	3	Other designated Land	10-100ha or 10-50%	
4	4	Scarce Habitat	2-20 ha or 10-50%	
5	5a	Widespread Habitat - Non-designated Land	>10ha	
6	5b	Widespread Habitat - Non-designated Water	>10ha	
7	6	Groundwater Body - Source Protection Zone (SPZ) for Public Drinking Water Supplies (Note - refer to EA website for SPZ aquifer maps.)	>1ha SPZ or >1000 person-hours interruption	
8	6	Groundwater Body (non-SPZ)	>1ha	
9	6	Groundwater (non-groundwater body wrt Water Framework Directive)	Please indicate if non groundwater body is a pathway to another receptor.	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Credible MATTE Scenarios
10	7	Soil or sediment (i.e. as receptor rather than purely a pathway)	Contamination leading to environmental damage (as per ELD), or significantly affecting overlying water quality.	
11	8	Built environment	Damage above a level at which designation of importance would be withdrawn.	
12	9	Various receptors. Not used to identify and assess MATTE.		
13	10	Particular species (Note - these criteria apply nationally - i.e. England, Wales, Scotland)	Loss of >1% of animal or >5% of plant ground cover in a habitat.	
14	11	Marine	>2ha littoral or sub-littoral zone, >100ha of open sea benthic community, >100 dead sea birds (>500 gulls), >5 dead/significantly impaired sea mammals	

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Row	DETR Table Ref	Receptor Type	MATTE threshold	Credible MATTE Scenarios
15	12	Fresh and estuarine water habitats	WFD Chemical or ecological status lowered by one class for >2km of watercourse or >10% area (estuaries or ponds) or >2 ha of estuaries and >2ha of ponds. Plus interruption of drinking water supplies, as per DETR Table 6	

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 4 – Dangerous Substances with Environmental Risk

Part 1 - Substance List

Substance Reference	Substance (or group of substances)					Maximum Inventory (tonnes)	Description	Physical State	Quantity	Ref for further info (e.g. SR section...)
	Common name	IUPAC Name	CAS Number	CHIP Index	Risk Phases					
1										
2										
3										
4										
5										
6										
7										
Etc.										
Etc.										

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Part 2 - Chemical Hazards

Substance Reference	A	B	C	D	E	F	G	Etc.	Etc.
Explosion/Flammability Hazards									
<i>Fire</i>									
<i>Deflagration/Detonation</i>									
<i>Electrical Static</i>									
Reactivity/Stability Hazards									
Immediate Health Hazards									
<i>Inhalation Toxicity</i>									
<i>Other Toxicity</i>									
<i>Irritant/Corrosive</i>									
<i>Sensitizer</i>									
Long Term or Delayed Health Hazards									
<i>Chronic Health Hazards</i>									
<i>Radiation</i>									
Nuisance									
<i>Odour</i>									
Environmental Hazards									
<i>Aqueous</i>									
<i>Gaseous</i>									
<i>Ground</i>									
Hazardous Breakdown Products									

CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Human Factors Review of Procedures

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members this guideline on completing a human factors review of procedures.

The intent of this document is to provide a reference for those organisations completing a human factors review of procedures.

It is not the intention of this document to replace any existing corporate policies or processes. The intent is to provide a reference to users to help in planning and completing the human factors review.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to human factors review of procedures.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Human Factors Review of Procedures".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

It should be understood that this document does not explore all possible options for completing human factors review, nor does it consider individual site requirements, policies or procedures – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

1.	EXECUTIVE SUMMARY.....	4
2.	PURPOSE AND SCOPE.....	5
2.1	Competency requirements.....	5
2.2	Using this guidance	5
3.	ASSESSMENT FRAMEWORK.....	7
3.1	Definition of terms.....	7
3.2	Framework for assessment	9
3.3	Safety critical task definition and selection.....	11
4.	ASSESSMENT FRAMEWORK STEPS – SAFETY CRITICAL TASKS	13
4.1	Identify procedures for further assessment.....	13
4.2	Identify safety critical tasks from within the procedure	14
4.3	Conduct task analysis.....	15
4.4	Complete human failure analysis and determine what credible human failures could occur	16
4.5	Review existing safe-guards that could prevent the human failure.....	18
4.6	Determine opportunities for recovery	19
4.7	Recommend additional safeguards	20
5.	REFERENCE DOCUMENTS	22
	Abbreviations.....	23
	Acknowledgements	24
	Revision History.....	25
	Appendix 1 – Example key words for Human Failure Analysis.....	26
	Appendix 2 – Example human failure types	28
	Appendix 3 – Example Performance Influencing Factors.....	30
	Appendix 4 – Example qualitative task analysis sheet	31
	Appendix 5 – Worked example	34

1. EXECUTIVE SUMMARY

Several incidents in recent years have highlighted the importance of procedures - ensuring procedures are fit for purpose and take adequate account of what people are required to do as part of a potentially hazardous activity is critical in reducing risks to both people and the environment.

The final report of the Process Safety Leadership Groups (PSLG) safety and environmental standards for fuel storage sites was published in December 2009, Appendix 5 gives some guidance on the management of operations and human factors, and further detailed guidance is available from both the Health and Safety Executive (HSE) and the Energy Institute (EI) as well as other sources (Refer to section 5, other relevant publications).

However, applying Human Factors (HF) as part of the review process for procedures has in some cases been difficult for duty holders to put into practice in a resource efficient way. This has led to instances whereby systems have been created that are burdensome to implement and difficult to maintain.

As part of its role to deliver improvements in health, safety and the environment, the CDOIF Process Safety Work-stream agreed to develop high level guidance that is concise, practical and flexible to allow duty holders to carry out a review of HF as applied to procedures. The guidance is intended to be at a sufficiently high level to enable non-HF specialists to complete a review, but also sign-post to more detailed guidance where appropriate.

2. PURPOSE AND SCOPE

The purpose of this document is to provide a high level guide to help the reader understand how to review and evaluate potential HF failures that could affect both safety and environmental risks. The guidance addresses both safety critical and non-safety critical activities, and both preventative and mitigatory barriers. It is the intention of this guidance to review existing procedures, and not to determine if those existing procedures are sufficient, unless a gap is identified as part of the HF review process.

Procedures control the activities that a person carries out, however procedures are written for many different purposes, not only related to the safe operation of process plant. In the context of this guidance, the HF review of procedures relates specifically to:

- Operating Procedures (e.g. site start-up, shutdown)
- Inspection and Maintenance Procedures
- Emergency Procedures

Work processes such as Human Resource procedures are not included within the scope of this review.

Whilst this guidance is primarily written for top tier COMAH (Control of Major Accident Hazard) sites, it may also provide a useful reference for lower tier and sub COMAH sites.

