

Safety and environmental standards for fuel storage sites

Process Safety Leadership Group final
report

© Copyright of the Process Safety Leadership Group 2009

ISBN 978 0 7176 ##### #

Contents

Foreword

Abbreviations

Introduction

Scope and application

Summary of actions required

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

Appendices

Appendix 1: Mechanisms and potential substances involved in vapour cloud formation

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

Appendix 3: Guidance on defining tank capacity

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

Appendix 5: Guidance for the management of operations and human factors

Appendix 6: Emergency planning guidance

Appendix 7: Principles of process safety leadership

Appendix 8: Process Safety Forum: Governance and terms of reference

Appendix 9: BSTG report cross reference

Appendix 10: Acknowledgements

References

Further information

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 Competent Authority; 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 Competent Authority 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, Competent Authority and trade unions, which sets 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

Abbreviations

ACOP Approved Code of Practice

ALARP as low as reasonably practicable

AIChE American Institution of Mechanical 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

BCPS basic process control system

BCPF basic process control function

BSTG Buncefield Standards Task 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

DSEAR Dangerous Substances and Explosive Atmospheres Regulations 2002

DRA dynamic risk assessment

ECC emergency control centre

EEMUA Engineering Equipment Materials User's Association

ERP emergency response plan

FMEA

FMP fatigue management plan

FRS Fire and Rescue Service

HAZID

HAZOP

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

PSF performance shaping factors

PSLG Process Safety Leadership Group

PSMS process safety management system

RBI risk-based inspection

RCS risk control system

ROV remotely operated valve

ROSOV remotely operated shut-off valve

RVP reed vapour pressure

SEPA Scottish Environment Protection Agency

SIC site incident controller

SIL safety integrity level

SIS safety instrumented system

SG

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

TSA Tank Storage Association

TWI

UKPIA United Kingdom Petroleum Industry Association

UKOPA United Kingdom Onshore Pipeline Operator's Association

VCE vapour cloud explosion

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 Process Safety Leadership Group (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 Competent Authority Control of Major Accident Hazards (COMAH) Containment Policy.

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 Buncefield Standards Task Group (BSTG) using a small, focused, oversight team to lead, provide leadership and standards for onshore sites within the UK petrochemical and associated chemical industries. PSLG was supported by dedicated, expert working groups dealing with 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 Major Incident Investigation Board's (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 *Design and operation*¹ 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 11.

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 requirement may be split across multiple 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 4;
- 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 3 to determine the architecture and nature of the protection system.

Scope and application

9 For the purposes of this report gasoline is defined as in paragraph 24.

10 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 large storage tanks. In this guidance liquid dangerous substances are considered to be gasoline, other fuels as defined in the containment policy and other products defined within Appendix 1. PSLG has not defined the meaning of large storage tanks beyond the definition in paragraph 24 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.

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: that 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. In relation to overfill protection wherever possible this guidance indicates where this may occur. 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 Competent Authority.

Application to new COMAH establishments or sites subject to substantial modification

14 All new or substantially modified establishments storing liquid dangerous substances should follow this guidance in full with respect to tanks meeting the criteria set out in paragraph 24. For facilities falling within scope of the COMAH Competent Authority Containment Policy, dutyholders should comply with Part 4 in full. Other new sites 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 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 61511,² 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 a vapour cloud in the event of an overfill. An indicative list of such substances is also provided.

20 The Competent Authority together with industry will determine the extent to which this guidance should apply to tanks meeting these 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 consequences of a major accident. In the meantime, dutyholders should take account of this guidance in complying with their normal legal duties under COMAH. This will be especially important when conducting new or reviewing existing risk assessments.

***Existing establishments with tanks falling within scope 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 the other parts of this report when determining control measures for the bulk storage of liquid dangerous substances.

Existing establishments storing other dangerous substances in bulk tanks

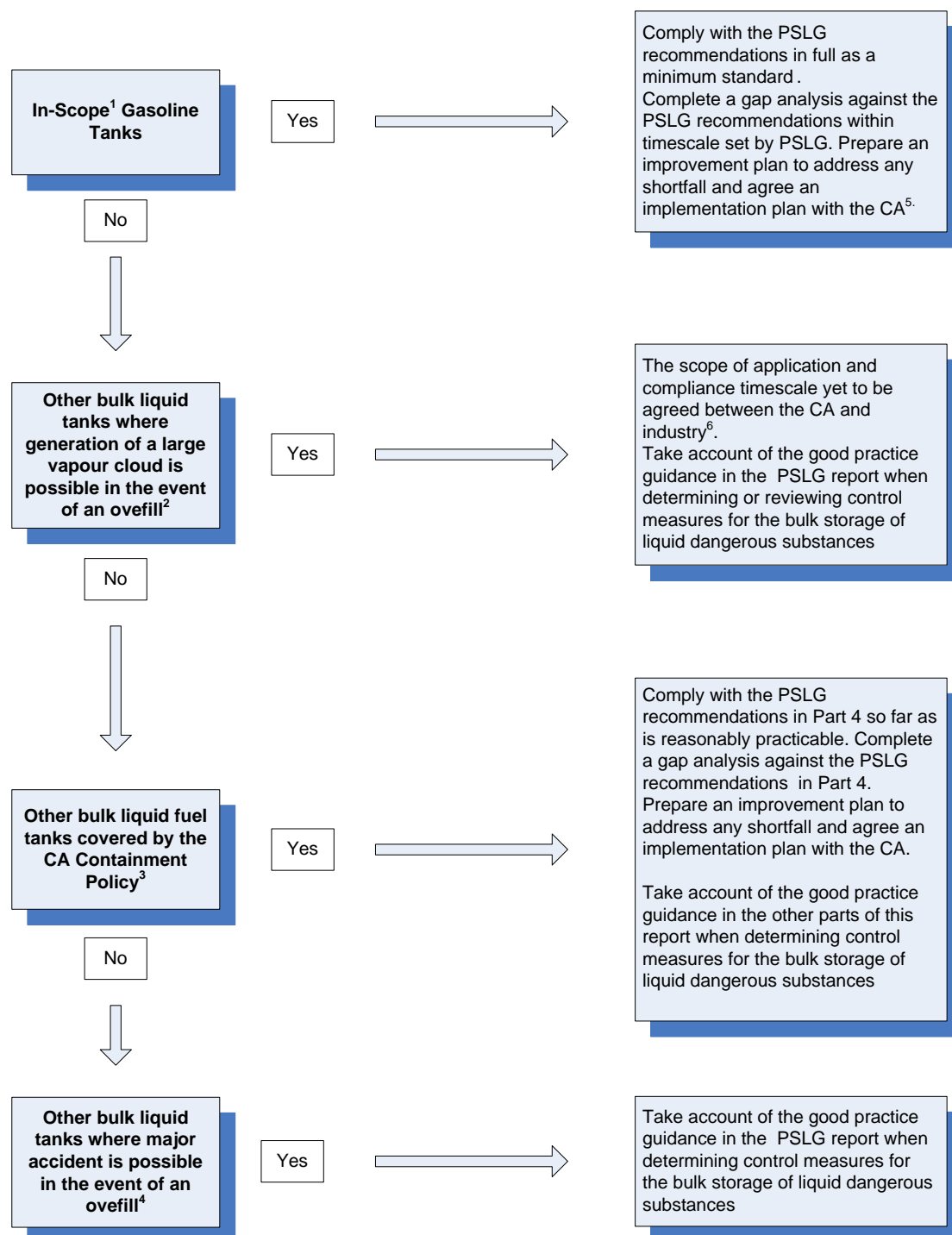
23 This report contains generic guidance on the storage of bulk liquids, product transfers and management systems, including competence and human factors. Dutyholders for establishments not specifically covered above are advised to take account of this guidance when determining the control measures covering such activities.

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).

Figure 1 Compliance at existing COMAH establishments



Notes:

1 As defined in paragraph 24.

2 As set in Appendix 1.

3 Competent Authority COMAH Containment Policy www.environment-agency.gov.uk/business/sectors/37107.aspx.

4 For COMAH top-tier establishments a description of the possible major accident scenarios and an assessment of the extent of the consequences should be included within the safety report for the establishment.

5 See paragraphs 25 and 26.

6 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 2. The Competent Authority will agree future proposals on implementation with industry.

Summary of actions required

25 This section provides a summary of the MIIB *Design and operation report* recommendations. Dutyholders should have already have met the recommendations within the BSTG report. The Competent Authority has a programme of work to check compliance.

26 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 and record their findings. Within nine months of the publication of this report dutyholders should agree with the Competent Authority an improvement plan to comply with this guidance.

27 Detailed guidance on how to meet these recommendations is given in Parts 1 to 6 of this report. The information is presented in the same order as the recommendations in the MIIB report *Recommendations on the design and operation of fuel storage sites*.

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 | |
|--|---|-------------------------|---|
| <i>Systematic assessment of safety integrity level requirements</i> | | | |
| 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: 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. | 1(a) | The existence of nearby sensitive resources or populations |
| | | 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 |
| <i>Protecting against loss of primary containment using high integrity systems</i> | | | |
| 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 | 2(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 |

| MIIB recommendation | | MIIB sub-recommendation | |
|---------------------|---|-------------------------|---|
| | include, but not be limited to reviews of the following: | 2(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 |
| 3 | <p>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.</p> <p>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)</p> | | |
| 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 'safety instrumented systems', Part 1 of BS EN 61511 | | |
| 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. | | |

| MIIB recommendation | | MIIB sub-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 | | |
| 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 | | |
| 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: | 8(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 |
| | | 8(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 |
| | | 8(c) | systems to control and log override actions |
| 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 |
| | | 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 Competent Authority, 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 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 <i>Developing process safety indicators</i> HSG254 | | |

| MIIB recommendation | | MIIB sub-recommendation | |
|---|--|-------------------------|---|
| Engineering against escalation of loss of primary containment | | | |
| 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 | | |
| 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 | | |
| 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: | 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 |
| | | 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 |
| | | 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 |
| 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 | | |

| MIIB recommendation | | MIIB sub-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 | | |
| 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 | | |
| Engineering against loss of secondary and tertiary containment | | | |
| 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: | 17(a) | developing a minimum level of performance specification of secondary containment (typically this will be bunding) |
| | | 17(b) | developing suitable means for assessing risk so as to prioritise the programme of engineering work in response to the new specification |
| | | 17(c) | formally specifying standards to be achieved so that they may be insisted upon in the event of lack of progress with improvements |
| | | 17(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 |
| | | 17(e) | providing greater assurance of tertiary containment measures to prevent escape of liquids from site and threatening a major accident to the environment |
| 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 Competent Authority risk-based plans for phased upgrading as close to new plant standards as is reasonably practicable | | |
| Operating with high reliability organisations | | | |
| 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 | 19(a) | understanding and defining the role and responsibilities of the control room operators (including in automated systems) in ensuring safe transfer processes |
| | | 19(b) | providing suitable information and system interfaces for front line staff to enable them to reliably detect, diagnose and respond to potential incidents |

| MIIB recommendation | | MIIB sub-recommendation | |
|--|---|-------------------------|--|
| | importance are: | 19(c) | training, experience and competence assurance of staff for safety critical and environmental protection activities; |
| | | 19(d) | defining appropriate workload, staffing levels and working conditions for front line personnel |
| | | 19(e) | ensuring robust communications management within and between sites and contractors and with operators of distribution systems and transmitting sites (such as refineries); |
| | | 19(f) | prequalification auditing and operational monitoring of contractors' capabilities to supply, support and maintain high integrity equipment |
| | | 19(g) | providing effective standardised procedures for key activities in maintenance, testing, and operations |
| | | 19(h) | clarifying arrangements for monitoring and supervision of control room staff |
| | | 19(i) | effectively managing changes that impact on people, processes and equipment |
| 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 | | |
| 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 | | |
| 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 | | |
| <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 | | |
| 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 |

| MIIB recommendation | | MIIB sub-recommendation | |
|---------------------|---|-------------------------|--|
| | | 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 1: Systematic assessment of safety integrity level requirements

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 must be of high integrity, with sufficient independence to ensure timely and safe shutdown to prevent tank overflow.

30 Dutyholders 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 must be able to justify each and every 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 with 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 Layer of protection analysis (LOPA) is a suitable methodology to determine safety integrity levels within the framework of BS EN 61511-1.

Overfill protection systems for storage tanks

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

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

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

36 Shutdown of product flow to prevent an overfill should not depend solely upon systems or operators at a remote location. The receiving site must 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 and SIL determination; BS EN 61511 Part 3 provides a summary of the method. Detailed guidance for the application of LOPA 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
- safety instrumented systems and management systems meet BS EN 61511, so far as is reasonably practicable.

Operator responsibilities and human factors

42 Monitoring and control of levels, and protection against overfill, may depend on operators taking the correct actions at a number of stages in the filling procedure. These actions may include:

- 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; and
- response to level alarm high-high.

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 critical actions required, so the human factors associated with operator responsibilities need careful consideration. A useful guide is *Reducing error and influencing behaviour* HSG48.⁷ Also refer to Annex 8 of Appendix 2.

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

44 The MIIB's third progress report⁸ 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 when required to operate. Therefore overfill protection systems should be tested periodically to prove that they will operate safely when required.

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.

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 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.

48 BS EN 61511 requires that for all SIL 1 and higher safety instrumented systems (SIS) there is a management system in place for the whole the lifecycle of the SIS, which will manage all appropriate measures.

49 Systems providing a risk reduction of less than 10 are not in scope of BS EN 61511; however, they may still provide a contribution to the safety function and have a risk reduction of up to a factor of 10. Such systems should comply with the management systems requirements of BS EN 61511 so far as is reasonably practicable.

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

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

Management of safety instrumented systems

52 A safety instrumented system (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 must 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 those tasks. The required competence is wide ranging and depends on the type of task. Competence typically includes engineering knowledge, process knowledge, system technology knowledge and experience, safety engineering, legal and regulatory requirements, management and leadership skills, understanding of the potential consequences of a failure and hazardous event, safety integrity levels and maintenance and testing activities.

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. 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

62 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 61508⁹).

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 safety instrumented system.

63 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. 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

64 Where changes or modifications to a safety instrumented system 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.

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

Documentation

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

67 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

68 EEMUA 159¹⁰ 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 help ensure that dutyholders 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.

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).

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 'safety instrumented systems', Part 1 of BS EN 61511.

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

69 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.

70 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.

71 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

72 All in-scope tanks should be fitted with a high integrity overfill prevention system that complies with BS EN 61511-1. Dutyholders should conduct a risk assessment to determine the appropriate safety integrity level to meet the requirements of BS EN 61511-1. The outcome of that risk assessment should demonstrate that the risk of a tank overfilling in a way that may give rise to major accident is ALARP. Appendix 2 provides guidance on the use of LOPA as a means of undertaking a suitable risk assessment.

73 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 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.

74 Where the automatic operation of such an independent overfill prevention system at an existing storage tank is demonstrated to give rise to other more serious safety or

environmental consequences elsewhere then other alternative measures may be adopted to achieve the same ALARP outcome.

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

76 Alternative measures:

- must include an overfill prevention system to at least BS EN 61511-1 SIL level 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 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 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.

77 For existing installations dutyholders should complete a gap analysis against the standards set out in this guidance and prepare an improvement plan to bring the system up to standard where this is shown to be necessary.

Proof testing

78 Appendix 4 paragraphs 24–34 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 overfill, tanks should have headspace margins that enable the filling line to be closed off in time. High level alarms and operator or automatic actions should be adequately spaced to deal with a developing overfill 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 level being reached/exceeded. This is termed the ‘tank rated capacity’, which will be lower than the actual physical maximum.

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 high-high level (level alarm high-high (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; and
- 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 level alarm high (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); and
- 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. Plant 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 don 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.)

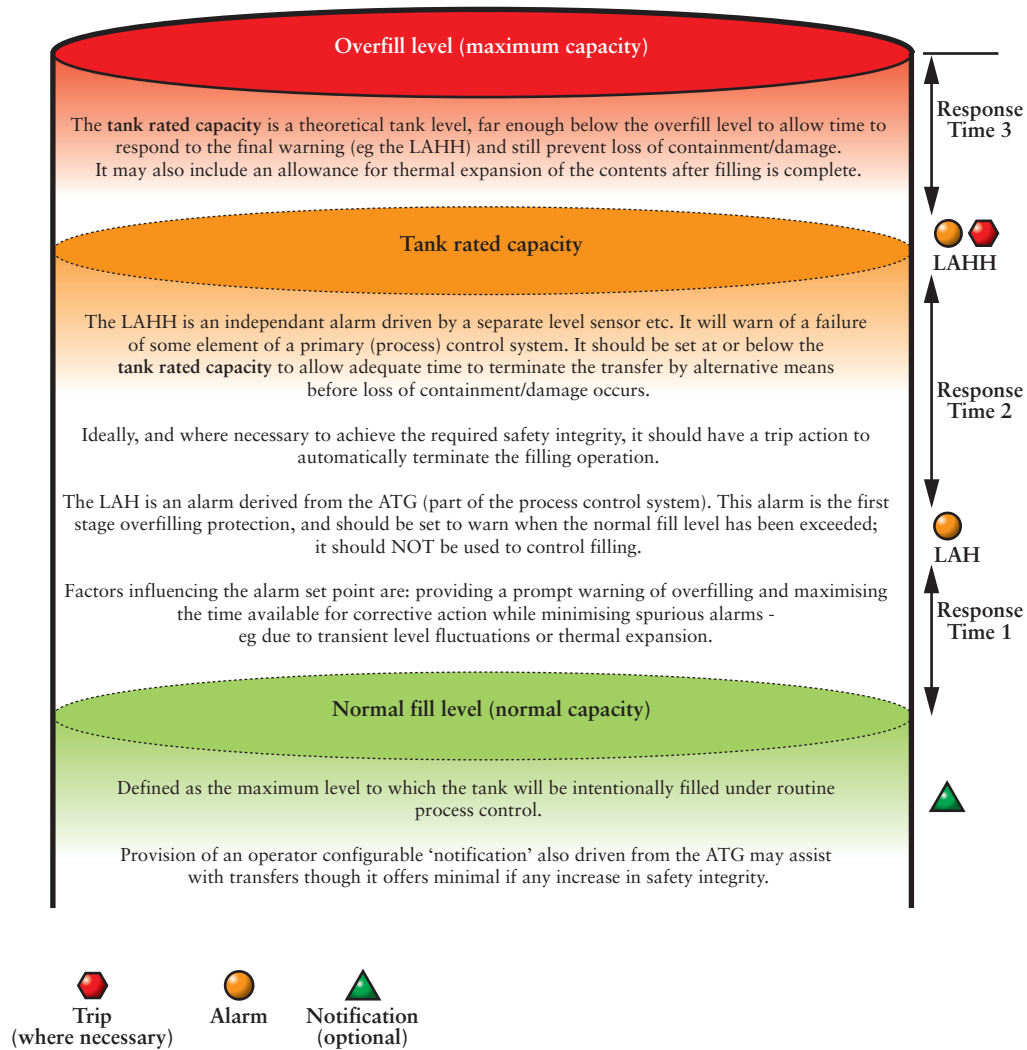


Figure 2 Overfilling protection: tank levels (based on API2350¹¹)

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† close the valve. 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 must be recorded in writing.

Response time 2: LAH to LAHH

99 The response time between the high level alarm (LAH) and the independent high-level (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.‡

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 must 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.

* 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.

† The remote and automatic systems must now be assumed to have failed – even if they appear to be working – and positive human action is now required to prevent overfill.

‡ 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.

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 must be fitted close to the tank on both inlet and outlet pipes. Valves must either conform to an appropriate standard (BS 6755-2¹² or BS EN ISO 10497¹³), 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 foreseeable 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* HSG244¹⁴ 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 must 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 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.

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.

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)*,¹⁵
- 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.

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; and
- (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 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 of 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.

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 safety instrumented systems can be found in the guidance provided against Recommendation 2, 'Management of instrumented systems for fuel storage tank installations'.

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 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.

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 IP15 *Area classification for installations handling flammable fluids*¹⁶) 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) L138¹⁷ and where relevant the additional activity related DSEAR ACOPs:

- *Unloading petrol from road tankers* L133;¹⁸
- *Design of plant equipment and workplaces* L134;¹⁹
- *Storage of dangerous substances* L135;²⁰
- *Control and mitigation measures* L136;²¹ and
- *Safe maintenance, repair and cleaning procedures* L137.²²

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.

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.

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-skinned 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 183,²³ 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 all likely relief conditions. Emergency vents should comply with an appropriate design standard (API 2000²⁴ or equivalent).

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 653²⁵ 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/35²⁶ 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 provide 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 598.²⁷

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*)²⁸ 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/163²⁹ 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.