The following sections provide a high level framework for assessing the HF component of procedures. Other techniques are available, and reference should also be made to the other relevant publications listed.

2.1 Competency requirements

When completing a HF review of procedures there is a need to ensure that relevant competent resources are used throughout the process. In the context of this guidance, it is likely that those with knowledge of process safety and risk assessment will be needed to help identify safety critical tasks. Similarly it is likely that those with knowledge of HF will be involved with the identification of procedures, tasks, task steps and credible human failures.

Refer to section 4.4 of this guidance for further information relating to competency requirements.

2.2 Using this guidance

Figure 1 below provides a reference to the assessment process, and the relevant sections within this guidance.

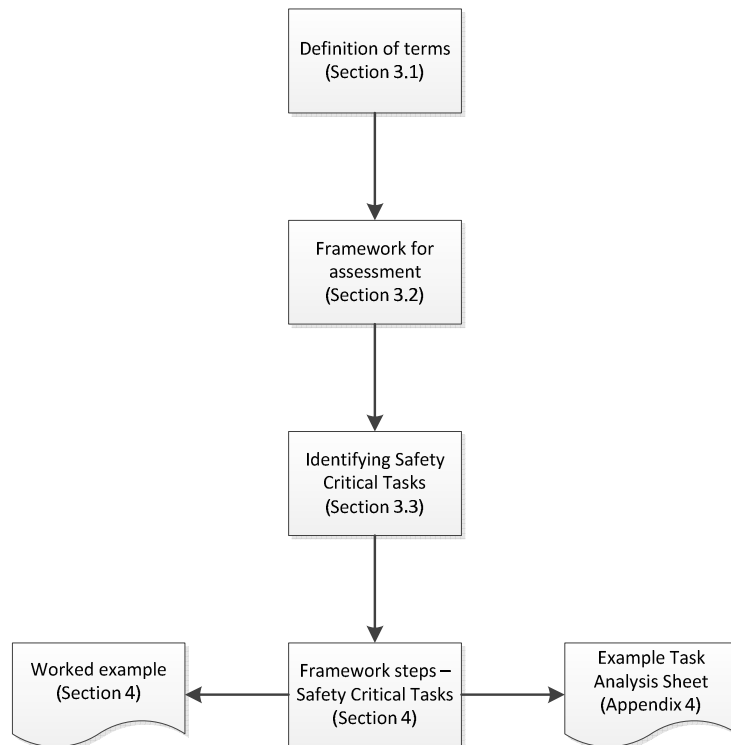


Figure 1 – Using this guidance

3. ASSESSMENT FRAMEWORK

A safety critical measure is a course of action taken (human, mechanical, electrical or otherwise) that if carried out incorrectly, may result in a major accident.

In more specific terms various measures can be defined as:

1. A *Safety Critical Activity*, a process control which can be subdivided into *Procedures* and *Tasks* (e.g. Import Control)
2. A *Safety Critical Procedure*, a defined series of steps or individual *Safety Critical Tasks* which can be further sub-divided into individual *Safety Critical Task Steps*.

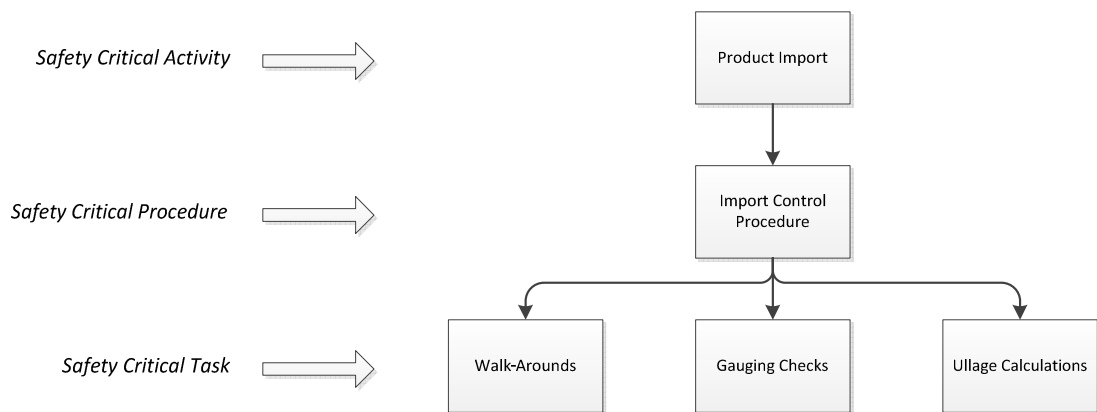


Figure 2 – Safety Critical Activities, Procedures and Tasks

The following provides a framework by which Safety Critical Activities, Procedures and Tasks can be identified and assessed.