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 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).

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.

Recommendation 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 Competent Authority risk-based plans for phased upgrading as close to new plant standards as is reasonably practicable.

Bund integrity (leak-tightness)

167 Bund wall and floor construction and penetration joints should be leak-tight. Surfaces should be free from any cracks, discontinuities and joint failures that may allow relatively unhindered liquid trans-boundary migration. As a priority, existing bunds should be checked

and any damage or disrepair, which may render the structure less than leak-tight, should be remedied.

168 Bund walls should be leak-tight. As a priority, existing bund walls should be checked and any damage or disrepair, which may render the wall less than leak-tight, should be remedied.

Fire-resistant bund joints

169 This guidance does not address the fire-resistance of the main material of construction for existing bunds, because:

- this was not believed to be a significant factor in the Buncefield incident, except insofar as:
 - the contraction on cooling of concrete walls may have caused the opening up of wall joints and consequent integrity failure; and
 - the reason for concrete floor heave and associated loss of integrity, and the comparative performance of earth/clay, is not known;
- further information from the Buncefield investigation and additional civil engineering studies will be needed to properly consider the comparative impact of fire on earth/clay bund walls and floors compared to reinforced concrete.

170 Joints in concrete or masonry bunds walls should be capable of resisting fire. Existing bunds should be modified to meet this requirement. In addition to repairing any defects in bund joints, steel plates should be fitted across the inner surface of bund joints, and/or fire-resistant sealants should be used to replace or augment non-fire-resistant materials.

171 The current good practice standard for the construction of reinforced concrete bunds is BS 8007.³⁰ Bund joints are currently required to be rendered leak-tight by the adoption of flexible barriers such as waterstops and sealants, bonded into or onto the concrete joint surface.

172 BS 8007 does not address the retention of non-aqueous liquids or of liquids above 35 °C, or the construction of bund joints at pipework and other penetrating structures. CIRIA reports 163³¹ and 164³² address bund design and construction issues in detail. The CIRIA/Environment Agency joint guidance³³ referring to CIRIA report 163 is also relevant to the design and construction of smaller reinforced concrete bunds.

173 To achieve bund joints capable of resisting fire, improvements may be required to the fire resistance of:

- the main material(s) of construction (not addressed in this guidance);
- the waterstops and flexible sealant(s) used to make joints leak-tight; and
- joints to wall and floor penetrations such as pipework. It may also be necessary to provide additional fire protection to joints by fitting a 'fire-proof' barrier such as steel plate.

Masonry (brickwork and block-work) bund walls

174 On older sites masonry bund walls are still in use. Vertical expansion and contraction joints and penetration joints rely on sealants to keep the bund watertight. These may require improvement to fire resistance. In addition, where significant cracks in masonry joints have been repaired with flexible sealant, these may also require improvement.

Earth/clay bunds

175 Earth and clay are in very common use, often as floors of bunds with concrete or masonry walls. In such floors there are normally no construction joints, but penetrating drains or other pipework result in points of weakness and potential failure.

176 The following modification options for improving fire resistance should be assessed for practicability and likely effectiveness.

Flexible sealants

177 Sealants claiming enhanced fire resistance are now available. The only fire-resistance standards that are quoted on these products are BS 476-20:1987 and BS 476-22:1987.³⁴ The maximum fire resistance quoted to BS 476 is four hours. The relationship of performance to this standard to actual performance in a bund-joint application is yet to be determined. In considering the use of fire-resistant sealants, due regard should also be given to the suitability and compatibility of candidate products (eg hydrocarbon and water resistance) in the specific application.

178 While fire-resistant sealants represent a significant improvement over non-fire-resistant sealants, a very severe pool fire, such as seen at Buncefield, is still likely to result in failure of joints. The prolonged pool fire scenarios at Buncefield are thought to have resulted in considerable longitudinal expansion of wall sections, and consequent compression of wall joints, resulting in extrusion of sealant from joints and the burning out of the extruded sealant. When walls cooled and contracted after the fire was extinguished, it is thought that joints opened up and, with sealant burnt out, loss of integrity and containment resulted. This potential mode of failure emphasises the need to consider suitable tertiary as well as secondary containment provision.

Steel protection plates

179 Steel plates, observed in some locations at the Buncefield incident site, are thought to have provided significant additional protection to bund joints. It is believed that these plates were not, however, designed for fire protection purposes. Nevertheless, the relevant joints appeared to withstand a severe pool fire without losing integrity. **It therefore appears that where it is practicable to fit them, suitably designed protective steel plates may provide more effective fire resistance than fire-resistant sealants.**

180 Detailed information is not currently available for the design of steel plate fire protection, and dutyholders should design for specific applications. 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, minimum 30 cm intervals; and
- additional protective features to be considered:
 - fireproof backing material such as cement board; and/or
 - fire-resistant coating such as intumescent material to the front face.

Note: in designing protection plates, consideration should be given to avoiding weakening the wall structure in relation to resistance to fire, hydrostatic and hydrodynamic forces. Numerous practicable designs for existing installations have now been developed and implemented.

Recommended improvements

Existing bunds

181 Improvements should be made to the fire-resistance of bund joints by suitable protection (eg metal plate covering) and/or by the use of fire-resistant sealants. Problems experienced in sourcing compatible sealants in suitable packaging for this application, together with uncertainties in actual joint fire resistance performance or requirements, unavoidably result in a range of ad-hoc improvement solutions.

182 **Bund wall penetration joints:** For penetrations of concrete and masonry, the first option should be to consider rerouting pipework or other penetrating structures to eliminate the need for the joint. Where this is not practicable, or planned removal is significantly delayed for operational reasons, the fire-resistance of the joint must be improved. Fitting steel collars, bellows or similar to improve fire resistance at pipework penetrations may introduce

local corrosion initiation sites in the pipework, and is therefore not recommended where this may be likely. In such cases joints should be improved by replacing existing sealants with fire-resistant sealants. For penetration of earth bund walls, these joints may be inherently less vulnerable because of the greater joint thickness. However, insufficient information has been considered to allow reliable guidance to be produced for this case. Joints should be assessed on a site-specific basis.

183 **Bund floor construction joints:** For concrete bund floors, vulnerability to fire should be capable of being reduced by managed emergency response measures such as maintaining an insulating water layer on the bund floor. Removal of existing flexible sealant for replacement with fire-resistant alternatives may result in reduced performance with regard to water tightness. Floor joints nevertheless remain potential weaknesses for loss of integrity in a severe pool fire. A case-by-case assessment of floor joint fire-resistance improvement options should be made.

184 **Bund floor penetration joints:** Bund floor penetration joints are points of inherent weakness where any failure of integrity is very difficult to detect and may continue unnoticed for some time. Consequently, existing bund floor penetrations should be eliminated wherever practicable. Where flexible sealants are used in floor penetration joints, these should be removed and replaced with fire-resistant sealants.

185 **Cracks in concrete and masonry bund walls and floors:** Repaired cracks in existing bund surfaces must be assessed for significance with regard to the potential to fail in a fire scenario, resulting in loss of secondary containment. Where cracks are superficial, improvement may not be required, but where cracks are significant, the flexible sealant used must be replaced by fire-resistant sealants.

Selection of lining systems

186 The COMAH Containment policy states that ‘bunds shall be impermeable’ and that in addition to concrete and earth, the use of liners and lining systems can be used to make bunds leak-tight.

187 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.

188 The scope covers the preparation of the tank base and foundation plus the selection of lining systems; concrete, earth or polymeric or polymeric and mineral composites.

189 The selection of any system is based on a combination of risk (to the environment and people), cost and practicality.

Fire protection for lining systems

190 The COMAH Containment policy states that 'bunds shall have fire resistant structural integrity, joints and pipework penetrations'.

191 Improvements should be made to the fire-resistance of bund joints by suitable protection (eg metal plate covering) and/or by the use of fire-resistant sealants.

192 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 resistant and the risk to loss of integrity is provided by joints and penetrations and the way these features are sealed.

193 Polymeric or polymeric and mineral composites (combinations of plastics, textiles and bentonite) are at risk from fire and if affected will lose impermeability. The use of these systems presents a number of advantages in terms of relative cost, containment effectiveness and practical application.

194 It is important that protection from fire is included in risk assessment for these types of systems (BS 476).

Secondary containment systems under tanks

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

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

197 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.
- EEMUA 183 *Guide for the Prevention of Bottom Leakage from Vertical, Cylindrical, Steel Storage Tanks* Chapter 3 also provides similar data, but again quotes 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, welded, steel tanks for the storage of liquids at ambient temperature and above*.

New bunds

198 For new bunds, to achieve the maximum practicable fire resistance for bund joints the following additional measures should be taken:

- **Bund wall and floor construction joints:** Joints should be designed to be fire resistant. Consideration should be given to incorporating stainless steel waterstops and expansion joints bonded into the structure, in combination with fire-resistant sealant.
- **Bund wall penetration joints:** Wall penetrations should not be incorporated into new bunds unless alternative over-wall routings are impracticable. Where wall penetrations are unavoidable, joints should be designed to be fire resistant. Consideration should be given to incorporating puddle flanges cast into the concrete structure.
- **Bund floor penetration joints:** Floor penetrations should not be incorporated into new bunds.

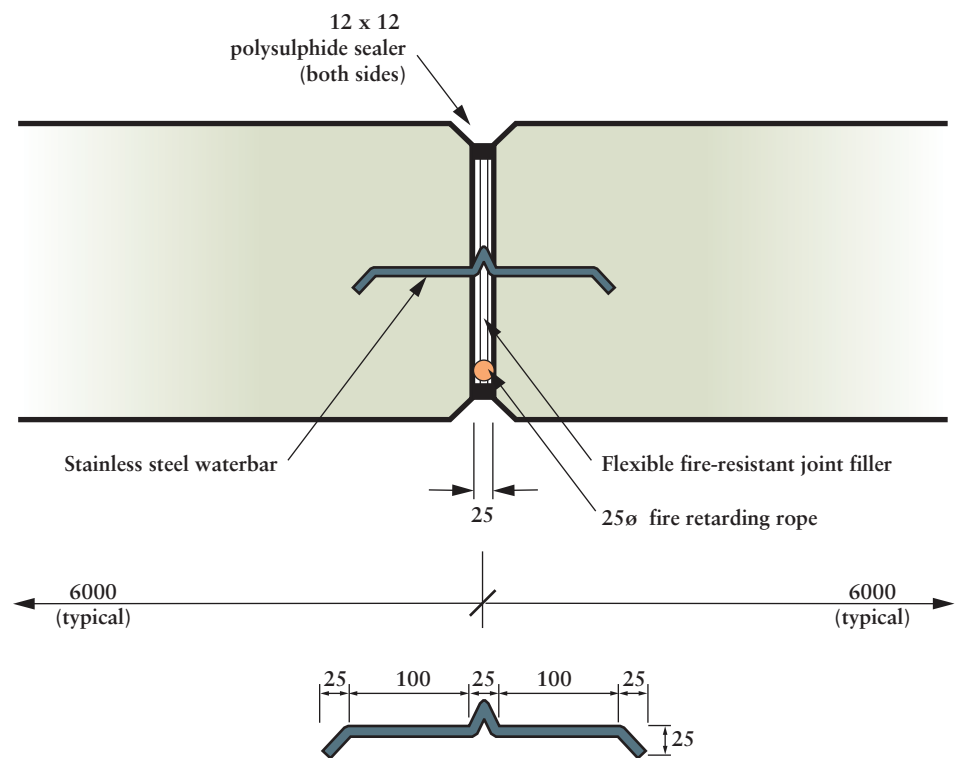
Stainless steel waterstop designs

199 The addition of steel plates to cover movement joints provides enhance fire resistance. Where necessary, improvements should be made to the fire-resistance of bund joints by suitable protection (eg metal plate covering) and/or by the use of fire-resistant sealants.

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

201 Waterstops provide the most effective way of minimising leakage from bund joints. Steel plates have been seen to significantly reduce leakage rates, both due to their role in enhancing fire resistance (eg they could provide protection to a plastic waterstop) and in reducing leakage where no fire has occurred. New designs are available incorporating stainless steel waterstops into bund walls.

202 An example of a steel water stop is shown in Figure 3.



- Notes:**
- 1: Fire retarding rope to be placed on both sides of an internal bund wall and on internal side only of an external wall
 - 2: Waterbar, rope and polysulphide sealant to be omitted in bundwalls footings
 - 3: Stainless steel for waterbar to be grade 316 and 1.0 mm thick

All measurements are in millimetres

Bund wall expansion joint detail (1/10)

Figure 3 Bund wall expansion joint showing stainless steel waterstop (detail)

Fire-resistant wall penetration joints

203 Figure 4 shows an example puddle flange cast into a bund wall – a 200 NB pipe in a 250 NB sleeve passing through a bund wall.

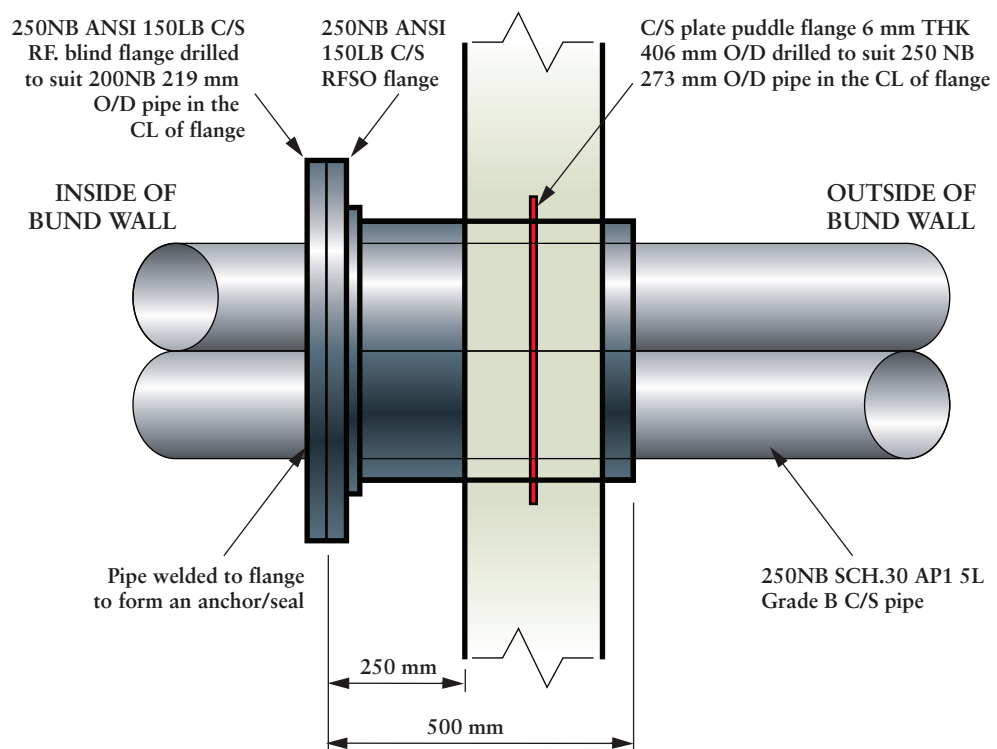


Figure 4 Example puddle flange cast into a bund wall

Bund capacity

204 The minimum capacity for bunds containing tanks in scope at existing installations is 110% of the largest tank.

205 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.’

206 An important aspect is the definition of tank capacity. There are a number of terms stated in various sources.

207 Tank capacity and bund capacity are important elements in the mitigation of the following types of incidents:

- overfill;
- leak from the base;
- catastrophic tank failure.

Firewater management and control measures

208 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; and
- controlled-burn options appraisal, and pre-planning/media implications.

Tertiary containment

209 This guidance applies only to the loss of secondary containment from bunds containing tanks within the 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.

210 The term ‘tertiary containment’ is used to describe containment systems and measures to contain potentially polluting liquids which may escape as a result of loss of secondary containment, and would otherwise be released into the environment causing pollution.

Risk assessment

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

- foreseeable bund failure modes, including:
 - the amount of spilled substances, including hydrodynamic effects of catastrophic tank failure and emergency response actions such as firefighting;
 - the potential impact of fire on bund integrity including joints in walls and floors;
 - worst-case foreseeable delivered firewater volumes including firefighting agents (see IP19³⁵); 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*,³⁶
 - proximity of receptor, eg 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

212 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 any 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, eg in the event of loss of the normal electrical power supply;
- avoid adverse impacts on firefighting 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 practicable measures for the management of rainwater and surface waters as required by the configuration; and
- facilitate clean up and restoration activities.

213 On-site effluent treatment facilities, sized to allow collection and treatment of polluted firewater, are a desirable design feature, but may only be justifiable at larger establishments.

Design options

214 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 164 Ch 13) is used to describe the means for collecting and conveying spillage/firewater to remote and combined secondary and tertiary containment.

215 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.

216 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.

217 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 (eg pumps) is independent and reliability of emergency operation is assured.

218 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 firefighting attack duration. Buncefield showed that consequences might be much more extensive than expected.

219 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, eg 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, eg pipe-blockers, drain sealing mats and land booms.

220 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

221 General guidance on the design of remote containment systems (including lagoons, tanks and temporary systems such as sewerage storm tanks and sacrificial areas, eg car parks, sports field and other landscape areas) is available in numerous documents including CIRIA 164, and PPG18.³⁷

222 Catchment areas used for tertiary containment often serve a dual purpose, eg 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.

223 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, Ch 6.

Risk assessment guidance

224 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 2.

Table 2 Environmental risk assessment checklist

| Action/parameter | Guidance |
|---|--|
| <i>For the worst-case foreseeable severe pool fire scenario</i> | |
| Identify firewater volumes | Energy Institute IP19 ³⁵ |
| Assess firewater management effects | |
| Identify bund potential failure points | MIIB second progress report ³⁸ |
| 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 | <i>Environmental guidelines for petroleum distribution installations</i> EI ³⁹ |
| Identify surrounding environmental receptors, eg 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/ ; <i>Guidance on the interpretation of major accident to the environment for the purposes of the COMAH Regulations 1999</i> ³⁶ Tables 1–12 |
| Identify geological characteristics | |
| Identify hydrogeology | British Geological Survey www.bgs.ac.uk/ |
| Identify flow gradients and likely flow outcomes | |
| Identify direct pathways, eg drains, boreholes | |
| Identify indirect pathways to sensitive receptors, eg permeable ground | |
| Assess permeability of ground and thus permeation flow-rates and quantities of pollutant into ground | CIRIA 164 ³² |
| <i>Consider appropriate defensive tertiary containment measures</i> | |
| Kerbing to roadways, car parks etc, toe walls, area grading | |
| Eliminate direct pathways, eg cap boreholes | |
| Emergency drain seals (eg 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

225 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.

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.

226 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.

227 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.

228 Refer to Appendix 5 for detailed guidance.

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.

229 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.

230 The Competent Authority, within its regulatory programme, should check that dutyholders are complying with this guidance.

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.

231 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.

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.

232 The Competent Authority 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

233 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.

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.

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.

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.

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

235 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.

236 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.

Appendix 1: Mechanisms and potential substances involved in vapour cloud formation

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

LIQUID DISPERSAL AND VAPOUR PRODUCTION DURING OVERFILLING INCIDENTS

Graham Atkinson¹, Simon Gant¹, David Painter¹, Les Shirvill² and Aziz Ungut²

¹HSE

²Shell Global Solutions

© Crown Copyright 2008. 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 [1–4]. 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.

1. PHYSICAL PROCESSES

1.1 LIQUID FLOW

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 a 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.

1.1.1 Liquid release from Type A tanks

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 10m around the perimeter.

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.

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 1.

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 2.

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 3m around the tank perimeter. If the vents are spaced at 10m 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.

1.1.2 Liquid release from Type B tanks

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 3). Small bore holes drain the top girder shelf but in the event of an over fill 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.

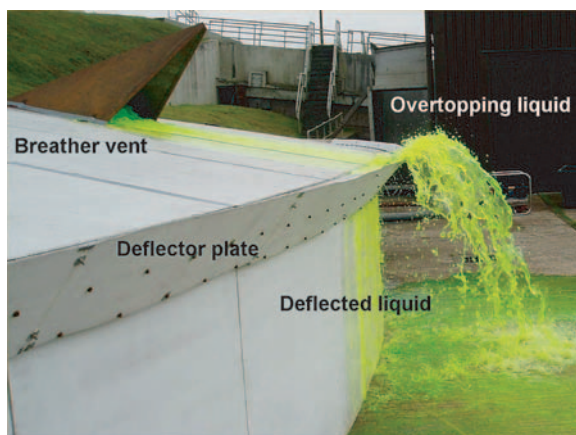


Figure 1. Liquid release from a vented fixed roof tank with a deflector plate



Figure 2. Intersection of free cascades from a Type A tank with a deflector plate



Figure 3. Top grider (walkway) in floating roof tank

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.

1.1.3 Liquid release from Type C tanks

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.

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.

1.2 LIQUID DISPERSAL

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.

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 (i.e. the amount of liquid falling through each square metre per second). If the flux density is relatively low most of the initial liquid fragments rapidly shatter 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.

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 fragment initially formed may persist for the full height of the drop.

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 i.e. wetted solid or deep liquid.

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.* [4]. 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 of the depth of liquid on the impact surface and may even exceed the incident droplet mass in some circumstances.

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.

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.

1.3 AIR ENTRAINMENT

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.

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 4. 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.

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.

1.4 VAPORISATION OF LIQUID

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 5.

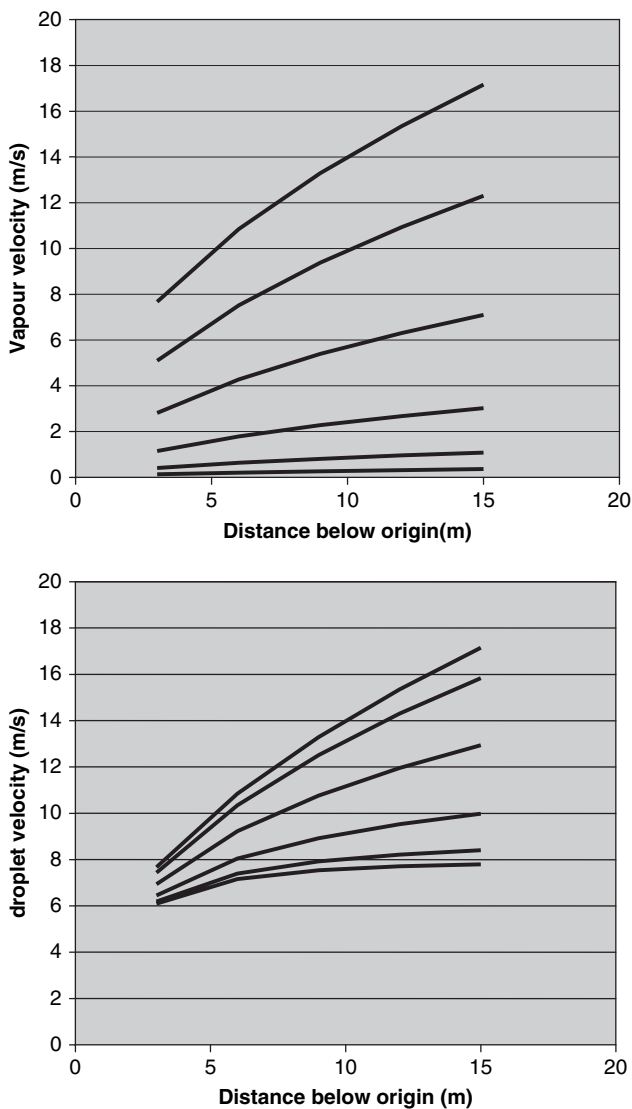


Figure 4. Vapour and droplet velocities induced by liquid cascades of different densities. The highest velocities shown in both plots (for comparison) correspond to free-fall with no air resistance. The lower velocities correspond respectively to liquid flux densities of 100, 10, 1, 0.1 and 0.01 kg/m²/s

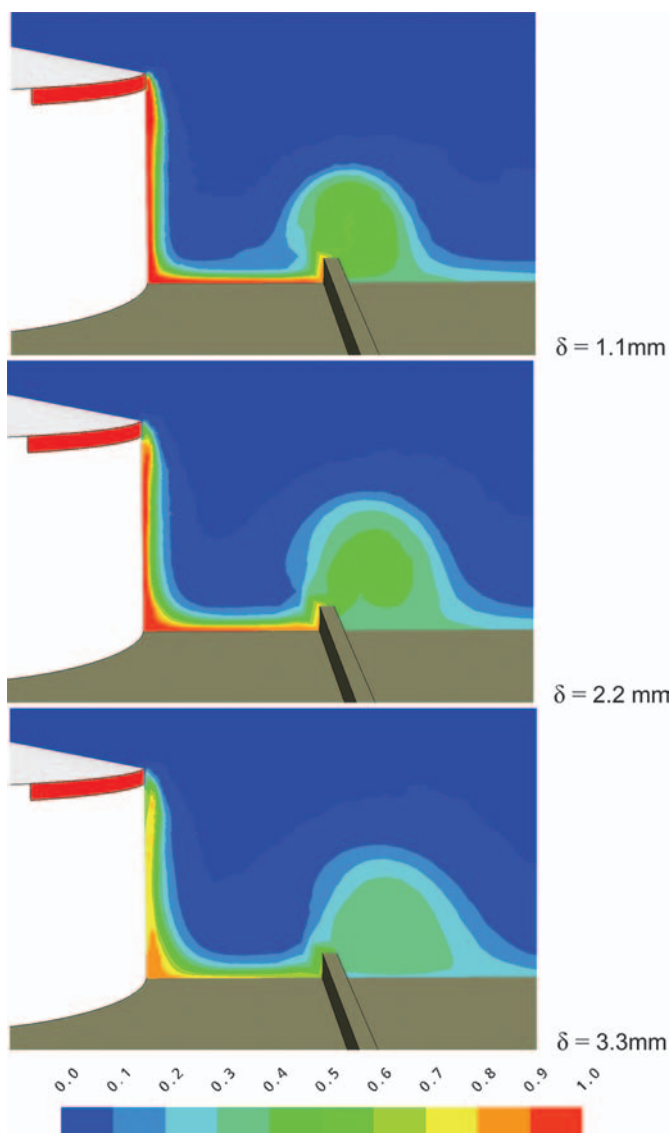


Figure 5. Contours of the ratio of predicted vapour volume fraction to the saturation volume fraction. A value of 1.0 indicates that the vapour is saturated. The three predictions are for different initial droplet size distributions using the Rosin-Rammler diameters shown

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.

The CFD modelling shown in Figure 5 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.

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.

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 e.g. light crude oils.

1.5 NEAR FIELD DISPERSION

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.

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 5) 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.

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

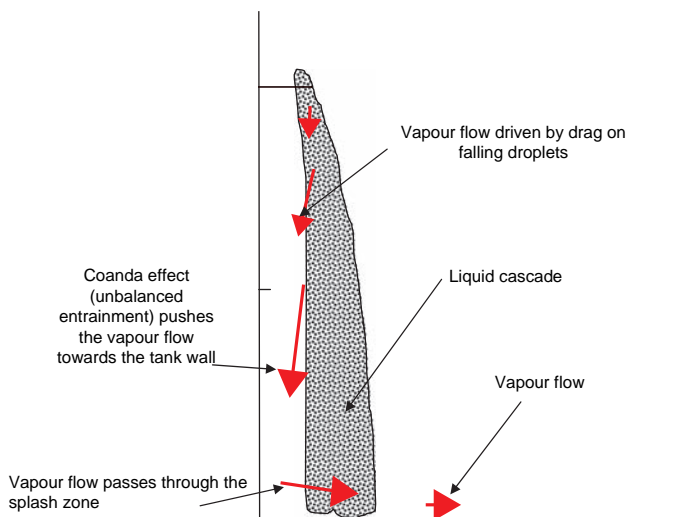


Figure 6. Schematic showing vapour flow driven by a free liquid cascade

the droplet splash zone at the base of the tank – see Figure 6. 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.

2. SCOPING METHOD

2.1. APPROACH AND ASSUMPTIONS

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 of the near-field dispersion.

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.

Although it may appear initially counter-intuitive, the likelihood of producing flammable vapour for many substances increases 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.

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 air flow

Given the liquid mass density the volume flow of entrained air can be taken from a plot such as that shown in Figure 4. 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 overflowing of the tank will produce a flammable cloud.

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.

Results of such scoping analyses on typical high volume refinery liquids and crude oils are shown in Figures 7 and 8. 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.

3. IMPLICATIONS FOR SAFETY AND ENVIRONMENTAL STANDARDS AT FUEL STORAGE SITES

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.

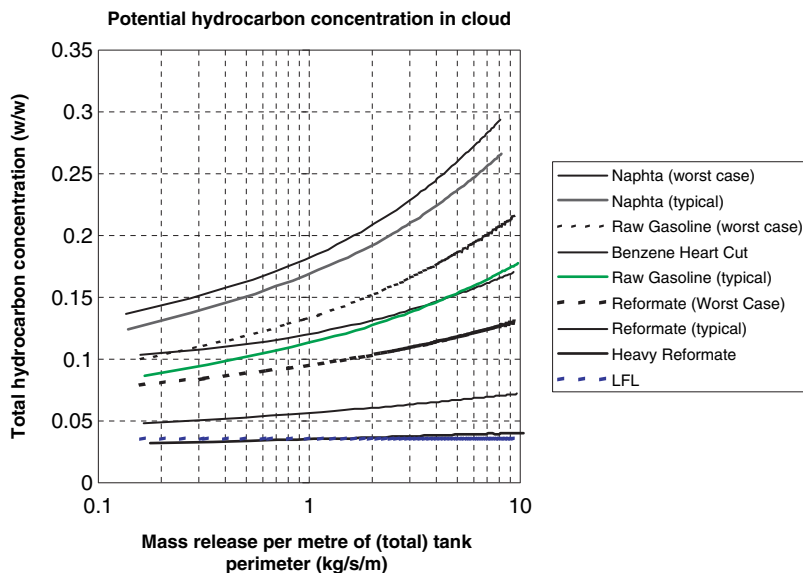


Figure 7. Vapour concentrations in air driven by cascades of various refinery liquids

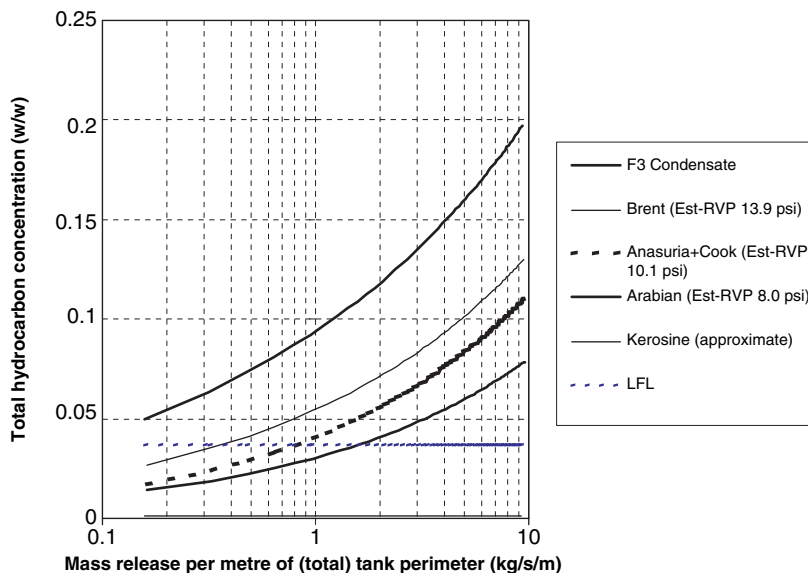


Figure 8. Vapour concentrations in air driven by cascades of various crude oils

To ensure focussed 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 (5). This was confirmed in the final report of July 2007 (6) 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).

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 section 1.1 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.

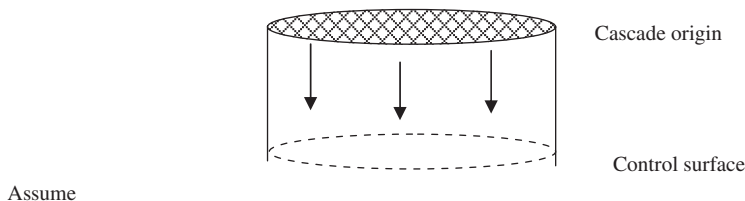
This work also indicates that there is the potential for other substances with similar physical properties to behave in a similar way in the event of a loss of primary containment following overfilling. Work continues in order to establish an agreed definition for the extension of scope to a limited 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.

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 (6) details these actions and includes the supporting guidance.

REFERENCES

1. Maremonti M., Russo G., Slazano E. and V. Tufano *Post-accident analysis of vapour cloud explosions in fuel storage areas*. Trans. IChemE, 1999, **77**: p.360–365.
2. Yuill, J. *A discussion on losses in process industries and lessons learned*. in 51st Canadian Chemical Engineering Conference (see <http://psm.chemeng.ca>), Halifax, Nova Scotia, Canada, 2001.
3. Buncefield Investigation – Third Progress Report. 2006 Major Accident Investigation Board. (available from <http://www.buncefieldinvestigation.gov.uk>).
4. Chang, J.I. and Cheng-Chung, L. *A study of storage tank incident*, J. Loss Prevention, 2006 **19**: p.51–59.
5. Bai, C.X., Rusche, H. and Gosman, A.D., (2002) *Modelling of gasoline spray impingement*, Atomisation and sprays, **12**: p. 1–27.
6. Buncefield Standards Task Group *initial report – recommendations requiring immediate action* 12 October 2006 (available from <http://www.hse.gov.uk/comah/buncefield/bstg1.htm>).
7. Buncefield Standards Task Group *final report – safety and environmental standards at fuel storage sites* 24 July 2007 (<http://www.hse.gov.uk/comah/buncefield/final.htm>).

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 ($\text{kg}/\text{m}^2/\text{s}$).

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 (i.e. all droplets are the same size).

Droplet dynamics

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

Vapour dynamics

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

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

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

$$\frac{A_{\text{drop}}}{m_{\text{droplet}}} = \frac{3}{4r_{\text{drop}} \rho_{\text{drop}}} (\text{characteristic of spherical droplet})$$

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 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
Final vapour and liquid temperature

96 m³/s
−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 |
| Naphta (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 overfill

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 overfill.

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 all refined 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 overfill 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.

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

- Use reed 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 ($\text{m}^3/\text{hr}^{-1}$) 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 1 shows the outcome of the application of the methodology in Part 1 and the refinement using reed vapour pressure, as set out in paragraph 6, to commonly stored liquids.

Table 1 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 |
| Gasoline | Methanol |
| Methyl ethyl ketone | Reformat (full range) |
| Naphthas | Reformat (heavy) |
| Reformat (worst case – light) | Special boiling point 3 |
| Natural gas liquids (condensates) | |

| | |
|-------------------------|--|
| Methyl ethyl ketone | |
| Methyl tert-butyl ether | |
| Pentane | |
| Special boiling point 2 | |
| Toluene | |

Appendix 2: Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric storage 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 61508⁹ and 61511.² 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 layer of protection analysis (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 (SIL) 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 1). 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*.⁴⁰ This appendix draws extensively on the guidance given in the book. However, 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.

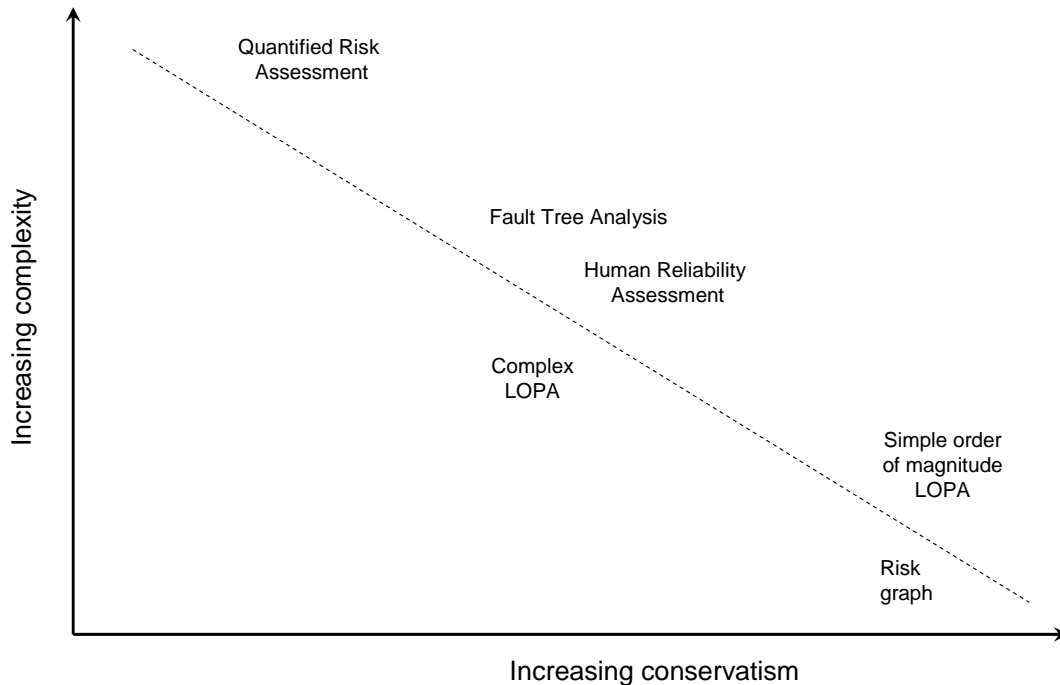
7 LOPA is often used to identify the shortfall in meeting a predetermined dangerous failure target frequency. For the purposes of this guidance, this shortfall, if it exists, is associated with the average probability of failure on demand of a demand mode safety function required to meet the target dangerous failure frequency. The identified shortfall is equated to the random hardware failure probability component of a safety integrity level (SIL), 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. 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 1 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 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_i^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 safety instrumented system (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*,⁴¹ 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. Consequence modelling is required or a Buncefield-type explosion assumed to help determine this. Uncertainties are present in all calculations but sensitivity analysis can be used to help reduce 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 and dispersion modelling. Also, as the analysis becomes more complex, it may prove harder to provide long-term assurance that the assumptions in the assessment 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 and perform as originally expected.

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 2).

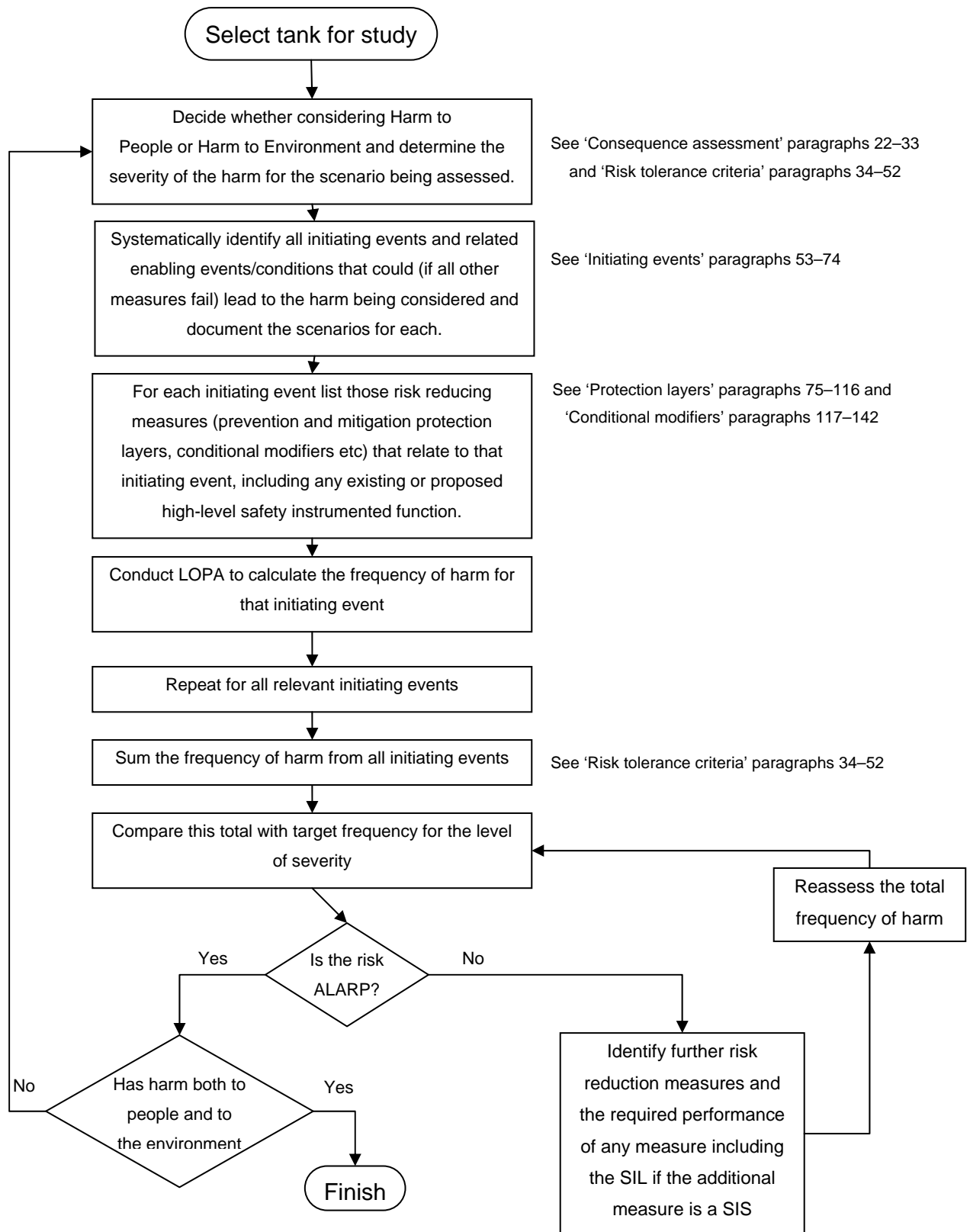


Figure 2 Flowchart for application of LOPA process

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, many of which will not arise from the kind of explosion that happened at Buncefield. 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 from the ensuing pool fire.
- 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.