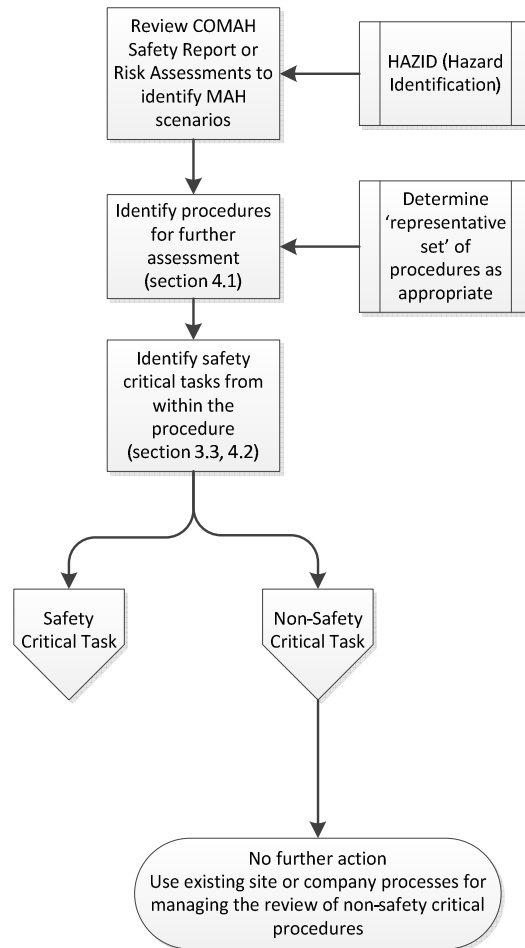
3.1 Definition of terms

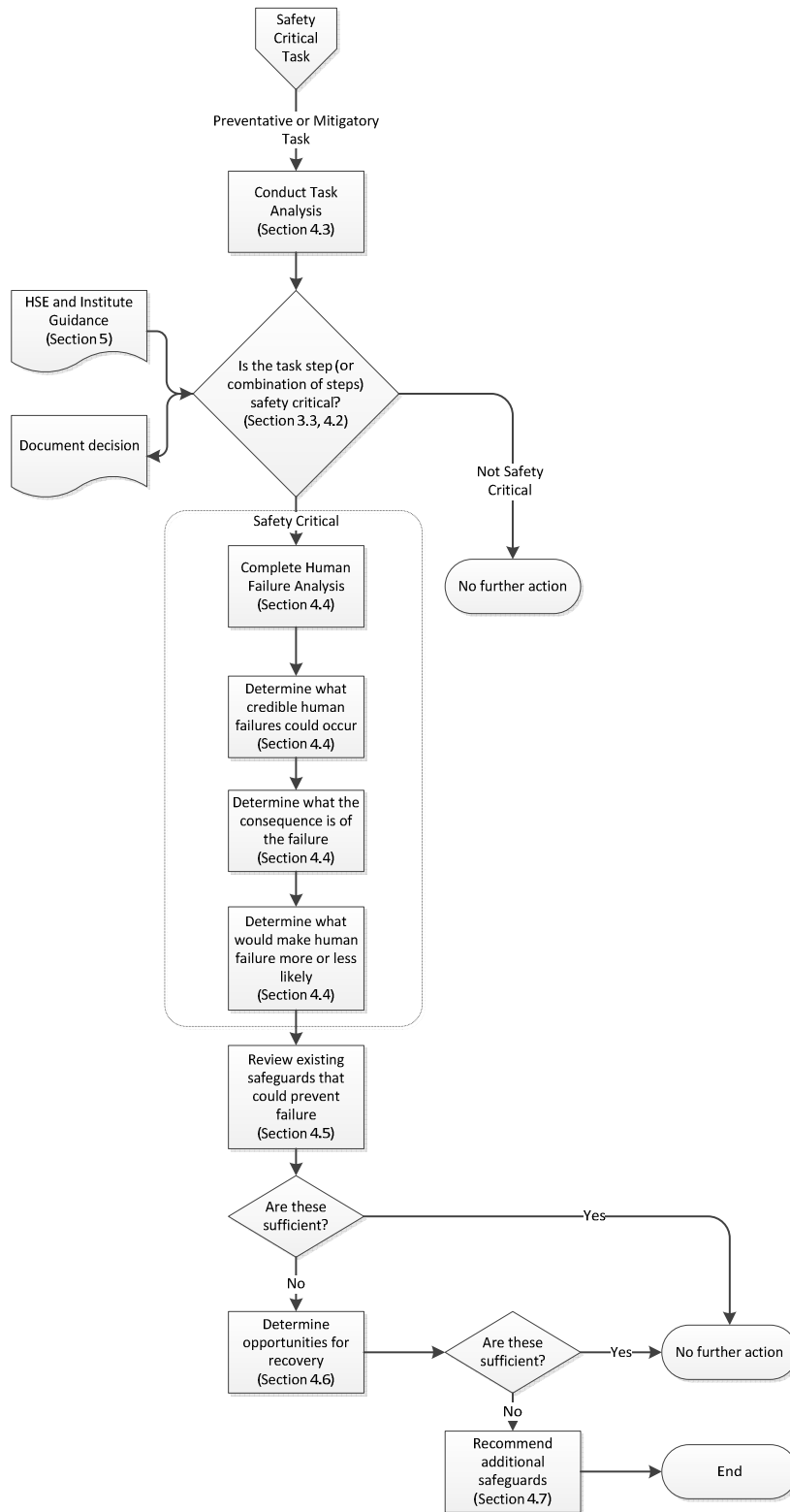
There are four key terms used in this guidance to discuss each of the elements that a procedure comprises of, these are:

- **Procedure** – the overall operation that is being controlled, for example
 - Loading a road tanker with gasoline
 - Starting a Crude Distillation Unit (CDU)
 - Performing scheduled maintenance on a pump
- **Task** – the ‘human’ contribution to the **Procedure**, for example
 - Positioning the road tanker at the loading gantry

- Start-up fired heater
- Performing mechanical isolation
- **Task Steps** – the ‘human’ contribution to the **Task**, for example
 - Applying the parking brake on a road tanker
 - Commission pilots to fired heater
 - Close outlet valve from the pump
- **Credible Human Failure** – Failure of an action by the ‘human’ such that the **Task Step** is not completed correctly, for example
 - Product left on board in tanker compartment prior to loading activity, leading to a probe hit or potential overfill
 - Omitted to commission pilot on fired heater
 - Outlet valve on the wrong pump closed

3.2 Framework for assessment





3.3 Safety critical task definition and selection

A Safety Critical Task is any task where human failure could potentially *initiate, prevent, escalate* or fail to *mitigate* a major accident with consequences that are greater than the specified threshold for the site or company.

For example:

Initiate – a valve is left open which leads to a loss of containment

Prevent – An individual fails to respond to an alarm

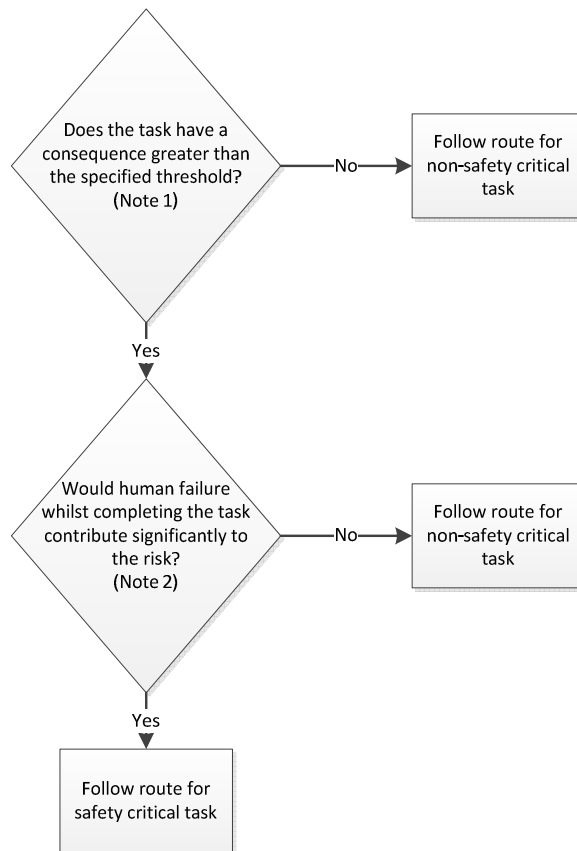
Escalate – Drenching system failed to operate due to poor maintenance

Mitigate – An individual fails to activate the emergency plan for the site or process unit

When determining the failures that could occur, the following are all of relevance:

- Inaction, the task was not completed
- Action (either a physical or mental action), the task was not completed correctly
- Time, the task was completed at the wrong time, or for the wrong duration

The following flowchart can be used as a simple tool to help in determining whether or not a task is safety critical:



Note 1: The specified threshold will be site/corporate based, and should be linked to the Major Accident definition with the COMAH safety regulations

Note 2: Does the task involve breaking of containment which could lead to a Major Accident Hazard (MAH)? For example taking samples, hot-work on pipes, preparing equipment for maintenance, water draws or filter changes.