It should be noted that when scenarios are selected for LOPA study, it is still necessary to consider events such as pool fire, flash fire as well as explosion.

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:

- 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 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.
- 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 an Individual Risk target 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.
- 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.

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 112–116) and conditional modifiers (probability of presence and probability of fatality, see paragraphs 136–141) are applied.

26 For a scenario-based assessment, there may be no single value for a given factor 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

27 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 (RR718⁴²). The available evidence suggests over-pressures of at least 200 kpa within the flammable cloud, but rapidly decaying outside the cloud.

28 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*.⁴³ 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.

29 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. Nor can the behaviour of the explosion in the near-field be reproduced by more commonly used models such as the multi-energy model. Therefore it is proposed that consequence assessments are based on the experience of the Buncefield incident.

30 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.

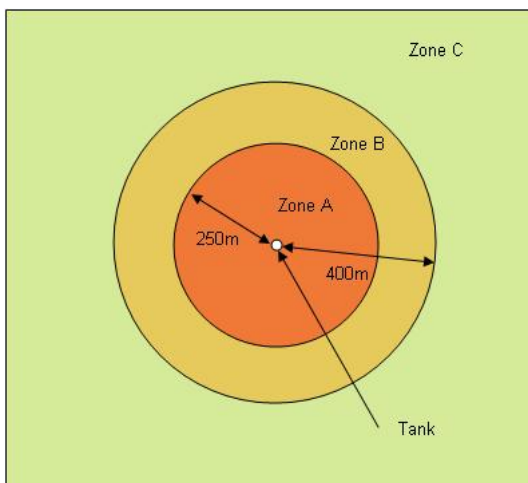
31 The following distances (Table 1) are considered to be a conservative approximation of the hazard zones for a Buncefield-type explosion and, in the absence of other information, are recommended as a method by which operators can determine relevant hazard zones.

Table 1 Hazardous zones for a Buncefield-type explosion

| Zone name | Zone size (measured from the tank wall) | Comment |
|-----------|---|--|
| A | $r < 250 \text{ m}$ | 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 | $250\text{m} < r < 400 \text{ m}$ | 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 | $r > 400 \text{ m}$ | 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 3). Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach.

Figure 3 Hazardous zones for a Buncefield-type explosion



32 The zones within Table 1 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 1 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 1 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. Typical, automotive, internal combustion engines are not a reliable source of ignition.
- Duration and rate of transfer into the tank. The quantity of petrol that overflowed Tank 912 at Buncefield during the 40 minutes from initial overflow to ignition was approximately 300 tonnes. If the transfer rate or overflow duration is estimated to be significantly different, then this may affect the formation and size of the cloud. An estimate of cloud generation could be made based on the 'HSL entrainment calculator' and a 2 m cloud height (for further information see Appendix 1).

33 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 hazards 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 125). Additionally, sensitive populations just beyond the 250 m, eg a school or old people’s home, should also be considered.

Environmental consequences

34 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 Competent Authority Policy on Containment of Bulk Hazardous Liquids at COMAH Establishments*⁴⁴).

Risk tolerance criteria

General

35 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.

36 Regulation 4 of the COMAH Regulations requires dutyholders to ‘take all measures necessary (AMN) to prevent major accidents’. This is equivalent to reducing risks ‘as low as reasonably practicable’ (ALARP). HSE’s semi-permanent circular *Guidance on ALARP decisions in COMAH*⁴⁵ 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’.

37 See also paragraphs 108 and 109 of *A Guide to the COMAH Regulations* L111.⁴⁶

38 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 24.

Scenario-based safety risk assessment

39 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 2).

Table 2 Risk matrix for scenario-based safety assessments

| Likelihood of ‘n’ fatalities from a tank explosion per tank per year | Risk tolerability | | |
|--|--------------------|--------------------|--------------------|
| $10^{-4}/\text{yr} - 10^{-5}/\text{yr}$ | Tolerable if ALARP | Tolerable if ALARP | Tolerable if ALARP |
| $10^{-5}/\text{yr} - 10^{-6}/\text{yr}$ | Broadly acceptable | Tolerable if ALARP | Tolerable if ALARP |
| $10^{-6}/\text{yr} - 10^{-7}/\text{yr}$ | Broadly acceptable | Broadly acceptable | Tolerable if ALARP |
| $10^{-7}/\text{yr} - 10^{-8}/\text{yr}$ | Broadly acceptable | Broadly acceptable | Broadly acceptable |
| Fatalities (n) | 1 | 2–10 | 11–50 |

40 Table 2 is based on HSE’s *Guidance on ALARP decisions in control of major accident hazards (COMAH)* SPC/Permissioning/12. Note that a scenario with a single fatality is not an

Individual Risk calculation for a specific individual; it is an aggregation over all personnel affected by the scenario.

41 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 should be considered. This may be adequately addressed by the individual and societal assessments detailed below, but may require a separate assessment.

Individual Risk assessment

42 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.

43 The relationship between a scenario-based safety risk assessment (ie the likelihood that a single major accident hazard results in a fatality) and the risk to a particular individual (Individual Risk) is presented below. This simplified approach can be used to determine the Individual Risk at an establishment (the likelihood of fatality for the 'most at risk' individual).

| | |
|---|--|
| Likelihood of fatality for a specific individual due to a single major accident hazard scenario | f |
| Percentage of year individual is at work | t |
| Number of fatal major accident hazard events the individual is exposed to at work | n |
| Aggregate likelihood of fatality for the specific individual (Individual Risk). | $F = t \times \left(\sum_{i=1}^n f_i \right)$ |

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 consequences. 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 Competent Authority.

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 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 2003.⁴⁷ The tolerability criteria from this reference is summarised in matrix form in Table 3 below. Further guidance on environmental risk matrix can be found in Annex 5 of HSE's SPC/Permissioning/11.⁴⁸

52 Dutyholders seeking to demonstrate compliance with the COMAH Regulations should adopt an approach consistent the information provided in Tables 3 and 4 and with that in their COMAH safety reports and pollution prevention control permit applications.

Table 3 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 | $\sim 10^{+1}$ to 10^{-2} per year | $\sim 10^{+1}$ per year |
| 1 | Minor | All shown as acceptable | - | - |

53 For the purposes of this guidance, the categories from Table 3 have been aligned to COMAH terminology as follows:

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

Table 4 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 BAT⁴⁷

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 (in hours/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 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 (depending on what checks are done) 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 either a fully automated control system or 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. 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 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 should be considered as a contributing factor to the reliability claimed for the operator in carrying out the basic process control function, and are therefore part of the basic process control system.

71 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. In such cases, the failure rate for the action no longer relates to the failure of the operator but becomes only the failure rate of the feature. It is

important to identify this type of situation to avoid making reliability claims which include both the operator and the 'feature'.

The role of cross-checking

72 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).

73 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.

74 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.

75 Various human reliability assessment techniques may be used to evaluate the effectiveness of cross-checking activities – eg THERP (technique for human error rate prediction). 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

76 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.

77 Note that the requirement for all rules 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*.

78 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.

79 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.

80 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.

81 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.

- 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).

- The simplest application of LOPA requires absolute independence between protection layers and between protection layers and initiating events. Therefore if the prospective protection layer shares a common element with another protection layer (eg a sensor, human operator, valve) or initiating event, no risk reduction credit could be taken for the prospective protection layer. Instead, its performance would have to be included as part of the initiating event or other protection layer.
- A more detailed application of LOPA requires 'sufficient' rather than absolute independence between protection layers or between a protection layer and an initiating event. Sufficiency is not explicitly defined, but would have to be demonstrated taking into consideration the principles in clauses 9.4 and 9.5.1 of BS EN 61511-1 and 61511-2. 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 at different points of the analysis.
- 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?
- 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 (valve). 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

82 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 they 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.

83 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 57–59).

The basic process control system as a protection layer

84 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 or 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.’

85 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.

86 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 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.

87 Claims for risk reduction achieved by the BPCS should in conformance with BS EN 61511-1 9.4.2 and 9.5.1.

Response to alarms

88 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.

89 Where process alarms are delivered through the BPCS, consult Annex 5 for the requirements for independence when credit is being claimed for more than one function implemented through the BPCS. The analysis should meet the requirements of Clauses 9.4 and 9.5 in BS EN 61511-1 and BS EN 61511-2.

90 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.

91 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 element which appears in a succeeding protection layer or any failed component of a previous protection layer.
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 BPCS failure 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).

92 Some tank monitoring systems include ‘unscheduled movement’ alarms and systems which monitor for ‘stuck’ tank gauges. These systems are not designed or maintained in accordance with BS EN 61511 and so the risk reduction credit which can be taken for them is limited accordingly. These systems rely on human input to provide the status of each tank, and response to them is typically by the same operator who is overseeing the filling operation. Therefore it is suggested that they are considered as part of the normal control arrangements and process alerts, which are included in the BPCF, where they may contribute to any risk reduction claimed for the BPCF.

Safety instrumented systems

93 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 a SIS that does not comply with BS EN 61511 would have a reliability assessment associated with it, and would have to be assessed to determine the performance level that could be claimed.

Other safety-related protection systems

94 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 75–80 of this appendix. Such protection layers are referred to as ‘other technology’ in BS EN 61511 and are not subject the performance limits required by BS EN 61511, eg pressure relief valves.

Mitigation layers

95 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);
- 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.

96 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; and
- properly designed to prevent the undesired consequence;
- effective in preventing the undesired effect; and
- tested periodically to assure continued effectiveness.

97 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

98 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.

99 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.

100 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.

101 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.

102 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 gas 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.

103 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. Therefore consideration needs to be given to the emergency exercise and operator training programs in place.
- 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?);
- the means of communication between operators (eg radio or telephone), if more than one operator is involved. The reliability and effectiveness of communications should be included in the consideration of the potential effectiveness of action in response to the detection of an overflow;
 - 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

104 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.

105 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

106 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.

107 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. Note that the Department of Environment, Transport and the Regions definition of a MATTE (in *A guide to risk assessment and risk management for environmental protection*⁴⁹) due to the impact on ground water is not dependent on whether the ground water is used for any purpose.

108 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.

109 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 split material (if it is safe to do so) and the extent to which loss of integrity may occur for the event being considered.

110 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.

111 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.

112 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

113 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.

114 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?

115 Any credit taken for warning and evacuation systems should be fully justified in the LOPA report (eg *Guidelines for Consequence Analysis of Chemical Releases*⁵⁰).

116 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.

117 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

118 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.

119 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.

120 The use of a given conditional modifier may not be appropriate in all circumstances depending on the type of calculation being performed. See paragraphs 24–25 of this guidance.

121 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 22–33 of this appendix).

122 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

123 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.

124 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 CRR133⁵¹). 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.

125 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.

126 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

127 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.

128 As a general rule, as the size and duration of a Buncefield-type release increases the probability of ignition will increase, eventually tending towards 1.0. For shorter duration large releases, some available data has been quoted in LOPA studies by operators based on Lees' *Loss Prevention in the Process Industries*⁵² 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.

129 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, assumptions 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 including 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

130 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*⁵³ and section 8.1.3 of *A risk-based approach to hazardous area classification*⁵⁴), 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.

131 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.

132 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.

133 Where a more detailed estimate of ignition probabilities is required further information is given in the HSE's research report CRR201⁵⁵ and the Energy Institute's *Ignition probability review, model development and look-up correlations*. However, it should be noted that these publications are both pre-Buncefield and therefore may not be fully relevant. 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

134 The reasons why the vapour cloud at Buncefield exploded as opposed to burning as a flash fire are not fully understood. Factors such as ambient temperature; cloud size, shape, and homogeneity; topography; congestion (including that from vegetation); droplet size; fuel

properties; and weather conditions may have a significant effect on the probability of an explosion compared to a fire.

135 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 process and offshore 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.

136 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 under significantly different weather conditions. 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

137 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 112–116). 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.

138 Where the risk to a specific individual worker is being considered (Individual Risk), 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.

139 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.

140 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

141 This conditional modifier is often referred to as ‘vulnerability’.

142 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

143 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

144 The process should be repeated for the other scenarios as outlined in paragraph #, where a given hazardous event can be caused by two or more initiating events. It must be remembered that the resulting predicted frequency of the unmitigated hazardous 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 34–52).

145 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 conservative assumptions. Sensitivity of assumptions on initiating events and consequence side of a risk assessment are also required.

Concluding the LOPA

146 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.

147 The LOPA should provide the basis for the safety requirements specification of the safety instrumented systems (where required). This should include:

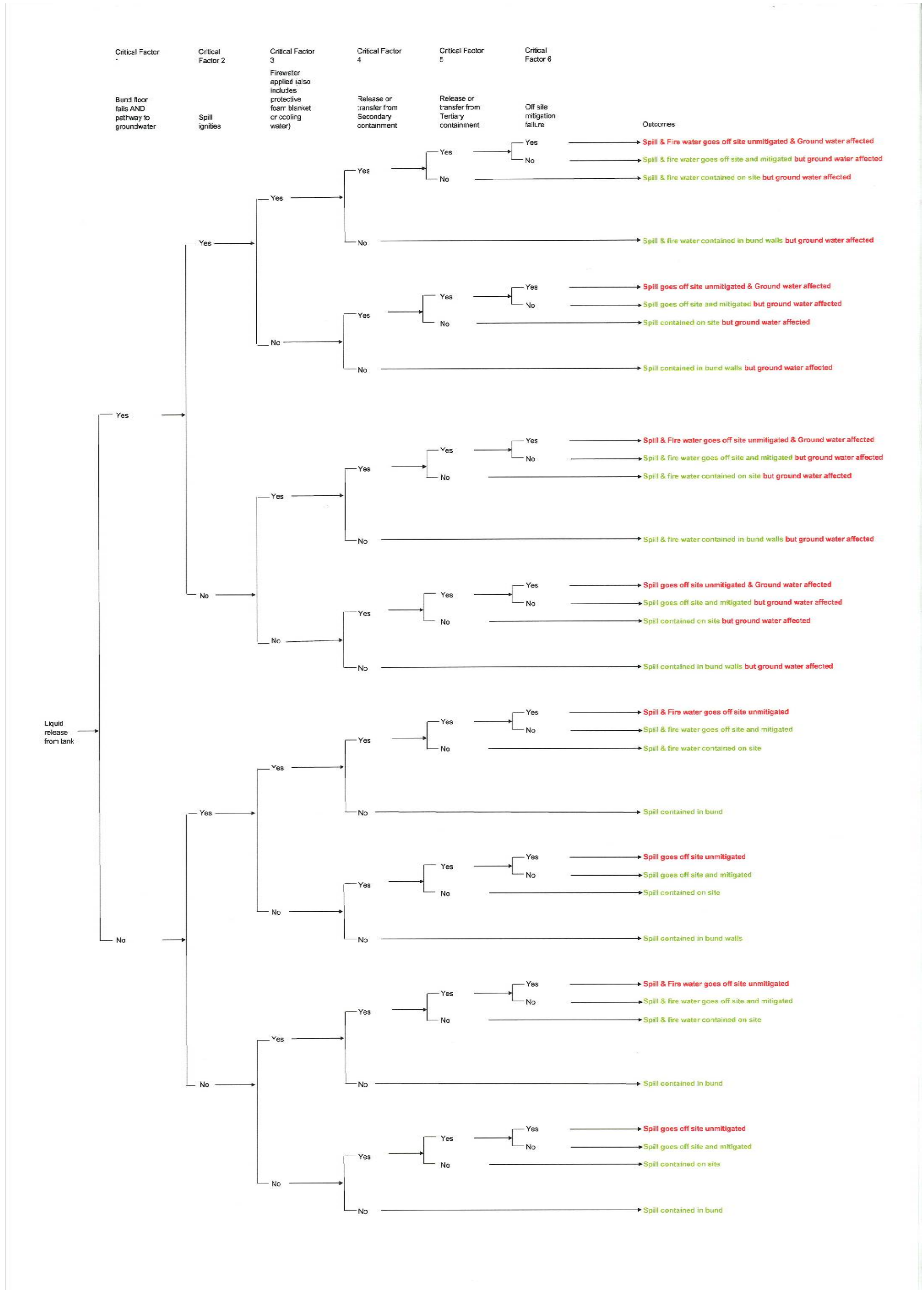
- clear definition of the SIL level required for the safety instrumented system in terms of reliability level, eg probability of failure on demand (PFD);
- it should also provide the basis of the functional specification of the SIS.

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

148 HSE reviewed a number of early LOPA studies of overfill protection completed following the Buncefield incident (see RR716⁵⁶). 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 automatic tank gauging (ATG) errors and failures;
- incorrect logic used to combine various factors;
- incorrect handling of number of filling operations;
- difficulty in analysing time at risk ie filling duration;
- uncertainty of ignition probability;
- uncertainty of probability of fatal injury;
- uncertainty of occupancy probability;
- uncertainty of probability of human detection of overflow;
- unjustified valve reliability;
- data not justified by site experience;
- no consideration of common cause failures of equipment;
- inappropriate risk targets;
- all hazard risk targets applied to single events;
- incorrect handling of risk targets eg sharing between tanks;
- difficulty in estimating probability of vapour cloud explosion; and
- difficulty in establishing and verifying all initiating events (causes).

Annex 2 Critical factors for environmental damage from a tank overflow



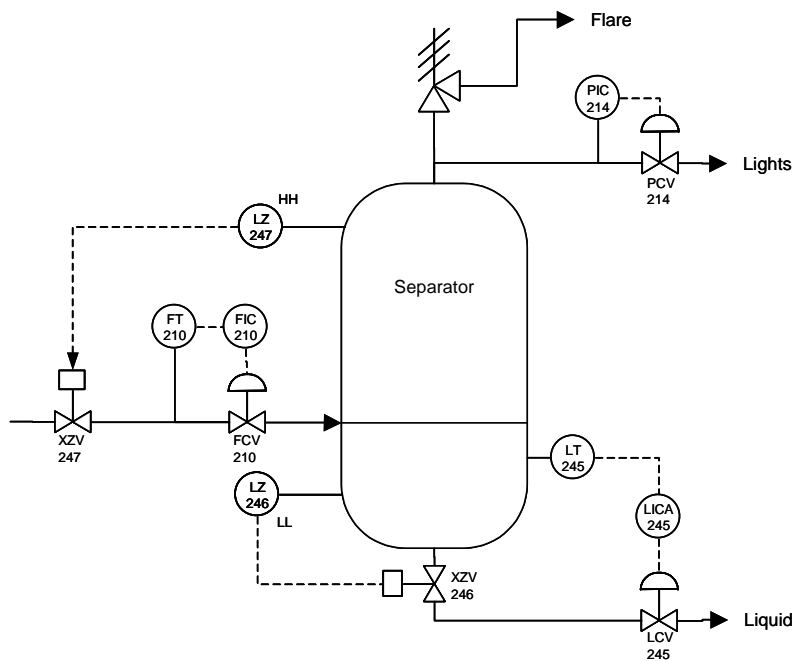
Annex 3 Demand tree methodology for systematic identification of initiating causes

149 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

150 Figure 4 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 4 Simplified process schematic



151 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 exist from the vessel.

152 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 which protects against liquid entering the vapour line.

153 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’

154 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.

155 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

156 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 5 below may be used as a prompt to assist the systematic process.

Table 5 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 | | | | |

157 In Table 5 services could include any or all of the following:

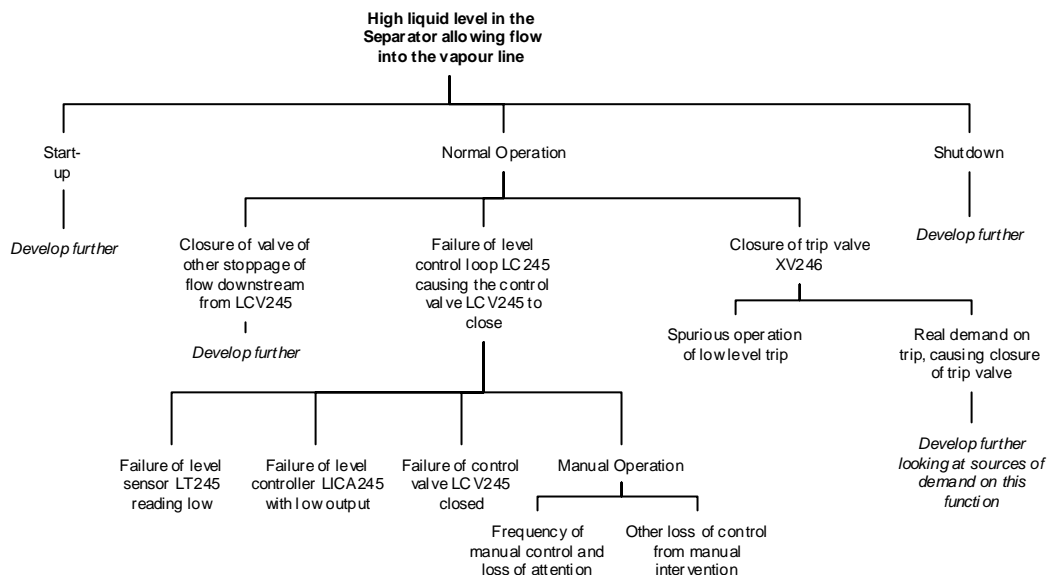
- loss of electrical power;
- loss of steam;
- loss of instrument air;
- loss of cooling water;
- other.

Example demand tree

158 Figure 5 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.

159 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 5 Demand tree illustration



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

161 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

162 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’

163 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.

164 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.

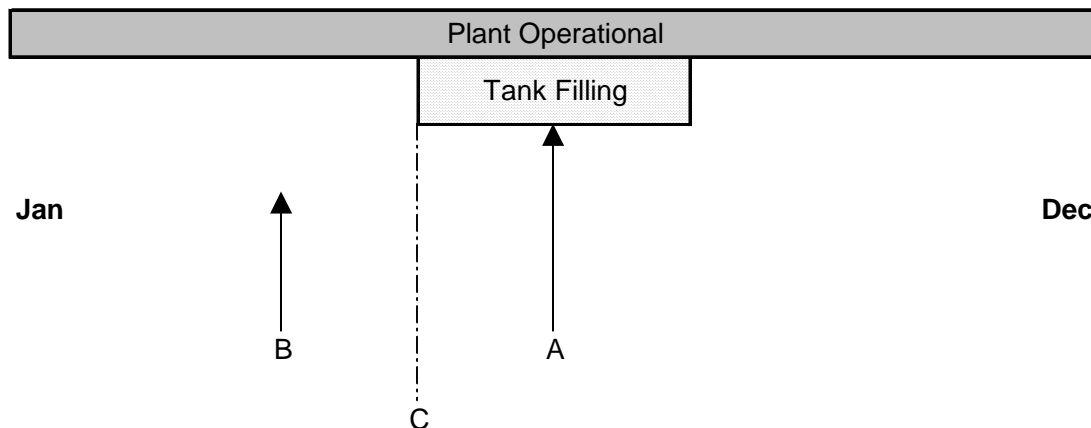
Failure of equipment

165 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.

166 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 then 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.**

167 Figure 6 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 6 Equipment item failure



168 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.

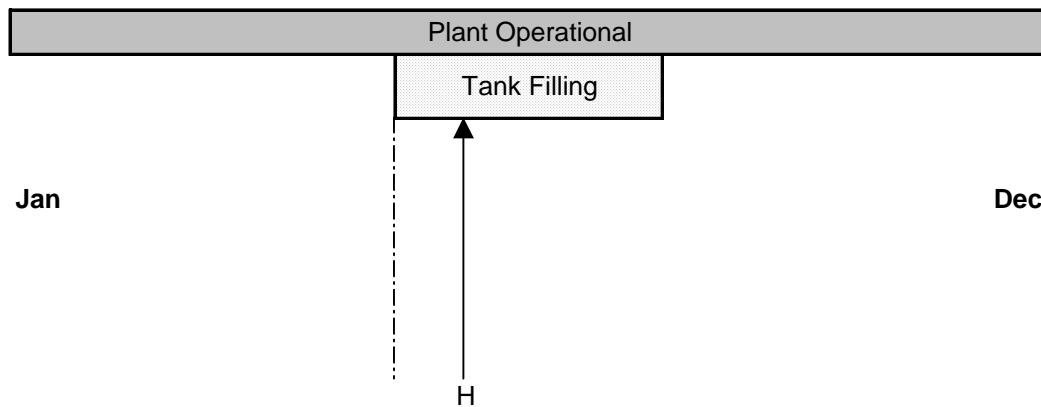
169 If detection at time C is carried out with a high degree of reliability by some form of checking operation (eg independent gauging or stock checks) then it can be assumed that only gauge failures that occur during tank filling can affect the filling operation. The checking activity fulfils a similar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

170 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 as $t/8760$. 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

171 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 7 Human action



172 The human task of controlling the filling operation to stop at the intended level is represented in Figure 7 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.

173 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

174 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

175 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 LOPA on presents two approaches for the application of LOPA. Approach 'A' generally meets the requirements of BS EN 61511. The CCPS LOPA book also presents (with caveats) a less conservative approach. 'Approach B', which does not meet 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.

176 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 be considered.

Programmable electronic systems

177 Credit can be given to more than one control function implemented through the BPCS where there is sufficient rather than complete independence. With regard to any programmable electronic systems that are part of the BPCS the following requirements) should be met.

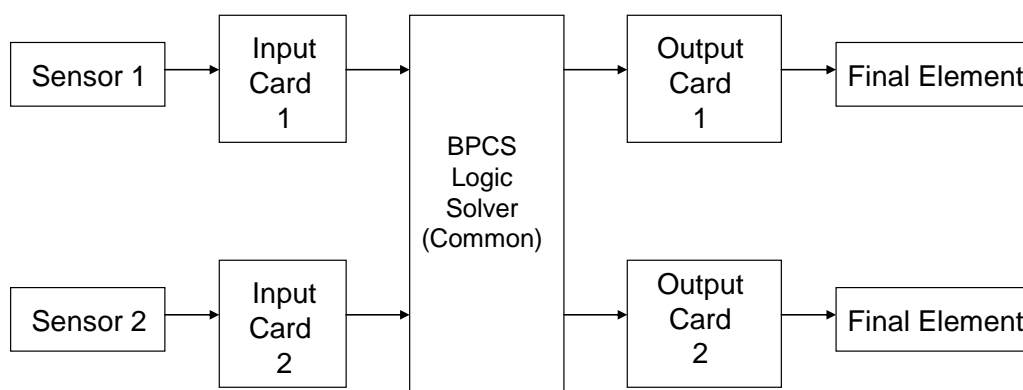
- There should be formal access control and security procedures for modifying the BPCS. The access control procedures should ensure that programming changes are only made by trained and competent personnel. The security procedures should prevent unauthorised changes and should also ensure software security, 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.
- Where the BPCS functions share a common I/O card, they should not be treated as independent functions unless sufficient reliability can be demonstrated by analysis.
- The BPCS logic solver should have sufficient redundancy to deliver a PFD of no more than 1×10^{-2} . This should be demonstrated by analysis and is likely to require redundancy of cards and power supplies within the programmable electronic system.
- 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 be in conformance with BS EN 61511-1 9.4.2 and 9.5.1.

178 Figure 8 illustrates what the application of these principles could require in practice.

Figure 8 Possible structure of independent control functions within the BPCS



179 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 8, 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.

180 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.

181 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.

182 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

183 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).

184 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.

185 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.

186 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

187 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.

188 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.

189 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.

190 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.

191 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

192 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?'

193 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.

194 The error may be:

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

195 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.

196 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 tells 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.

197 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.

198 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.

199 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.

200 The Table 6 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 6 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 6 Levels of cross-checking effectiveness

| Level of checking |
|---|
| No justifiable reason why the checker should identify the failure when the person carrying out the original action has not. |
| The checker is able to verify the correct course of action that should have been undertaken by a different means from the person carrying out the original action. Checker has a common link with the person carrying out the original action or there is reason to believe that there is a high likelihood that the checker will be influenced in the same way as the person carrying out the original action. |
| Checker has a weak link with the person carrying out the original action or there is reason to believe that there is a moderate likelihood that the checker will be influenced in the same way as the person carrying out the original action. |
| Checker has sufficient independence from the person carrying out the original action and the check is designed to highlight errors that may have occurred. |

201 **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

202 The first of these two steps requires an element of task analysis. This starts by identifying which tasks are critical tasks in relation to the overflow event. In this context, a critical task is one in which a 'failure' can trigger a sequence leading to the hazardous event being considered – the overflow scenario. The identification of critical tasks is best achieved during the development of a demand tree, as described in Annex 3.

203 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 7 shows an example.

Table 7

| 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 filling the tank under review which has too little ullage and causing the tank to overflow. |
| | | |
| | | |
| | | |

Review of each critical task

204 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.

205 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 8):

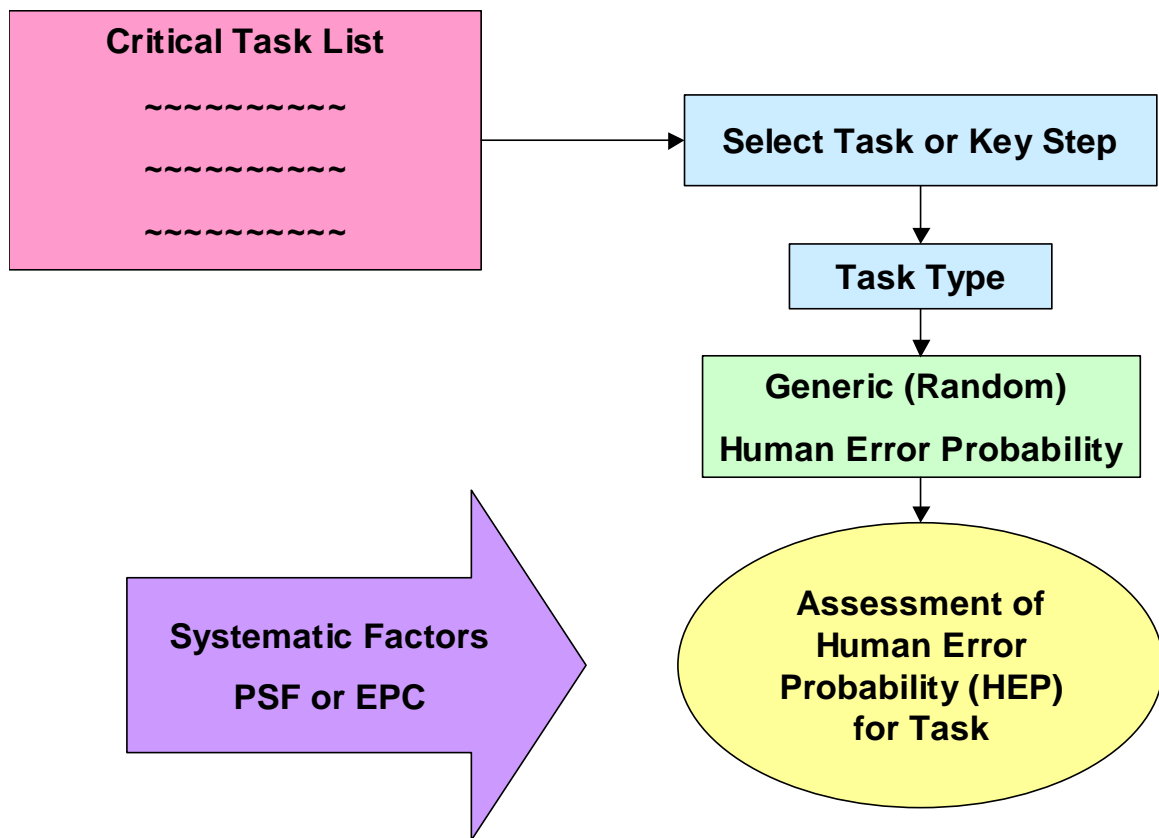
Table 8 Critical task list

| 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 filling 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

206 Figure 9 illustrates the process of assessing the human error probability (HEP) for the critical task or key step within the task.

Figure 9 Process for assessing human error probability



207 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.

208 There are a number of standard methods such as APJ (absolute probability judgment), HEART (human error assessment and reduction technique), THERP (technique for human error reliability prediction) 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

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

- task frequency (/yr);
- human error probability (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.

210 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:

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

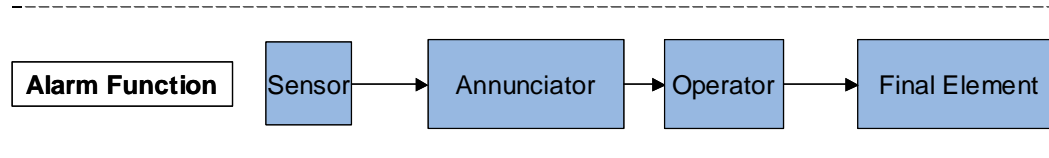
Note that enabling events or conditions can be included in the task frequency (the number of times the activity is carried out under operational conditions which could lead to the undesired consequence) and do not require separate identification.

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

Annex 8 Response to alarms

212 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 10.

Figure 10 Alarm function



213 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.

214 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

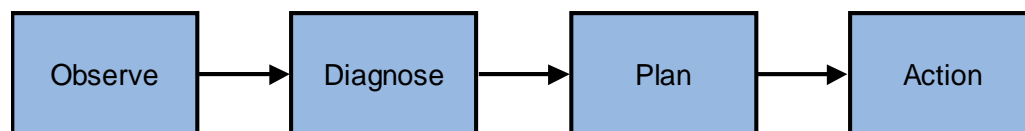
215 Before proceeding with the analysis of the performance of the alarm function, the required function should be carefully defined. It is not enough simply to identify an instrument and consider that as a protection layer. The protection layer will need to make up a complete loop and should therefore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

216 Operator response to an alarm contains four sub-tasks as illustrated in Figure 11.

Figure 11 Sequence of operator sub-tasks

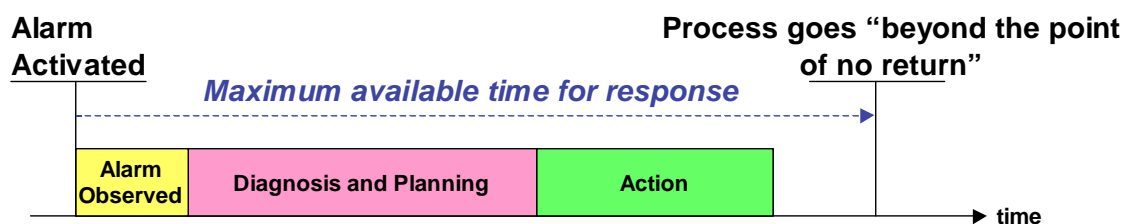


- **Observe:** The first of these sub-tasks, observing the indication, is relatively quick to do, so long as an operator is present to hear or observe the indication. However, it does rely on the indication of the alarm being clear and not being hidden by other alarms or information being communicated 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

217 The key consideration relating to ‘time for response’ is an understanding of the maximum time available from when the alarm is activated until the process goes ‘beyond the point of no return’. This is illustrated in Figure 12.

Figure 12 Time for response to alarm



218 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 (Human Error Assessment and Reduction Technique) methodology.)

219 It is suggested that the 'Maximum available time for response' is a minimum of 20 minutes. Note that the required amount of time needs to be evaluated on a case by case basis and it may be considerably longer.

220 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

221 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 3) 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.

222 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 covering each of the four sub-task elements: 'Observation', 'Diagnosis', 'Planning', and 'Action'; this is a specialist activity.

223 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-1278.⁵⁷

Additional notes

224 PSLG support the recommendation of EEMUA 191⁵⁸ in that it considers that SIL 2 or higher cannot be claimed for a SIF that includes operator response. (EEMUA 191 table 5, p14.)

225 If an alarm protection layer is not a complete (ie having all four elements shown in Figure 11) 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).

226 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.

227 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 $10\,000 \text{ m}^3$ 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 $1200 \text{ m}^3/\text{hr}$.

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 $2.43 \text{ m}^3/\text{hr}$.

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 61511² 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.

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 70–75 in the main report sets out the overall requirement for overfill protection. Tanks storing gasoline 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 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 basic process control system (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 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 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.

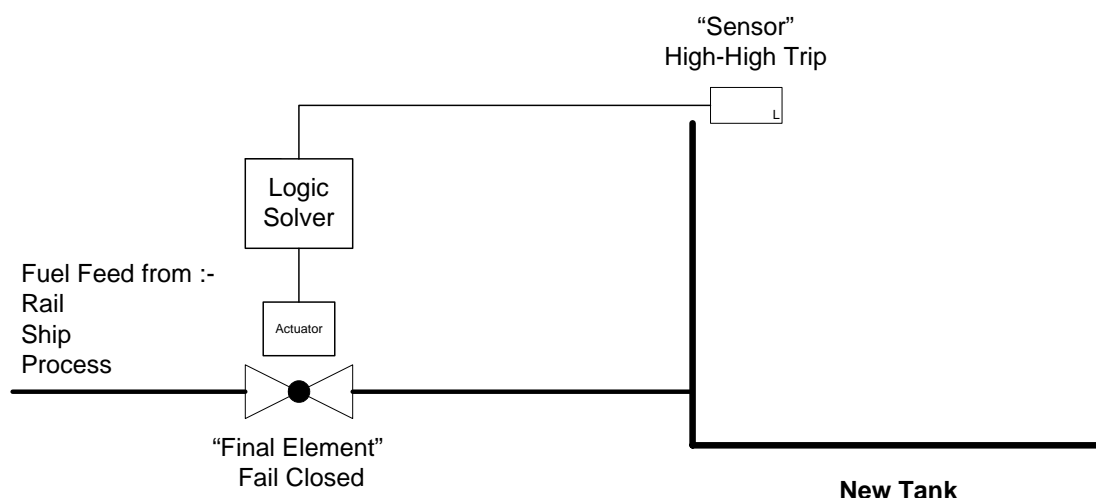
Architectures of overfill protection systems

New tank automatic overfill protection system

10 New tank automatic overfill protection systems should meet the requirements of paragraph 7.

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 1 High-high level trip



12 Figure 1 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 A functional safety assessment should be carried out in accordance with BS EN 61511.

14 A gap analysis should be conducted to determine if the existing system complies with BS EN 61511.

15 Where an existing tank meets the requirements set out in paragraphs 70–75 of the main report in all respects other than fully complying with BS EN 61511, then the following issues should be considered.

16 For SIL 2 or higher the installation should fully comply with BS EN 61511.

17 To add an automatic overfill protection to an existing tank the design should be as for a new tank installation, refer to paragraphs 10–12.

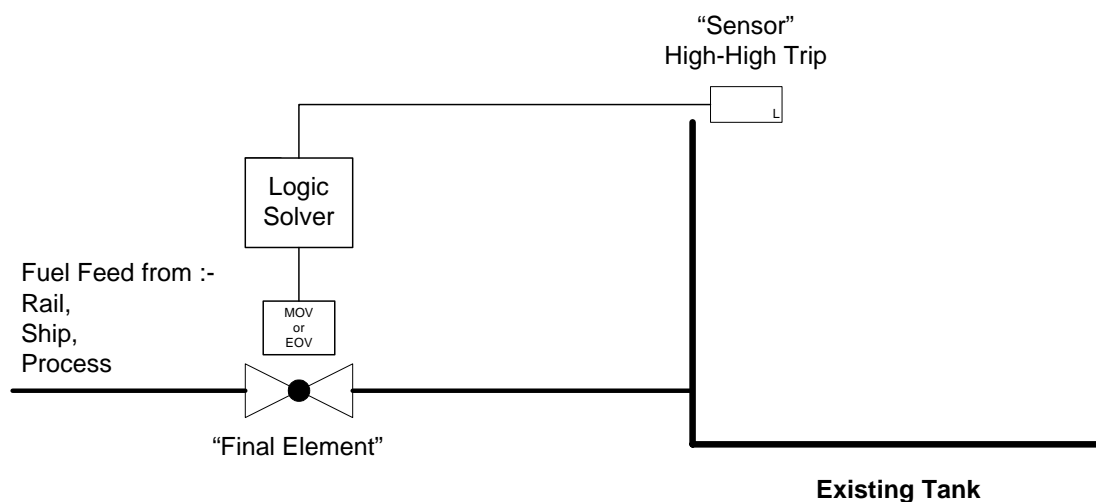
18 Should the cost of implementing an overfill protection system to an existing tank to fully meet the requirements of BS EN 61511 be demonstrated to be grossly disproportionate then further risk reduction may still be appropriate using existing equipment to provide automated overfill protection meeting BS EN 61511 so far as reasonably practicable. 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 existing logic solvers;
- degree of independence from BPCS;
- demonstration and evidence of prior use;
- suitability of final elements: Can the existing valves be made 'fail-safe' or alternative measures taken?