Alternatively, does the task directly involve the management of safety critical equipment? For example, proof test of a Safety Instrumented System (SIS) or maintenance of a Pressure Relief Valve (PRV).

4. ASSESSMENT FRAMEWORK STEPS – SAFETY CRITICAL TASKS

The following provides an overview of the process to be followed when completing each of the assessment framework steps for safety critical tasks.

Note that a worked example for each step is included at the end of each section. The complete worked example is provided in Appendix 5.

4.1 Identify procedures for further assessment

Procedures which are in place to ensure the safe operation of process plant may take many different forms, including:

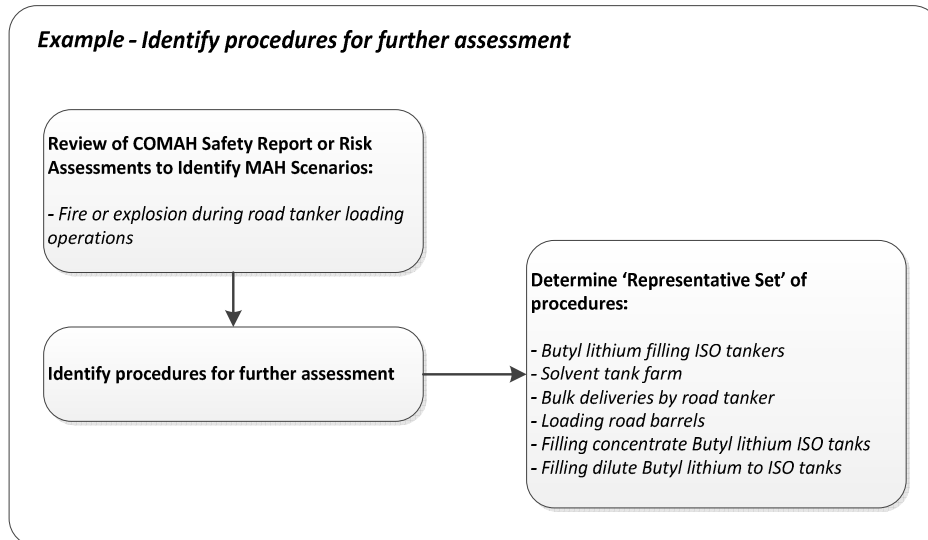
- Operating tasks
- Routine tasks
- Emergency tasks
- Maintenance tasks
- Inspection tasks
- Job/task cards (for example routine tasks, work instructions)

Procedures can be reviewed to determine if any of the **tasks** that they include have the potential to be safety critical. The following methodology can be used to determine which **procedures** should be reviewed:

1. Identify the MAH you have on the site
2. Identify the activities that relate to the MAH (for example Product Import)
3. Identify the **procedures** which relate to those activities
4. Identify those that apply to prevention and mitigation
5. Identify those **procedures** which are common/and can be used as a representative set¹
6. Prioritise those that have the highest risk (for example using a colour code), and complete a detailed assessment of the highest priorities first

¹For example, there are ten similar or common start-up procedures. A detailed assessment of one of these can be completed, and the findings applied to all others, providing the Performance Influencing Factor's (PIFs) are also similar or the same (Refer to section 4.4) – i.e. the same procedure may be used across multiple sites and as the environments are different, so to may be the PIFs.

Example - Identify procedures for further assessment



4.2 Identify safety critical tasks from within the procedure

Prior to identifying safety critical tasks, it is assumed that procedures have been reviewed to ensure that they are an accurate representation of the task(s) to be carried out.

Once relevant **procedures** have been identified (i.e. those that contribute toward the safe operation of the process plant, and have some level of human interaction), it is necessary to determine if there are any **tasks** within those procedures that could be safety critical. Reference can be made to section 3.3 for one methodology that can be used to identify safety critical **tasks**. This methodology asks two questions:

1. Does failure to complete the task have an unmitigated consequence greater than the specified threshold?

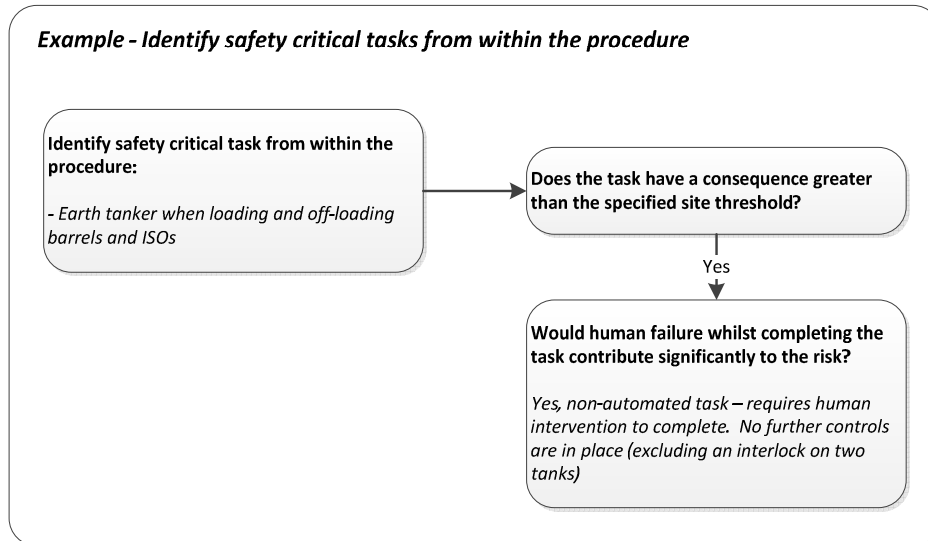
Can human failure whilst performing the task lead directly to the MAH or hazards?

And

2. Would human failure whilst completing the task contribute significantly to the risk?

Does a risk assessment for this scenario require a high degree of certainty that personnel will execute this task flawlessly? This is likely to include those tasks which are identified as the "Last Line of Defence" i.e. those activities where no additional safeguard is in place to prevent one of the consequences above from occurring. If an equipment safeguard is in place (for example, a Pressure Safety Valve, a contained blow down system or an instrumented interlock system) then the task typically would not be a "last line of defence".

If the answer to these two questions is *yes*, then the task is safety critical. However it is worthwhile examining further to see if the **task** can be removed from the **procedure** or the **procedure** can be changed to make the **task** non-safety critical.