19 It should be noted that a prescriptive description of the steps needed to meet BS EN 61511 so far as reasonably practicable can not be provided in this guidance. The degree of compliance should be discussed and agreed between the dutyholder and the Competent Authority on a case by case basis.

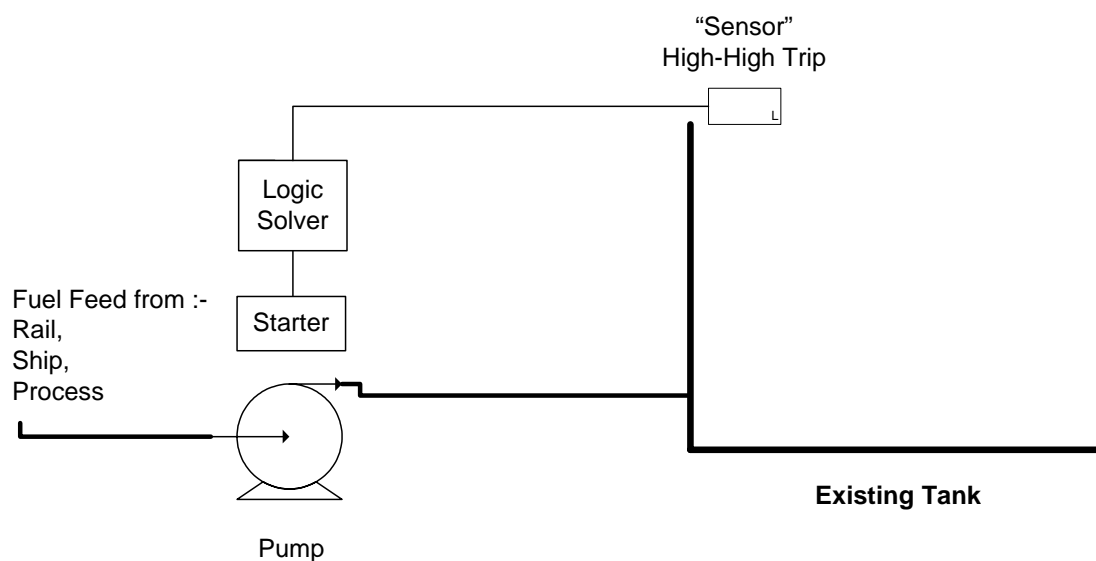
20 Use of electrical motorised valve MOVs/EOVs: Figure 2 shows an overfill protection system using an electrically operated valve for isolation.

Figure 2 Electrically operated valve final element



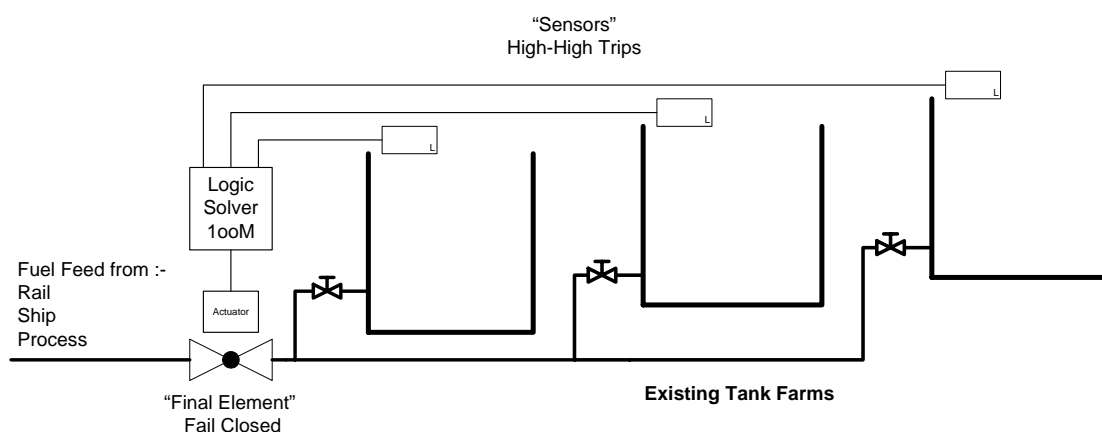
21 Use of supply pump: Figure 3 shows a supply pump that can be used as the final element of an automatic trip system where it can be demonstrated that the gravitation feed through the stopped pump does not continue with an unacceptable overfill rate. This system should be followed with manual closure of an isolation valve.

Figure 3 Supply pump as final element



22 Multiple tanks:

Figure 4 Use of a single final element (valve or pump) to isolate multiple tanks. Any sensor trips the final element



Lifecycle maintenance

23 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 principle activity of maintenance is proof testing to identify any dangerous unrevealed 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

24 Overrides during tank filling should not be used. 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 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

25 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

26 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

27 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.

28 Proof testing should be end to end so far as is reasonably practicable including the detector at the liquid interface and the valve closure 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.

29 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, and exercise the system and demonstrate that the system will function as intended when required.

Test coverage

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

Part tests

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

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

Proof test method

33 This should be to carry out, where practicable, using wetted process conditions to operate the sensor. Where not practicable then simulated test of the sensor (eg radar,

vibronics or RF 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.

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

35 Testing should cover the testing of any diagnostic features.

36 Further guidance is in the HSE research report CRR428 *Principles for proof testing of safety instrumented systems in the chemical industry*.⁵⁹

Documentation

37 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 possible.

Recommended data sources for SIL calculations

38 Where a company does not have their own failure data, paragraph 42 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.

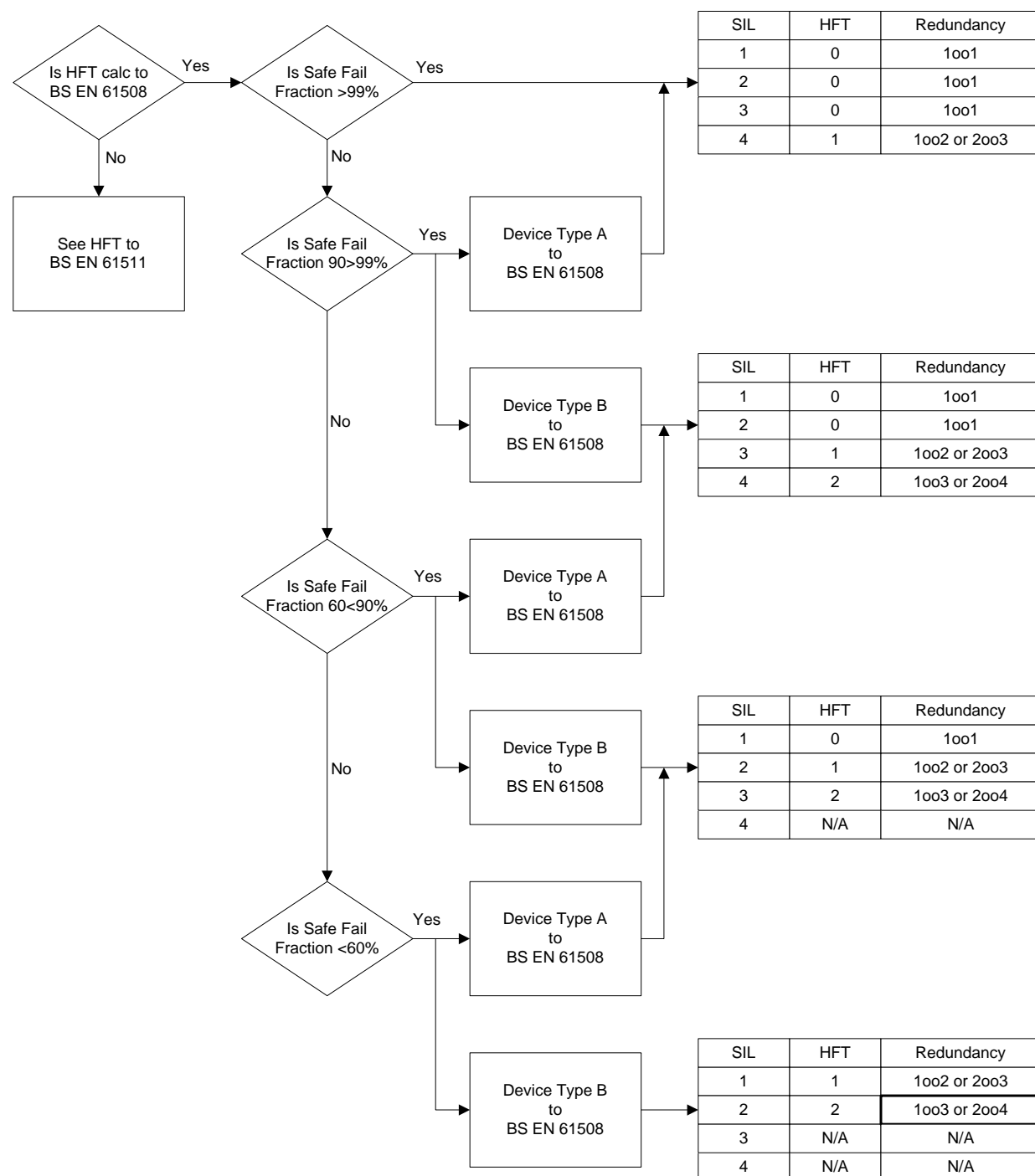
39 Users should consider the effect of the installed and process environment on the data used.

40 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.

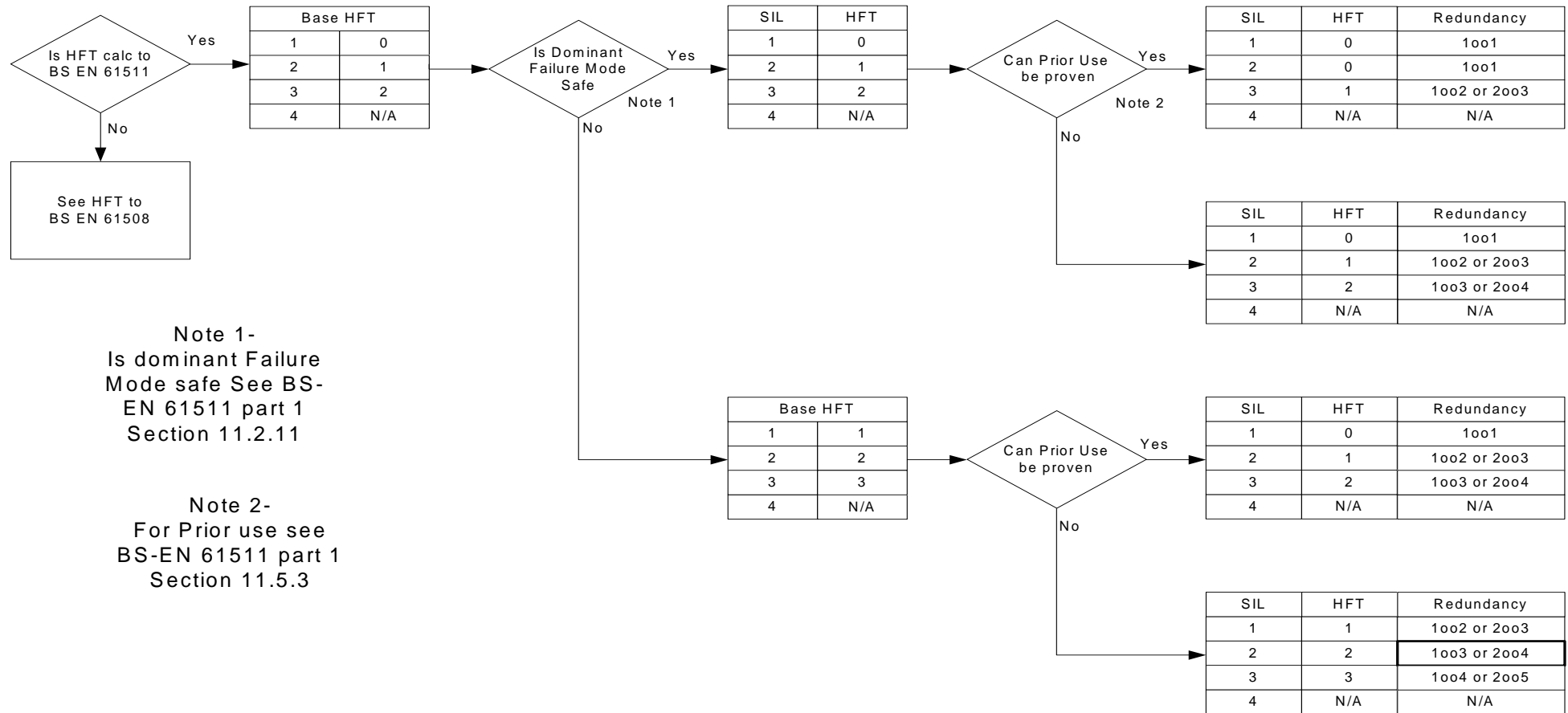
41 Suggested data sources for SIL calculations:

- *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 calculation to BS EN 61511 (for sensors, final elements and non-programmable Logic solvers)



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

42 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)

43 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.

44 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

45 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, PFD_S 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

46 For the example given in Figure 5 (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)

1oo2 architecture

47 For the example given in Figure 6 (1oo2 architecture) it can be shown that the average probability of failure on demand for a system with a very low failure rate is:

$$PFD_{G(1oo2)} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \left(\frac{T_1}{2} + MTTR \right)$$

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 $PFD_{G(1oo2)}$ is the average probability of failure on demand of the 1oo2 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 $PFD_{(avg)}$

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

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

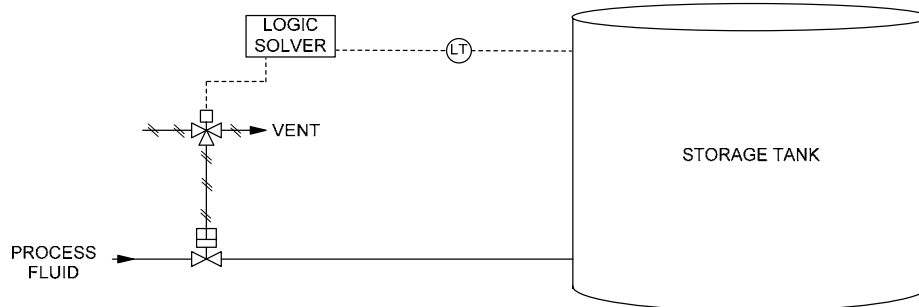
49 In the example below, the same instrumentation has been used but in two configurations to achieve a minimum of SIL 1, 1oo1 and 1oo2.

50 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.

1oo1 architecture

Figure 5 Typical tank overfill protection using 1oo1 architecture



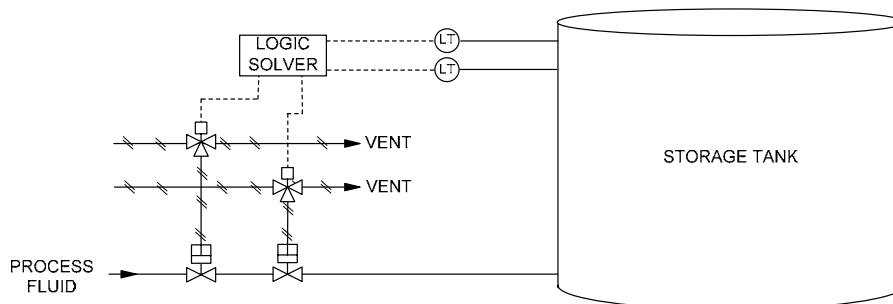
51 Using the $PFD_{(avg)}$ calculations and the assumptions stated previously, the following values for the $PFD_{(avg)}$ have been calculated for the 1oo1 architecture with a proof test interval of 1 year.

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

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

1oo2 architecture

Figure 6 Typical tank overfill protection using 1oo2 architecture



52 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 1 year.

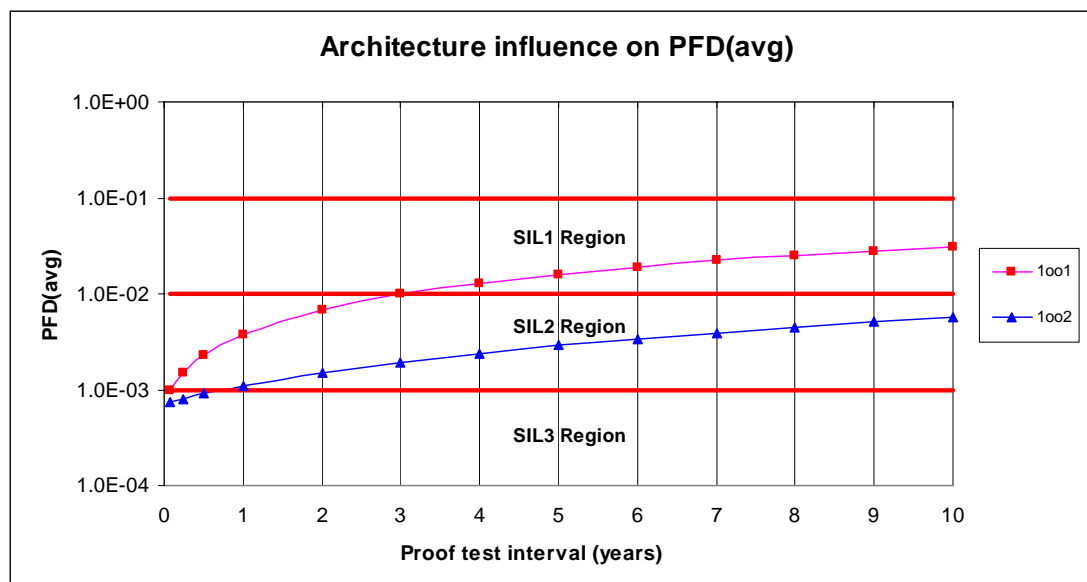
| | |
|-----------------------|----------|
| Sensor $PFD_{(1oo2)}$ | 3.82E-04 |
|-----------------------|----------|

Valve $PFD_{(1002)}$ 5.72E-06
 Total loop $PFD_{(avg)}$ 1.10E-03

53 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.

54 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 7 Effect of architecture and proof test interval on system $PFD_{(Avg)}$



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 MIIB *Design and operation*¹ 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 safety management system (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 Report⁶¹). Two key attributes of high reliability organisations (see 'Managing the unexpected'⁶²) 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 front-line 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 Report⁶² 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 (HSG48⁷) 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 7⁶³).

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* INDG277⁶⁴ 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 RR367⁶⁵ 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* HSG217⁶⁶ 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

The Center for Chemical Process Safety (CCPS) of the American Institution of Chemical Engineers (AIChE) guidance *Guidelines for risk based process safety*⁶⁷ 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).

24 The HSE internal document *Process safety management systems*⁶⁸ 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.

25 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

26 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

27 Prior to the Buncefield incident, the Safety Report Assessment Guide (SRAG) for highly flammable liquids⁶⁹ 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.

28 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*⁷⁰). 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.

29 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

30 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.

31 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/11⁴⁸ 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

32 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) (L111⁴⁶). 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.

33 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

34 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 overfill' etc.

35 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).

36 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).

37 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.

38 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)

39 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

40 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.

41 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.

42 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.

43 The evaluation of the safety-management-system (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

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

45 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

46 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.

47 The final Buncefield MIIB Report⁷¹ 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.

48 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 (RR086⁷²). 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.

49 Elsewhere, the gas plant explosion in Longford, Australia (*Lessons from Longford*⁷³) 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.

50 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.

51 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 competence*⁷⁴). Fitness may be impaired through, for example, drink, drugs or fatigue.

Guidance on roles and responsibilities

52 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.

53 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 191–204);
- 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.

54 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.

55 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.

56 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.

57 Industry guidance on human–computer interfaces (HCIs) (*Process plant control desks utilising human-computer interfaces*[#]) and alarm systems (*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.

58 The main source of guidance on supervision is *Successful health and safety management* HSG65.[#] 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.

59 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.

60 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 258–282.

Guidance on competence

61 HSE and Energy Institute Briefing Notes No 2,[#] CTI[#] and 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.

62 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.

63 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.

64 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[#]).

65 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.

66 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).

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

68 The Office of Rail Regulation (ORR) guide *Developing and Maintaining Staff Competence*[#] 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.

69 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.

70 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.

71 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.

72 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.