4.3 Conduct task analysis

Following the identification of the **procedures** (or representative procedure), and the safety critical **tasks** within those **procedures**, it is necessary to identify the **task steps** that are safety critical as not all steps within a task will be safety critical, and therefore not subject to further investigation.

Examples of human interactions (**task steps**) with a **task** that may require further analysis include:

- Those which have the potential to initiate an event sequence (for example incorrect valve operation causing a loss of containment)
- Those required to stop an event sequence (for example activation of an Emergency Shut Down [ESD] system)
- Those required to initiate an evacuation procedure for the area or the site
- Actions that may escalate an incident (for example inadequate maintenance of a fire control system)

The purpose of this analysis is to identify which of the **task steps**, if carried out incorrectly, in the wrong order or are omitted could result directly to the MAH or hazards identified in section 4.1.

Existing published guidance¹ agrees that as a minimum, an operator responsible for carrying out the **task** should be involved to identify the correct sequence of **task steps**, and the consequences if a **task step** is incorrectly executed. The preferred method of conducting this analysis is to carry out a 'walk through, talk through' with the operator.

If it is not practical to complete a 'live walk through, talk through', for example the **task** is carried out on an infrequent basis; one of the techniques listed below could be used:

- Field simulated walk through/talk through
- Desk top review/talk through

¹Existing published guidance includes (refer also to section 5):

- HSE Core Topic 3: Identifying Human Failures, <http://www.hse.gov.uk/humanfactors/topics/core3.pdf>
- HSE Understanding the task, <http://www.hse.gov.uk/humanfactors/resources/understanding-the-task.pdf>
- HSG48, Reducing Error and Influencing Behaviour, <http://www.hse.gov.uk/pubns/books/hsg48.htm>
- Energy Institute, Guidance on human factors safety critical task analysis

Example – Conduct task analysis

Identify safety critical task step:

*- Earth tanker when loading and off-loading
barrels and ISOs*

4.4 Complete human failure analysis and determine what credible human failures could occur

Once safety critical **task steps** have been identified, it is necessary to complete a human failure analysis (HFA) to determine how failures could occur; in essence an HFA is a Hazard and Operability study (HAZOP) for a human¹.

The following process can be adopted:

1. Determine what failure could occur, using a defined set of keywords (an example is provided in appendix 1)
2. Determine the type of failure that could occur (an detailed example of failure types is provided in appendix 2);
 - a slip error

- a lapse error
 - a mistake
 - a violation
3. Determine the consequences of those failures; refer to section 4.1 above, where the MAH for the site (and thus consequences) are identified.
 4. Identify factors which could make these failures more or less likely (commonly referred to as 'Performance Influencing Factors [PIF] or Performance Shaping Factors [PSF]).
 - PIFs are the characteristics of the job, the individual and the organisation that influence human performance. Optimising PIFs may reduce the likelihood of all types of human failure. A list of common PIF's can be found in the HSE publication 'Performance Influencing Factors', <http://www.hse.gov.uk/humanfactors/topics/pifs.pdf> (also included in Appendix 3 for reference).

¹ A record of the analysis results should be kept as part of the analysis process

To ensure the effectiveness of the HFA, the team assembled to complete the analysis should include as a minimum:

- HFA leader, competent² in the use of the *qualitative* or *quantitative* assessment techniques (see below)
- The person or persons who carries out the task (for example the operator, maintenance technician)

² The duty holder should define and be able to demonstrate the necessary competency requirements for this person.

When completing the HFA, either a *Qualitative* or *Quantitative* approach can be taken. In general a qualitative approach should be taken; where a more detailed analysis is required a quantitative approach may be considered.

Qualitative

From the information collected as part of the process above, a qualitative approach can be taken to analyse this data and identify potential. An example methodology for completing this analysis is included in appendix 4, however many different approaches are available.

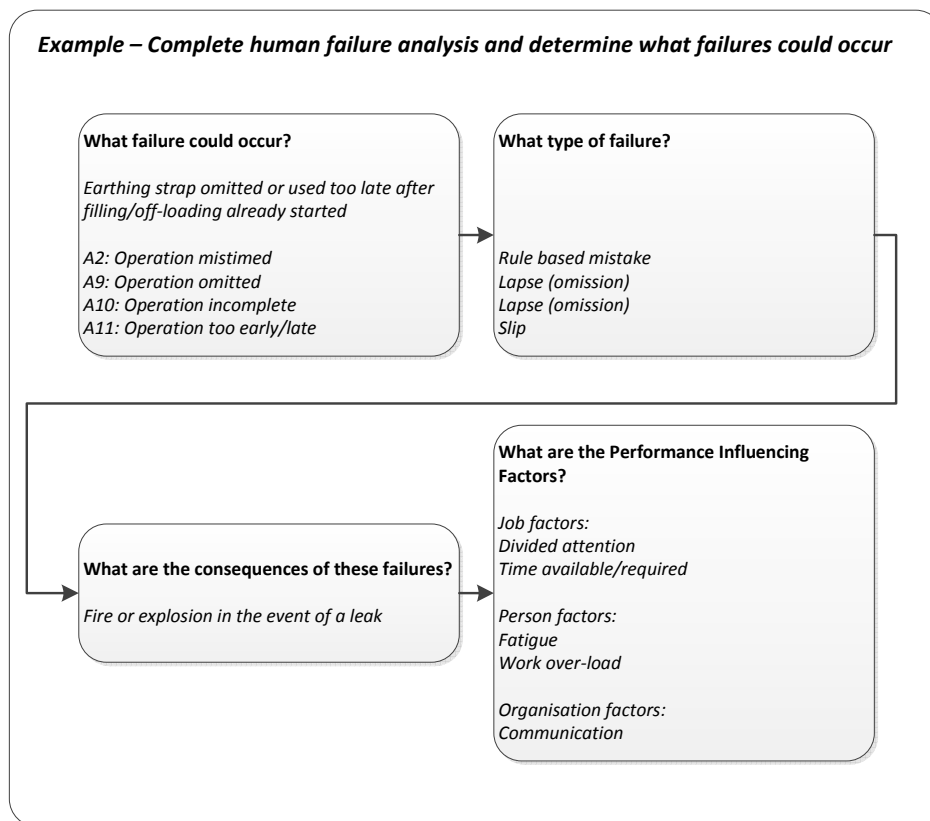
Quantitative

Where further detailed analysis is required, site operators may wish to use a validated Quantitative Human Reliability Assessment (QHRA) ³ to quantify the probability of human failure. The following tools are commonly used:

- Human Error Analysis and Reduction Technique (HEART)
- Technique for Human Error Rate Prediction (THERP)

Use of these techniques can provide Human Error Probabilities (HEPs) which can be used to inform quantitative risk assessment, Layers of Protection Analysis (LOPA), Safety Integrity Level (SIL) determinations and As Low as Reasonably Practicable (ALARP) demonstrations. These tools can be helpful in evaluating the benefit of taking additional measures to reduce human error, but should only be applied by a suitably competent person.

³ Further information on QHRA can be found in the Energy Institute publication 'Guidance on quantified human reliability analysis (QHRA)', <http://www.energyinst.org/technical/human-and-organisational-factors/qhra>



4.5 Review existing safe-guards that could prevent the human failure

In sections 4.4 and 4.5 the failures, type of failure, and the factors which influence that failure (PIF) have been identified. The next step is to determine what existing controls and safe-guards are already in place which may address each of the PIFs.

Following this analysis, those PIFs that do not have existing controls, weak controls that could be improved or safeguards will be identified.

Example – Review existing safeguards that could prevent the human failure

Measures to prevent the failure from occurring:

- Detailed procedures with Safety Critical task highlighted
- MAH scenario signage at earth point
- Earthing strap permanently fixed to plant
- Multiple and well positioned earth straps in place to avoid violation apathy

Measures to address PIFs:

*Divided attention; Time available/required;
Work overload;
May be distracted by other deliveries/
activities. Planning system includes dispatch
cover for offloading/loading activities. Shift
pattern allows for holiday/sickness cover.*

Communication:

*Planning system alerts technicians to activities
for the week ahead with additional daily
despatches to account for changes/additional
deliveries. Offloading check sheet and
handover log completed to communicate to
oncoming shift.*

4.6 Determine opportunities for recovery

Not all human failures will lead to an undesirable consequence. There may be opportunities for recovery before reaching the consequence. It is important to take recovery from errors into account in the assessment. A recovery process generally follows three stages:

1. Detection of the error
2. Diagnosis of what went wrong and how
3. Correction of the problem.

Example – Determine opportunities for recovery

Potential to recover (from the failure before the consequence occurs):

- Tank has interlock system ensuring earthing continuity
- Off-loading checklist including earth confirmation
- Operation completed with ADR qualified driver present

4.7 Recommend additional safeguards for preventing failure or improving recovery

Section 4.5 and 4.6 identified those PIF's for failure types that already have appropriate controls and safe-guards in place or have opportunities for recovery. For the remaining PIF's, consider what additional safeguards or recovery steps can reasonably¹ be implemented to mitigate the effect of the PIF, this may include:

Technical

- Removing human interaction by automating the process, e.g. introduce automatic loading shutdown in the event of a meter overrun to remove driver monitoring and manual intervention.
- Consider use of new signage or improving existing signs/ labels, e.g. improving valve labelling to ensure operator doesn't open incorrect valve by mistake.

Procedural

- Ensure safety critical steps are clearly identified and highlighted to those who carry out the tasks.
- For those tasks identified as safety critical, consider the use of job aids with detailed information of risks, minimum controls and potential human failures. E.g. breaking containment job aid, critical safety system maintenance.

Behavioural

- Introduce robust processes to maintain competency and compliance to procedures, e.g. competency checks for safety critical tasks.
- Introduce independents check at critical tasks, e.g. second permit to work authority verifies permit before issuing.

If the risk of the PIF for the task step cannot be mitigated, reference should be made to the risk assessment for the MAH to see where additional risk reduction measures can be introduced¹.

¹ Any further risk reduction measures should be subject to the ALARP principle.

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Example – Recommended additional safeguards

Measures to reduce the consequence/failure:

Consider expansion of earthing continuity protection system to all offloading points

Change laboratory offloading procedure to include independent check/confirmation of earthing in place

Task currently completed by self-managing team. Frequency of supervision checks/ presence in area to be increased including checks of safety critical tasks

5. REFERENCE DOCUMENTS

Further information relating Human Factors analysis can be found in the following publications

1. Process Safety Leadership Group, final report – Safety and Environmental Standards for Fuel Storage Sites
2. HSE, Core Topic 3: Identifying Human Failures
3. HSE, Understanding the task
4. HSE, Performance Influencing Factors
5. HSG48, Reducing Error and Influencing Behaviour
6. Energy Institute, Guidance on human factors safety critical task analysis
7. Energy Institute, Guidance on quantified human reliability analysis (QHRA)

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Abbreviations

Abbreviation	Description
ALARP	As Low as Reasonably Practicable
CDOIF	Chemical and Downstream Oil Industry Forum
CDU	Crude Distillation Unit
COMAH	Control of Major Accident Hazards
EI	Energy Institute
ESD	Emergency Shut Down
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study
HEART	Human Error Analysis and Reduction Technique
HF	Human Factors
HFA	Human Failure Analysis
HSE	Health and Safety Executive
LOPA	Layer of Protection Analysis
MAH	Major Accident Hazard
PIF	Performance Influencing Factor
PPE	Personal Protective Equipment
PRV	Pressure Relief Valve
PSF	Performance Shaping Factors
PSLG	Process Safety Leadership Group
QHRA	Quantitative Human Reliability Assessment
SIL	Safety Integrity Level
SIS	Safety Instrumented System
THERP	Technique for Human Error Rate Prediction
UK	United Kingdom
UKPIA	United Kingdom Petroleum Industry Association

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industries Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
David Smith (Chair)	Murco Petroleum Ltd
Barrie Salmon	Tank Storage Association
Chris Simes	Valero UK Ltd
Doug Leech	Chemical Business Association
James Greenhalgh	Valero UK Ltd
Karen Inchley	Essar Oil (UK) Ltd
Linda Dixon	Valero UK Ltd
Morven Ozanne	FMC Chemicals Ltd, representing the Chemical Industries Association
Nigel Collison	BP
Paul Kenny	Esso Petroleum Company Ltd
Peter Davidson	United Kingdom Petroleum Industry Association
Peter Hill	Total Lindsey Oil Refinery Ltd
Peter Jefferies	Phillips 66
Pippa Brockington	Health and Safety Executive
Stuart Duncan	Petrolneos Manufacturing Scotland Ltd
Vitor Monteiro	BP Oil UK Ltd

CDOIF

**Chemical and Downstream Oil
Industries Forum**

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Revision History

Rev.	Section	Description	Date	Changed By
0.0	All	First Issue	05-Jul-2013	Peter Davidson
0.1	All	Updated following working group comments	10-Jul-2013	Peter Davidson
0.2	All	Final comments from working group incorporated	01-Aug-2013	Peter Davidson
0.3	All	Stakeholder comments incorporated	20-Sep-2013	Peter Davidson

Appendix 1 – Example key words for Human Failure Analysis

Action Errors

- A1 Operation too long / short
- A2 Operation mistimed
- A3 Operation in wrong direction
- A4 Operation too little / too much
- A5 Operation too fast / too slow
- A6 Misalign
- A7 Right operation on wrong object
- A8 Wrong operation on right object
- A9 Operation omitted
- A10 Operation incomplete
- A11 Operation too early / late