73 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.

74 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.

75 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.

76 The research report *Competence Assessment for the Major Hazard Industries* RR086[#] is also a very useful reference for COMAH sites. This appendix 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.

77 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.

78 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.

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

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

81 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.

82 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.

83 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).

84 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.

85 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.

86 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.

87 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).

88 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.

89 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 are also effective.

Summary

90 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.

91 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

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

93 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.

94 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 348/2001[#] was commissioned by the HSE to provide a method to demonstrate that staffing arrangements are adequate for hazardous scenarios as well as normal operations.

95 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,[#] the US Chemical Safety and Hazard Investigation Board's *Investigation Report, Refinery Explosion and Fire*[#]). 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'[#]). Shift work arrangements, and working conditions, should be such that the risks from fatigue are minimised.

Guidance on safe staffing arrangements

96 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*.[#] Other methodologies could also be used, provided they are robust.

97 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.

98 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 2 hours per scenario);
- benchmarking of 11 organisational factors using 'ladders' – this is a general assessment by the team and not scenario based (approximately 1 hour per ladder).

99 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.

100 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.

101 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.

102 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

103 An overview is given in Note 10 of HSEs *Human Factors Toolkit*.[#] More comprehensive guidance is given in *Managing shift work* HSG256,[#] and in the oil and gas industry guide *Managing Fatigue Risks in the Workplace*.[#]

104 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.

105 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.

106 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 Tool[#] and Epworth sleepiness scale.

107 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*,[#] or the oil and gas industry guide *Managing Fatigue Risks in the Workplace*.[#]

108 *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.

109 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).

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

Control room working conditions

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

112 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.

113 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.

114 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

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

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

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

Shift handover

118 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.

119 *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.

120 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.

121 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

122 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*.[#] 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.

123 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.

124 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.

125 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.

126 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

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

128 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

129 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.

130 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.

131 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.

132 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

133 *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.

134 HSE's Information Sheet *Organisational change and major accident hazards* CHIS7[#] sets out a framework for managing organisational changes, and is recommended for high-hazard industries.

135 *Principles for the assessment of a licensee's intelligent customer capability[#] and Contractorisation⁴* are documents used internally by HSE's Nuclear Directorate to assess and inspect contractorisation and intelligent customer issues.

136 *Managing contractors* HSG159[#] is a guide for employers in managing contractors in the chemical industry.

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

138 *Health and safety management systems interfacing[#]* provides a methodology for interfacing/integrating safety management systems between clients and contractors.

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

Organisational change

140 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.

141 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

142 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*.[#])

143 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*.[#])

144 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’.

145 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.

146 A dutyholder who proposes to contractorise 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.

147 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. The implication from the guidance is that the resource should be in-house.

148 *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.

149 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.

150 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.

151 This report also reviewed contractorisation in other high-hazard industries, including nuclear, offshore, and onshore chemicals.

152 A national passport scheme (the Client Contractor National Safety Group Safety Passport – www.ccnsng.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

153 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.

154 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

155 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.

156 This checklist deals with relevant elements of a safety management system (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.

157 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.

158 *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.

159 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.

160 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.

161 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

162 Dutyholders should ensure that there is a suitable policy and procedure for managing organisational changes.

163 Dutyholders should ensure that there is a suitable policy and procedure for retention of corporate memory.

164 Dutyholders should ensure that it retains adequate technical competence and 'intelligent customer' capability when work impacting on the control of major accident hazards is outsourced or contractorised.

165 Dutyholders should ensure that suitable arrangements are in place for management and monitoring of contractor activities.

166 Dutyholders should ensure that in addition to retaining intelligent customer capability, they consider using industry guidance for SMS interfacing where core business is contracted out.

167 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

168 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.

169 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.

170 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

171 *Guide to the COMAH Regulations* L111[#] summarises the range of changes that should be subject to management of change control procedures.

172 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.

173 As part of its commitment to process safety leadership, UKPIA has developed guidance and a self assessment tool for MOC.[#] 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.

174 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.

175 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 audit 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.

176 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

177 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

178 The Initial Report[#] of the Buncefield Major Incident Investigation Board 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

179 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.

180 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

181 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

182 Dutyholders involved in the transfer and storage of fuel should adopt good practice principles for safe management of fuel transfer.

183 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

184 Human factors issues are important at various safety-critical stages in fuel transfer operations including operational planning.

Guidance

185 Operational planning takes into account all stages of the plan development and approval, up to the stage of implementation via the consignment note.

186 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

187 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

188 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

189 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

190 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

191 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

192 The Initial Report of the Buncefield Major Incident Investigation Board[#] 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 177–182. These include the adoption of principles for consignment transfer agreements, as described below.

Guidance

193 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.

194 For the purposes of these agreements the sender is the party primarily responsible for the final transfer of fuel to the receiving terminal.

195 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.

196 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

197 Agreed in writing, between sender and receiver, as close as practicable to Stage 2 (for example, during the current or previous shift).

198 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.

199 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

200 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

201 Significant changes should be communicated between sender and receiver, and recorded by both parties.

202 The appropriate party should also record actions taken.

Summary

203 Dutyholders involved in the transfer of fuel by pipeline should develop consignment transfer agreement procedures consistent with good practice principles.

204 Dutyholders involved in inter-business transfer of fuel by pipeline should agree on the nomenclature to be used for their product types.

205 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

206 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

207 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.

208 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.

209 *Revitalising procedures*[#] 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

210 Procedures should be consistent with the sections of this appendix 'Principles for safe management of fuel transfer' (paragraphs 177–182) and 'Principles for consignment transfer agreements' (paragraphs 191–204).

211 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.

212 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

213 This requires an effective means of communication between sender and receiver, which should be achieved by means of a **consignment transfer agreement**.

214 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.

215 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

216 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.

217 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.

218 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.

219 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.

220 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 level alarm high (LAH) to avoid spurious activation of the alarm. (In this context alarms do not include alerts for process information).

221 Procedures should also be clear about the response required on LAH and level alarm high high (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

222 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.

223 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

224 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

225 All tank farms should ensure that there is a physical site check, to defined 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.

226 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

227 For each phase of the operation foreseeable 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.

228 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

229 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.

230 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

231 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

232 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)).

233 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.

234 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.

235 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.

236 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.

237 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.

238 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.

239 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.

240 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.

241 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.

242 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.

243 BS EN ISO 11064[#] 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.

244 In the absence of a more up-to-date company standard, procedure or specification, projects should follow this standard for new control rooms, and it can be usefully referred to for modifications and upgrades to existing ones, especially where there are known problems.

245 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.

246 Other parts of BS EN ISO 11064 deal with more detailed requirements, and may be considered as advanced references.

Guidance on alarm systems

247 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.

248 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).

249 The Energy Institute's *Alarm handling*,[#] and HSE's *Alarm handling*[#] and *Better alarm handling*[#] provide useful summaries of alarm handling issues with case studies.

250 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.

251 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

252 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

253 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.

254 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.

255 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

256 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

257 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

258 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

259 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.

260 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 U.S. 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.

261 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.

262 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.

263 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[#]).

264 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

265 Recommendation 10 of the MIIB's Design and Operations report asks the sector to 'agree with the competent authority 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 (CBS'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'.

266 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 the US, and this theme has been further developed in guidelines published by the Centre for Chemical Process Safety in December 2007.

267 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 leading 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.

268 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.

269 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.

270 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.

271 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.

272 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.

273 They should also include other key systems that may not be so 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

274 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

275 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.

276 OECD has also developed *Guidance on Safety Performance Indicators*[#] to assess the success of chemical safety activities.

277 **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.

278 **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.

279 **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

280 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.

281 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

282 Dutyholders should ensure that a suitable active monitoring programme is in place for key systems and procedures for the control of major accident hazards.

283 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

284 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.

285 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.

286 Investigation procedures should address both immediate and underlying causes, including human factors.

Guidance

287 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

288 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.

289 Other suitable references include *Human factors in accident investigations*[#] and *Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents*.[#]

Summary

290 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

291 The terms ‘audit’ and ‘review’ are used for two different activities (see L111[#] and HSG65[#]).

292 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.

293 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.

294 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.

295 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

296 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.

297 Various methods can achieve this. AIChE guidelines (*Guidelines for auditing process safety management systems*[#] and *Guidelines for technical management of chemical process safety*[#]) draw a distinction between process safety auditing, and process safety management systems (PSMS) auditing.

298 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).

299 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.

300 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.

301 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 (eg 3–5 years basis). 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 Competent Authority, parent companies or joint venture partners, insurers, trade associations), and the extensiveness of the active monitoring programme.

302 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

303 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.

304 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

305 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.

306 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)

307 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

308 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.

309 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

310 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

311 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.

312 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

313 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.

314 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

315 This step is important as it 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

316 Draw up a risk control matrix as illustrated in Table 1, to help decide which risk control systems are the most important in controlling the challenges to integrity identified within the incident scenarios.

Table 1 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

317 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.

318 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).

319 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?

320 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

321 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 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;
- flowrate 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 2 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 to required frequency. |
| 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. |

| Challenge to integrity | Lagging indicator | Leading indicator |
|---|---|---|
| 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: Reading list 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 www.energyinst.org.uk/

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 User's 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/content/files/bn7.pdf

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.ccnsq.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 HSE

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

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 User's 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 User's 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 www.energyinst.org.uk/content/files/guidancemay08.pdf

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

Route map to emergency planning guidance

Legal requirements for the production of on-site and off-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).

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 (LA) to produce an off-site plan. Full details of the COMAH Regulations and guidance on the legal requirements is given in *A guide to the Control of Major Accident Hazards Regulations 1999 (COMAH). Guidance on Regulations L111*.¹

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)* HSG191.²

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 LA 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)* HSG190.³

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 CHIS3.⁴ However, this document highlights the requirements in HSG191 as guidance for emergency plans.

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*⁵ (available from Emergency Planning College) and in *Dealing with disasters together* (Second edition),⁶ available from the Scottish Executive Office.

A brief summary of the key requirements from the main Health and Safety Executive (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.

Requirement for MAPP to give high level of protection to people.

| L111 ¹ | HSG191 ² | HSG190 ³ |
|--|--|---|
| <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

Health and Safety at Work etc Act 1974,⁷ Management of Health and Safety at Work Regulations 1999.⁸

Regulation 5(3)

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 paragraphs 3 and 4 of that Schedule.

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

CHIS3:⁴ 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)

MAPP shall be reviewed and revised where necessary in the event of significant modifications.

| L111 | HSG191 | HSG190 |
|---|--------|--------|
| 138: Reinforces when changes are required and references guidance under regulation 8(4) on what constitutes significant change. | | |

Regulation 5(5)

The operator shall implement the policy set out in their MAPP.

| L111 | HSG191 | HSG190 |
|--|--------|--------|
| 139: Emphasises must implement the policy in the MAPP. | | |

Regulation 5(6)

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

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/LA etc.</p> <p>240: Requires arrangements for communications with LA, 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>251, 256–259: Requires SMS to describe risk control systems for planning for emergencies.</p> |

Regulation 9(1)

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)

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)

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 /LA. 60–61: Suggests ways of working together on the plans. | |

Other documents

RCS8–41:⁹ refers to consultation with relevant statutory consultees.

Regulation 9(4)

The operator shall consult the LA (except where the LA 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 LA. | |

Regulation 10(1)

The LA, in whose area there is an establishment, shall prepare an off-site emergency 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 LA 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 LA 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)

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)

Operator must supply information to LA to allow off-site plan to be drawn up.

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: Describes 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)

Operator must supply any further information requested by the LA.

| 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)

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 LA with other responders. | |

Other documents

*Dealing with disaster together*⁶

Regulation 10(7), (8)

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)

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 LA 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> | |

Regulation 11(1) (continued)

| 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>181: Testing on-site and off-site plans at the same time can produce significant benefits.</p> <p>182: The objective of testing the plan should be to give confidence in:</p> <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> | |

Regulation 11(1) (continued)

| L111 | HSG191 | HSG190 |
|------|---|--------|
| | <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)

LA 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

Implement plan when required because of major accident or because of potential escalation to a major accident.

| L111 | HSG191 | HSG190 |
|--|--|--------|
| <p>300: Requires decision-making criteria to be in place.</p> <p>301: Requires specification of who can initiate alarms and plans.</p> | <p>69–73: Cover requirements for use of emergency plans when required, and during testing.</p> <p>196–199: Cover initiation of the emergency plans.</p> <p>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.</p> | |

Regulation 13

Allows for LA 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

Requires information to be given to the public as detailed in Schedule 6.

| L111 | HSG191 | HSG190 |
|---|--|--------|
| Schedule 6 includes informing the public of any warning alarms/information. Schedule 6(10) requires reference to the off-site emergency plan to be included. | 206–209: Cover provision of information to the public. 210: Covers warning of the public. | |

Regulation 16(3)

Pass information to other establishments in domino groups to allow them to assess effects on their on-site plans.

| L111 | HSG191 | HSG190 |
|---------------------------------------|--------|--------|
| 339: Information must be appropriate. | | |

Regulation 18(2)

Competent Authority may prohibit operation if reports and information required by Regulations not supplied.

| L111 | HSG191 | HSG190 |
|--|--------|--------|
| 360: Allows prohibition if information not supplied to LA to allow preparation of off-site plan. | | |

Schedule 4 Part 1(4)

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 |
|--|--------|---|
| 468: Reinforces requirements of regulations 9 and 10 to prepare internal emergency plans and to provide information to the LA to prepare off-site plans. | | 37: Sets out purpose of safety report that demonstration is made that MAPP/on-site plan and SMS are drawn up. |

Schedule 4 Part 2

Sets out information required to be included in safety report for TT sites.

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

Details objectives of on-site plan are laid down.

| L111 | HSG191 | HSG190 |
|---|--|--|
| <p>Schedule 5 Part 1 specifies objectives:</p> <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. | <p>19: Objectives listed as L111</p> <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. | <p>457–458: Require consideration of:</p> <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

Lay down information required to be included in on-site plan.

| L111 | HSG191 | HSG190 |
|--|--|---|
| 1: Persons authorised to set emergency procedures in motion, in charge of co-ordinating the on-site mitigatory action. | 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. | 460a: Requires information on the functions of the different roles in managing an emergency, including who has authority to initiate plan. 460f: Requires details for how site response personnel, the emergency services and the LA are alerted and mobilised. 465–466: Require full details of the mobilisable resources and demonstration of their adequacy. |
| | 81–82: The plan should identify nominated key personnel by name or job title. 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). On smaller sites the SIC and SMC roles can be assigned to the same person. | |
| | 83: The SIC is responsible for taking control at the scene of the incident. Round-the-clock cover to fill this role is essential. 84: Details the responsibilities of the SIC. | |
| | 85: The SMC has overall responsibility for directing operations from the on-site emergency control centre (ECC). 86: Details the responsibilities of the SMC. | |
| 2: Person with responsibility for liaison with the LA. | 94: Normally person responsible for preparing the on-site plan. | 460a: Requires this. |

Schedule 5 Part 2 (continued)

| 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 personal protective equipment (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 actions 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> |

Schedule 5 Part 2 (continued)

| 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> | |
| 5. Arrangements for providing initial and updated information and warning to the LA. | 97: Arrangements for alerting and providing the information they will require to respond. | |
| 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>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> | 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. |

Schedule 5 Part 2 (continued)

| 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> | |
| 7. Arrangements for providing assistance with off-site mitigatory action. | 99: Details of any specialist equipment or expertise and role of operator staff in briefing media. | |

Other documents

IP19:¹⁰ details of pre-planning requirements for firefighting.

Schedule 5 Part 3

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> | |

References and further reading

- 1 *A guide to the Control of Major Accident Hazards Regulations 1999 (COMAH) Guidance on Regulations* HSE document L111 (HSE Books 1999 ISBN 0 7176 1604 5).
- 2 *Emergency planning for major accidents: Control of Major Accident Hazards Regulations 1999 (COMAH)* HSG191 HSE Books 1999 ISBN 978 0 7176 1695 4
- 3 *Preparing safety reports: Control of Major Accident Hazards Regulations 1999 (COMAH)* HSG190 HSE Books 1999 ISBN 978 0 7176 1687 9
- 4 *Major accident prevention policies for lower-tier COMAH establishments* Chemical Information Sheet CHIS3 HSE 1999 Web only version available at www.hse.gov.uk/pubns/comahind.htm
- 5 *Emergency response and recovery* Central Office of Information 2005 (available from Emergency Planning College)
- 6 *Dealing with disasters together* (Second edition) Scottish Executive Office
- 7 *Health and Safety at Work etc Act 1974 (c.37)* The Stationery Office 1974 ISBN 978 0 10 543774 1
- 8 *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
- 9 RCS8
- 10 *Model Code of Practice Part 19: Fire precautions at petroleum refineries and bulk storage installations (Draft)* IP19 (Second edition) Energy Institute 2007 ISBN 978 0 85293 437 1 www.energyinst.org.uk

See also:

Control of Major Accident Hazards Regulations 1999 SI 1999/743 The Stationery Office 1999 ISBN 978 0 11 082192 4, as amended by the *Control of Major Accident Hazards (Amendment) Regulations 2005* SI 2005/1088 The Stationery Office 2005 ISBN 978 0 11 072766 0

This document is available web-only at:
www.hse.gov.uk/comah/buncefield/final.htm.

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. An overview of emergency planning requirements can be found in Appendix 6.

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.

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 firefighting plan should be functionally tested and exercised at least annually. 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 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 Appendix 6. 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. It is not possible to provide precise information on the magnitude of the explosion at this time as research is currently (July 2007) ongoing. 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.

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 28[#] and the Fire and Rescue Service’s *Manual on environmental protection*.[#]

22 If it is decided to extinguish the fire then IP19 *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 IP19. 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 the IP19 code of practice 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. (IP19 code 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. (IP19 code 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. (IP19 code 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? (IP Code 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 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 Further research is underway on the explosion mechanism at Buncefield, however, the results of this research are not expected in the near future. Therefore, to identify what scale of explosion the emergency arrangements need to be capable of surviving, the best available information from the Buncefield incident itself has been used. Accordingly, a blast over-pressure in excess of 500 millibar over a radius of 250 m has been assumed to be the magnitude and extent of the explosion to be used as the basis of the credible incident with respect to emergency arrangements.

37 The research may reveal that a blast over-pressure considerably in excess of 500 mB occurred at Buncefield. The table below 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. It is thought highly unlikely that the research will conclude that the blast over-pressure was less than 500 mB.

Table 1 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 |

| Damage details | Incident equivalent peak over-pressure in mBar |
|------------------------------------|--|
| Extensive damage to chemical plant | >480 |
| Failure of a pressurised sphere | >700 |

38 At Buncefield, the damage from the vapour cloud explosion (VCE) occurred out to approximately 250 m from the bund containing the tank that was overfilled. While the behaviour of vapour clouds can be directional, the movement of the cloud is heavily dependant 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 bund, 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 edge of any relevant bund (eg contains a gasoline storage tank) (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 Appendix 6. 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 foreseeable 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 2 is derived from the Energy Institute guidance in IP19 *Fire precautions at petroleum refineries and bulk storage installations*.[#] 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 2 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 Reinstatement resources |
| | | | 4.6 Training and instruction |

Source: IP19 Annex E – an example ERT member competency profile based on four units.