Checking Errors

- C1 Check omitted
- C2 Check incomplete
- C3 Right check on wrong object
- C4 Wrong check on right object
- C5 Check too early / late

Information Retrieval Errors

- R1 Information not obtained
- R2 Wrong information obtained
- R3 Information retrieval incomplete
- R4 Information incorrectly interpreted

Information Communication Errors

- I1 Information not communicated
- I2 Wrong information communicated
- I3 Information communication incomplete
- I4 Information communication unclear

Selection Errors

- S1 Selection omitted
- S2 Wrong selection made

Planning Errors

- P1 Plan omitted
- P2 Plan incorrect

Violations

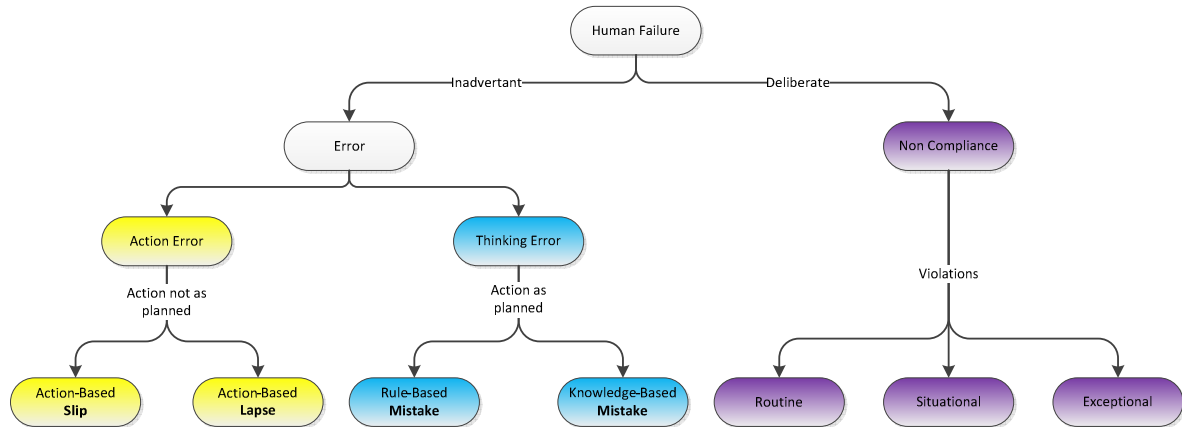
- V1 Deliberate actions

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 2 – Example human failure types



	Characteristics	Failure Type	Examples	Typical Control Measures
Skill-based errors	Associated with familiar tasks that require little conscious attention. These 'skill-based' errors occur if attention is diverted, even momentarily. Resulting action is not intended: 'not doing what you meant to do'. Common during maintenance and repair activities.	Slip (Commission)	A simple, frequently-performed physical action goes wrong: <ul style="list-style-type: none"> put on indicators instead of operating windscreen wash/wipe function move a switch up rather than down (wrong action on right object) take reading from wrong instrument (right action on wrong object) transpose digits during data input into a process control interface 	<ul style="list-style-type: none"> human-centred design (consistency e.g. up always means off; intuitive layout of controls and instrumentation; level of automation etc.) checklists and reminders; procedures with 'place markers' (tick off each step) independent cross-check of critical tasks (PTW) removal of distractions and interruptions sufficient time available to complete task warnings and alarms to help detect errors often made by experienced, highly-trained, well-motivated staff: <u>additional training not valid</u>
		Lapse (Omission)	Short-term memory lapse; omit to perform a required action: <ul style="list-style-type: none"> forget to indicate at a road junction medical implement left in patient after surgery miss crucial step, or lose place, in a safety-critical procedure drive road tanker away, after bulk delivery, with hose still connected 	
Rule based errors	Decision-making failures; errors of judgement (involve mental processes linked to planning; info. gathering; communication etc.) Action is carried out,	Rule-Based Mistake	If behaviour is based on remembered rules and procedures, mistake occurs due to mis-application of a good rule or application of a bad rule: <ul style="list-style-type: none"> misjudge overtaking manoeuvre in unfamiliar, under-powered car assume £20 fuel will last a week but fail to account for rising prices ignore alarm in real emergency, following history of spurious alarms 	<ul style="list-style-type: none"> plan for all relevant 'what ifs' (procedures for upset, abnormal and emergency scenarios) regular drills/exercises for upsets/emergencies clear overview / mental model (clear displays; system feedback; effective shift handover etc.)

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

	Characteristics	Failure Type	Examples	Typical Control Measures
Knowledge based errors	as planned, using conscious thought processes, but wrong course of action is taken: <i>'do the wrong thing believing it to be right'</i>	Knowledge-Based Mistake	Individual has no rules or routines available to handle an unusual situation: resorts to first principles and experience to solve problem: <ul style="list-style-type: none"> rely on out-of-date map to plan unfamiliar route misdiagnose process upset and take inappropriate corrective action (due to lack of experience or insufficient / incorrect information etc.) 	<ul style="list-style-type: none"> diagnostic tools and decision-making aids (flow-charts; schematics; job-aids etc.) competence (knowledge and understanding of system; training in decision-making techniques) organisational learning (capture and share experience of unusual events)
Violations	<p>Deliberate deviations from rules, procedures, regulations etc. Also known as 'non-conformance'.</p> <p>Knowingly take short cuts, or fail to follow procedures, to save time or effort.</p> <p>Usually well-meaning, but misguided (often exacerbated by unwitting encouragement from management for 'getting the job done').</p>	<p>Routine</p> <p>Situational</p> <p>Exceptional</p> <p>Optimising</p>	<p>Non-compliance becomes the 'norm'; general consensus that rules no longer apply; characterised by a lack of meaningful enforcement:</p> <ul style="list-style-type: none"> high proportion of motorists drive at 80mph on the motorway PTWs routinely authorised without physical, on-plant checks <p>Non-compliance dictated by situation-specific factors (time pressure; workload; unsuitable tools & equipment; weather); non-compliance may be the only solution to an impossible task:</p> <ul style="list-style-type: none"> van driver has no option but to speed to complete day's deliveries <p>Person attempts to solve problem in highly unusual circumstances (often if something has gone wrong); takes a calculated risk in breaking rules:</p> <ul style="list-style-type: none"> after a puncture, speed excessively to ensure not late for meeting delay ESD during emergency to prevent loss of production <p>A person seeks to improve their experience or perception of a monotonous task by changing the way they carry it out:</p> <ul style="list-style-type: none"> Operatives compete to see how quickly they can carry out a task over-riding safety measures to increase speed 	<ul style="list-style-type: none"> improve risk perception; promote understanding and raise awareness of 'whys' & consequences (e.g. warnings embedded within procedures) increase likelihood of getting caught effective supervision reward compliance and investigate reasons for non-compliance; eliminate reasons to cut corners (poor job design; inconvenient requirements; unnecessary rules; unrealistic workload and targets; unrealistic procedures; adverse environmental factors) improve attitudes / organisational culture (active workforce involvement; encourage reporting of violations; make non-compliance 'socially' unacceptable e.g. drink-driving).

Appendix 3 – Example Performance Influencing Factors

Job factors

Clarity of signs, signals, instructions and other information
System/equipment interface (labelling, alarms, error avoidance/ tolerance)
Difficulty/complexity of task
Routine or unusual
Divided attention
Procedures inadequate or inappropriate
Preparation for task (e.g. permits, risk assessments, checking)
Time available/required
Tools appropriate for task
Communication, with colleagues, supervision, contractor, other
Working environment (noise, heat, space, lighting, ventilation)

Person factors

Physical capability and condition
Fatigue (acute from temporary situation, or chronic)
Stress/morale
Work overload/underload
Competence to deal with circumstances
Motivation vs. other priorities

Organisation factors

Work pressures e.g. production vs. safety
Level and nature of supervision / leadership
Communication
Manning levels
Peer pressure
Clarity of roles and responsibilities
Consequences of failure to follow rules/procedures
Effectiveness of organisational learning (learning from experiences)
Organisational or safety culture, e.g. everyone breaks the rules

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 4 – Example qualitative task analysis sheet

Table 1 Instructions

Task Step Description	Likely Human Failure	Is it a Slip, Lapse, Mistake or Violation	Potential Consequence	Performance Influencing Factors (PIF's)	Potential to Recover From Human Failure	Measures to Prevent Failure	Measures to Reduce the Consequence
Task steps taken from procedures. Walk through with shift controller	This column records the types of human error that are considered possible for this task step. Note there may be more than one type of error. Use the error codes to determine the error type. Use the error codes listed on the error code tab below for a list of all error types and their coding	Use the human failure sheet to assess the human failure type. This may be a mistake or a violation. It is important to determine this as it will have a direct impact on the solution.	This column records the consequences that may occur as a result of the human failure described in the previous columns. Use the risk matrix to determine the level of risk	This column records any factors which may have an influence on the operator's ability to undertake the task. This may include fatigue, weather conditions, distractions, workload etc. Use the PIF's detailed on the PIF tab below for a comprehensive list of PIF's.	Not all human failures will lead to an undesirable consequence. There may be opportunities for recovery before reaching the consequence detailed in the next column. It is important to take recovery from errors into account in the assessment. A recovery process generally follows three stages:- detection of the error, diagnosis of what went wrong and how, correction of the problem	List practical suggestions on how to prevent the error from occurring in this column. This may include changes to procedures, training, engineering modifications	This column details suggestions as to how the consequences of an incident may be reduced or the recovery potential increased should a failure occur

Review the task criticality / frequency and complexity, using table 3	If procedural support is not available in the recommended format then this issue must be addressed
-----------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

Note: For Human Failure types refer to Appendix 2. For Performance Influencing factors refer to Appendix 3.

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 2 Task Sheet

Task Observed _____

Date _____

Observed by:- _____

Human Factors Analysis of Current Situation							Additional Measures to Deal With Human Factor Issues		
Step number	Task Step Description	Likely Human Failure	Is This a slip, lapse, mistake, or violation	Potential consequence	Performance Influencing Factors (PIF's)	Potential to Recover From Human Failure	Measures to Prevent Failure	Measures to Reduce the Consequence	Comments

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Table 3 Procedural Support

Task Criticality		Low			Medium			High		
Task Familiarity		Freq	Infreq	Rare	Freq	Infreq	Rare	Freq	Infreq	Rare
Task Complexity	Low	Green	Green	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Red
	Medium	Green	Yellow	Yellow	Yellow	Yellow	Red	Yellow	Red	Red
	High	Yellow	Yellow	Red	Yellow	Red	Red	Red	Red	Red

No Written Instructions Required
Job Aid Required i.e. Checklist
Step By Step Instructions Required

CDOIF

Chemical and Downstream Oil Industries Forum

CDOIF is a collaborative venture formed to agree strategic areas for joint industry / trade union / regulator action aimed at delivering health, safety and environmental improvements with cross-sector benefits.

Appendix 5 – Worked example

Human Factors Analysis of Current Situation							Additional Measures to Deal With Human Factor Issues		
Step number	Task Step Description	Likely Human Failure	Is This a slip, lapse, mistake, or violation	Potential consequence	Performance Influencing Factors (PIF's)	Potential to Recover From Human Failure	Measures to Prevent Failure	Measures to Reduce the Consequence	Comments
1	Earth tanker when loading and offloading barrels and ISO's	<p><i>Earthing strap omitted or used too late after filling offloading already begun</i></p> <p>A2: Operation mistimed A9: Operation omitted A10: Operation incomplete A11: Operation too early / late</p> <p><i>Earthing accidentally attached to non-conducting material</i></p> <p>A6: Misalign A7: Right operation on wrong object</p> <p><i>Failure to earth</i></p> <p>V1 : Deliberate actions</p>	<p>Rule based mistake Lapse (omission) Lapse (omission) Slip</p> <p>Slip (commission) Slip (commission)</p> <p>Violation (routine, situational)</p>	Fire / explosion in the event of leak	<p>Job Factors: Divided attention Time available / required</p> <p>Person Factors: Fatigue Work over load</p> <p>Organisation Factors: Communication</p> <p>Job Factors: Clarity of instructions Divided attention Tools for task Environment</p> <p>Person Factors: Fatigue</p> <p>Job Factors: Difficulty / Complexity of task Time available / required</p> <p>Person Factors: Stress Motivation vs. other priorities</p> <p>Organisation Factors: Work pressures Clarity of R&R</p>	<p>Tank has interlock system to ensure earthing continuity</p> <p>Offloading check list including earth confirmation</p> <p>Operation completed with ADR driver present</p>	<p>Detailed procedures with SCT highlighted</p> <p>MAH scenario signage at earth point</p> <p>Earthing strap permanently fixed to plant end</p> <p>Multiple and well positioned earth straps in place to avoid violation due to apathy</p>	<p>Consider expansion of earthing continuity protection system to all offloading points (capital project)</p> <p>Change laboratory offloading procedure to include independent check / confirmation of earthing in place (review assessment including C1: Check omitted)</p> <p>Task currently completed by self-managing team. Frequency of supervision checks / presence in area to be increased including checks of SCT (again, review assessment including C1: Check omitted)</p>	N/A