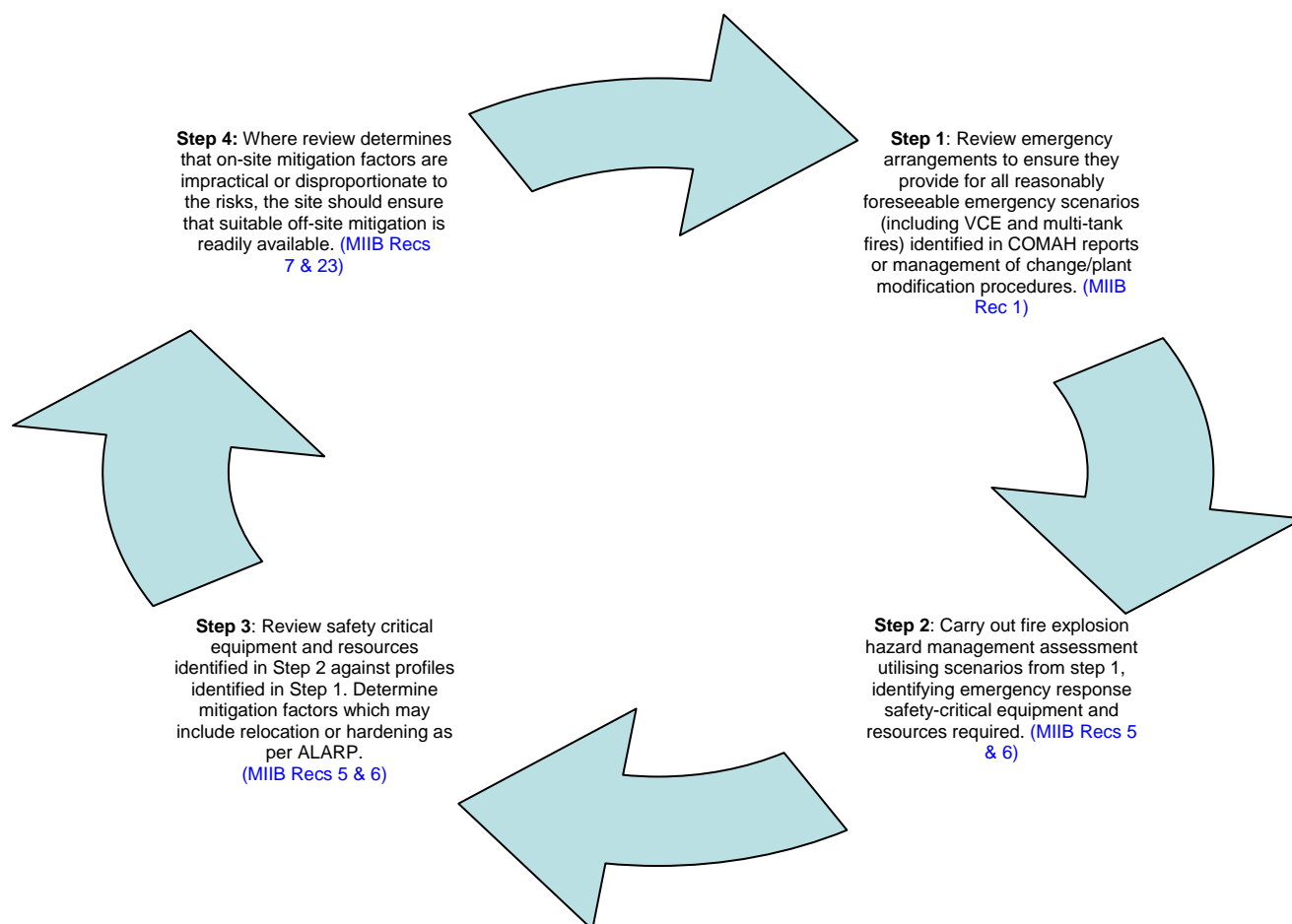
50 Dutyholders should evaluate the siting and protection of emergency response facilities, and put in place contingency arrangements either on or off site in the event of failure. This should include identifying and establishing an alternative emergency control with a duplicate set of plans and technical information.

51 IP19 *Fire precautions at petroleum refineries and bulk storage installations*[#] 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. 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 1 can be used to evaluate the vulnerability and siting of emergency response equipment and resources.

Figure 1 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 Appendix 6 provide a detailed list of emergency response equipment and resources, drawn from industry guidance, codes, reports of the Buncefield Standards Task Group (BSTG) and the MIIB. Relevant issues in *Buncefield: Hertfordshire Fire and Rescue Service's Review of the Fire Response*[#] 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 3:

Table 3

| 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 lost (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 lost (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 lost (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 Major Accident to the Environment (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 4 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 Table # | |
| | |
| 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. | |
| | |

| |
|--|
| <p>Safety of persons on site</p> <p>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</p> <p>Detail the site's means of collating a record of persons on site, identifying casualties and their locations.</p> |
| |
| <p>Safety of persons off site</p> <p>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> |
| |
| <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</p> <p>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</p> <p>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> |
| |

| | |
|---|--|
| 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 | |
| | |
| Detail how on-site emergency responders will be made readily identifiable to off-site responders | |
| | |
| Identify suitable locations and mandates for the all the control centres used to mitigate the incident | |
| Forward control point | |
| Site Emergency Control Centre (SECC) | |
| Silver Command | |
| Gold Command | |
| Health Advisory Team | |
| Identify key contact numbers for the establishment, eg SECC, alternative SECC, site main controller, operations control room, medical centre, operations control rooms | |
| | |
| 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 | |
| | |
| 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: <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. See Environment Agency web page www.environment-agency.gov.uk/ for further information see Pollution Prevention Guides, eg PPG18, PPG21 and PPG28. | |
| | |

Table 5 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 6 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 <i>New dimensions</i> 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 Table 2, 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 Table 2, 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 Table 2, 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 2, 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 2, 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 7 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 8 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 | | | | | |

| | Elements of plan | Exercise date | Audit date | Operator | Competent Authority | Comments Action required |
|----------|--|---------------|------------|----------|---------------------|-----------------------------|
| 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 | | | | | |
| 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 and 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 competent authority | | | | | |

| | Elements of plan | Exercise date | Audit date | Operator | Competent Authority | Comments Action required |
|----------|---|---------------|------------|----------|---------------------|-----------------------------|
| 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 | | | | | |
| 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 | | | | | |

| | Elements of plan | Exercise date | Audit date | Operator | Competent Authority | Comments Action required |
|----------|---|---------------|------------|----------|---------------------|-----------------------------|
| 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 9 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 **XXXXXX XXXXXX** 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 XXXXXX 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 **XXXXXX XXXXXX 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:

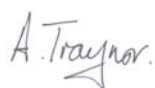
Organisation and resources:

- 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:



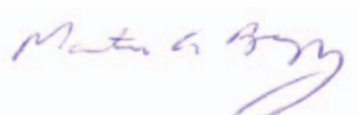
Tony Traynor
Chair
Process Safety Leadership Group



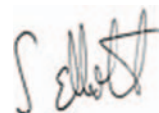
Peter Davis
UK Onshore Pipeline Operators' Association



Chris Hunt
Director General
UK Petroleum Industry Association



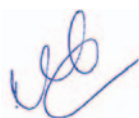
Martin Bigg
Head of Industry Regulation
Environment Agency



Steve Elliott
Chief Executive
Chemical Industries Association



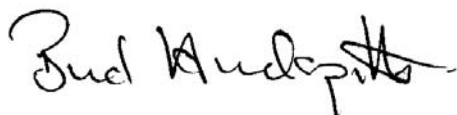
Allan Reid
Head of National Environmental Protection and Improvement
Scottish Environment Protection Agency



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 Major Incident Investigation Board 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 1 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 1 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 |

| BSTG paragraph reference | Status | PSLG report reference |
|---------------------------------|---------------|--|
| 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 |
| 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 |

| BSTG paragraph reference | Status | PSLG report reference |
|---------------------------------|---------------|--|
| 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 | Copied | Part 4 Engineering against loss of secondary and tertiary containment – Introduction |
| 159–160 | Copied | Recommendations 17, 18 – Bund Integrity (leak tightness) |
| 161–173 | Copied | Recommendations 17, 18 – Fire resistant bund joints |
| 174 | Deleted | Not required in final PSLG report |
| 175–181 | Copied | Recommendations 17, 18 – Fire resistant bund joints |
| 182 | Copied | Recommendations 17, 18 – Bund capacity |
| 183 | Copied | Recommendations 17, 18 – Firewater management and control measures |
| 184–200 | Copied | Recommendations 17 and 18 – Tertiary containment |
| 201 | Copied | 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 |
| 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 #–# |
| 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 |

| BSTG paragraph reference | Status | PSLG report reference |
|---------------------------------|---------------|--|
| 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 | Chemical Business Association |
| 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 |
| Colette Fitzpatrick | Health and Safety Executive |

Working Group 1 – Human factors

| | |
|-------------------------------|-----------------------------|
| Joanna Woolf (Chairperson) | Cogent |
| Stuart Robinson (Chairperson) | Health and Safety Executive |
| Mark Scanlon | Energy Institute |
| Peter Davis | BPA |
| 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 | Simon Storage |
| Allen Ormond | ABB Engineering Services |
| Craig Garbutt | Vopak |
| Kevin Shephard | Vopak |
| Glen Knight | ExxonMobil |
| Jon Evans | ExxonMobil |
| Mike Brown | ExxonMobil |
| Linda Dixon | Chevron |
| Paul Evans | Chevron |
| Fiona Brindley | Health and Safety Executive |
| Peter Mullins | Health and Safety Executive |
| Stuart Robinson | Consultant |
| Ron McLeod | Shell |
| John Gilbert | Kaneb |
| Bud Hudspith | UNITE the union |

Working Group 2 – Scope

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

Working Group 3 – Control and instrumentation

| | |
|----------------|----------|
| Chris Newstead | Simstor |
| Dave Ransome | Pidesign |
| Ian Neve | Total |

| | |
|---------------------------|------------------------------|
| Jeff Pearson | Health and Safety Executive |
| John Donald | Total |
| Joulian Douse | Petroplus |
| Malcolm Tennant | MHT Technology |
| Mark Broom | Environment Agency |
| Mark Scanlon | Energy Institute |
| Martyn Hewitson Griffiths | MHT Technology |
| Neil MacNaughton | INEOS |
| Neil Waller | INEOS |
| Peter Edwards | ConocoPhillips |
| Richard Gowland | EPSC |
| Richard Tinkler | ConocoPhillips |
| Rob Ayton | Petroplus |
| Robert Nicol | Shell |
| Stuart Williamson | Petroplus |
| Terry Lewis | Total |
| Colin Chambers | Health and Safety Laboratory |
| David Carter | Health and Safety Executive |
| Alan King | ABB |
| Paul Baker | ConocoPhillips |

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 |

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 | HSE (WG6 Chair) |
| 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

Working Group 7 – Coordination

| | |
|---------------------------|---|
| Jane Lassey (Chairperson) | 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 *Recommendations on the design and operation of fuel storage sites* Fifth report Buncefield Major Incident Investigation Board March 2007 www.buncefieldinvestigation.gov.uk
- 2 BS EN 61511:2004 *Functional safety. Safety instrumented systems for the process industry sector* British Standards Institution
- 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 API 620 *Design and construction of large, welded, low-pressure storage tanks* (Tenth edition) American Petroleum Institute 2002
- 6 API STD 650 *Welded tanks for oil storage* (Eleventh Edition) American Petroleum Institute 2008
- 7 *Reducing error and influencing behaviour* HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2
- 8 *The Buncefield Investigation: Third progress report* Third report Buncefield Major Incident Investigation Board 9 May 2006 www.buncefieldinvestigation.gov.uk
- 9 BS EN 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems* British Standards Institution
- 10 EEMUA 159 *User's Guide to the Inspection, Maintenance and Repair of Above ground Vertical Cylindrical Steel Storage Tanks* Publication 159 (Third edition) Volumes 1 and 2 Engineering Equipment Materials User's Association 2003 ISBN 978 0 85931 131 1
- 11 API RP 2350 *Overfill protection for storage tanks in petroleum facilities* (Third edition) American Petroleum Institute
- 12 BS 6755-2:1987 *Testing of valves. Specification for fire type-testing requirements* British Standards Institution
- 13 BS EN ISO 10497:2004 *Testing of valves. Fire type testing requirements* British Standards Institution
- 14 *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
- 15 *International Safety Guide for Oil Tankers and Terminals (ISGOTT)* (Fifth Edition) International Chamber of Shipping 2006 ISBN 978 1 85609 292 0
- 16 Model Code of Safe Practice Part 15: *Area classification code for installations handling flammable fluids* IP15 (Third edition) Energy Institute 2005 ISBN 978 0 85293 418 0 www.energyinstpubs.org.uk
- 17 *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

- 18 *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

- 19 *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

- 20 *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

- 21 *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

- 22 *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

- 23 *EEMUA 183 Guide for the Prevention of Bottom Leakage from Vertical, Cylindrical, Steel Storage Tanks* Publication 183 Engineering Equipment Materials User's Association 1999 ISBN 978 0 85931 115 1

- 24 *API STD 2000 Venting atmospheric and low-pressure storage tanks - Non-refrigerated and refrigerated* (Fifth edition) American Petroleum Institute 1999

- 25 *API STD 653 Tank inspection, repair, alteration, and reconstruction* (Fourth edition) American Petroleum Institute 2009

- 26 *Integrity of atmospheric storage tanks* SPC/Tech/Gen/35 HSE
www.hse.gov.uk/foi/internalops/hid/spc/spctg35.htm

- 27 *Chemical storage tank systems – good practice. Guidance on design, manufacture, installation, operation, inspection and maintenance* C598 CIRIA 2003 ISBN 978 0 86017 598 8

- 28 *Establishing the requirements for internal examination of high hazard process plant* RR729 HSE Books 2010 www.hse.gov.uk/research/rrhtm/index.htm

- 29 *Drainage of floating roof tanks* SPC/Enforcement/163 HSE 2009
www.hse.gov.uk/foi/internalops/hid/spc/spcenf163.htm

- 30 *BS 8007:1987 Code of practice for design of concrete structures for retaining aqueous liquids* British Standards Institution

- 31 *Construction of Bunds for Oil Storage Tanks* CIRIA Report R163 CIRIA 1997 ISBN 978 0 86017 468 4

- 32 *Design of Containment Systems for the Prevention of Water Pollution from Industrial Incidents* CIRIA Report R164 CIRIA 1997 ISBN 978 0 86017 476 9

- 33 *Masonry Bunds for Oil Storage Tanks* CIRIA/Environment Agencies Joint Guidelines

- 34 *BS 476-2-:1987, 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

- 35 *Model Code of Safe Practice Part 19: Fire precautions at petroleum refineries and bulk storage installations* IP19 Energy Institute 2007 ISBN 978 0 85293 437 1
www.energyinstpubs.org.uk

- 36 *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

- 37 *Managing fire water and major spillages* Pollution Prevention Guidelines PPG18 Environment Agency www.environment-agency.gov.uk

- 38 *The Buncefield Investigation: Second progress report* Second report Buncefield Major Incident Investigation Board 11 April 2006 www.buncefieldinvestigation.gov.uk

- 39 *Environmental guidelines for petroleum distribution installations* (Draft6) Energy Institute 2007 ISBN 978 0 85293 440 1 www.energyinst.org.uk

- 40 *Layer of Protection Analysis: Simplified Process Risk Assessment* Center for Chemical Process Safety 2001 ISBN 978 0 8169 0811 0

- 41 *Reducing risks, protecting people: HSE's decision-making process R2P2* HSE Books 2001 www.hse.gov.uk/risk/theory/r2p2.htm

- 42 *Buncefield explosion mechanism Phase 1: Volumes 1 and 2* RR718 HSE Books 2009 www.hse.gov.uk/research/rrhtm/index.htm

- 43 *The precautionary principle: Policy and application* Interdepartmental Liaison Group on Risk Assessment www.hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm

- 44 *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

- 45 *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

- 46 *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

- 47 *Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal* IPPC H1 Version 6 July 2003

- 48 *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

- 49 Department of the Environment, Transport and the Regions (DETR) *A guide to risk assessment and risk management for environmental protection* The Stationery Office 1999

- 50 *Guidelines for Consequence Analysis of Chemical Releases* Center for Chemical Process Safety 1999 ISBN 978 0 8169 0786 1

- 51 *The implications of dispersion in low wind speed conditions for quantified risk assessment* CRR133 HSE Books 1997 ISBN 978 0 7176 1359 5

- 52 *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control* (Third Edition) Elsevier 2005 ISBN 978 0 7506 7555 0

- 53 *Ignition probability review, model development and look-up correlations* EI Research Report January 2006 ISBN 978 0 85293 454 8

- 54 *A risk-based approach to hazardous area classification* Institute of Petroleum 1998 ISBN 0 85293 238 3
- 55 *Decompression risk factors in compressed air tunnelling: Options for health risk reduction* CRR201 HSE Books 1998 ISBN 978 0 7176 1650 3
- 56 *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
- 57 *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* NUREG/CR-1278
- 58 *EEMUA 191 Alarm Systems – A Guide to Design, Management and Procurement* Publication 191 (Second edition) Engineering Equipment Materials User's Association 2007 ISBN 978 0 85931 155 7
- 59 *Principles for proof testing of safety instrumented systems in the chemical industry* CRR428 HSE Books 2002 ISBN 978 0 7176 2346 4
- 60 *The Report of the BP U.S. Refineries Independent Safety Review Panel* January 2007 (The Baker Panel Report)
- 61 Weick KE and Sutcliffe KM *Managing the Unexpected: Assuring High Performance in an Age of Complexity* Jossey-Bassey 2001 ISBN 978 0 7879 5627 1
- 62 *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
- 63 *Safety Culture* HSE Human Factors Briefing Note No 7 www.hse.gov.uk/humanfactors/comah/07culture.pdf
- 64 *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
- 65 *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
- 66 *Involving employees in health and safety: Forming partnerships in the chemical industry* HSG217 HSE Books 2001 ISBN 978 0 7176 2053 1
- 67 *Guidelines for Risk Based Process Safety* Center for Chemical Process Safety 2007 ISBN 978 0 470 16569 0
- 68 *Process safety management systems* SPC/TECH/OSD/13 OSD Internal Document HSE www.hse.gov.uk/foi/internalops/hid/spc/spctosd13.pdf
- 69 *Safety Report Assessment Guide: Highly flammable liquids – Criteria* HSE www.hse.gov.uk/comah/sraghfl/index.htm
- 70 *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
- 71 *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

72 *Competence assessment for the hazardous industries* RR086 HSE Books 2003 ISBN 0 7176 2167 5 www.hse.gov.uk/research/rrhtm/index.htm

73 Hopkins A *Lessons from Longford: The Esso Gas Plant Explosion* CCH Australia Ltd 2000 ISBN 978 1 86468 422 3

74 *Training and Competence* EI Human Factors Briefing Note No 7 Energy Institute 2003 www.energyinst.org.uk/content/files/bn7.pdf

Recommendations on the emergency preparedness for, response to and recovery from incidents Sixth report Buncefield Major Incident Investigation Board 17 July 2006 www.buncefieldinvestigation.gov.uk

Controlled Burn PPG28 Environment Agency 2007 www.environment-agency.gov.uk

Fire and Rescue Manual: Volume 2 Fire Service Operations: Environmental Protection Communities and Local Government 2008 ISBN 978 0 11 341316 4

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

Emergency planning for major accidents: Control of Major Accident Hazards Regulations 1999 (COMAH) HSG191 HSE Books 1999 ISBN 978 0 7176 1695 4

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

Successful health and safety management HSG65 (Second edition) HSE Books 1997 ISBN 978 0 7176 1276 5

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 User's Association 2009 ISBN 978 0 85931 167 0

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

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

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

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 www.energyinst.org.uk/

- # *Managing shift work: Health and safety guidance* HSG256 HSE Books 2006 ISBN 978 0 7176 6197 8
- # Horne JA and Reyner LA 'Vehicle accidents related to sleep: A review' *Occupational and Environmental Medicine* 1999 56 (5) 289–294
- # *Managing Fatigue Risks* HSE Human Factors Toolkit: Specific Topic 2
www.hse.gov.uk/humanfactors/comah/specific2.pdf (unavailable)
- # *Managing fatigue in the workplace: A guide for oil and gas industry supervisors and occupational health practitioners* OGP Report Number 392 OGP/IPIECA 2007
www.ogp.org.uk/pubs/392.pdf
- # *The development of a fatigue/risk index for shiftworkers* RR446 HSE Books 2006
www.hse.gov.uk/research/rrhtm/index.htm
- # *Improving alertness through effective fatigue management* Energy Institute, London September 2006 ISBN 978 0 85293 460 9 www.energyinst.org.uk/
- # *Human factors: Safety critical communications* HSE
www.hse.gov.uk/humanfactors/comah/safetycritical.htm
- # *Organisational change and major accident hazards* Chemical Information Sheet CHIS7 HSE Books 2003 www.hse.gov.uk/pubns/comahind.htm
- # *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)
- # *Contractorisation* Technical Assessment Guide T/AST/052 HSE 2002
www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast052.pdf
- # *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/>
- # *Management of Change* UKPIA Ltd Self Assessment Module 1 and Appendix 1
www.ukpia.com
- # *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* Fourth report Buncefield Major Incident Investigation Board 13 July 2006
www.buncefieldinvestigation.gov.uk
- # *Revitalising procedures* HSE www.hse.gov.uk/humanfactors/comah/procinfo.pdf
- # BS EN ISO 11064: Parts 1-7 *Ergonomic design of control centres* British Standards Institution
- # *Alarm handling* Human Factors Briefing Note No 2 Energy Institute 2003
www.energyinst.org.uk

- # *Alarm handling* HSE Human Factors Briefing Note No 9 HSE
www.hse.gov.uk/humanfactors/comah/09alarms.pdf
- # *Better alarm handling in the chemical and allied industries* Chemical Information Sheet CHIS6 HSE Books 2000 www.hse.gov.uk/pubns/comahind.htm
- # *Guidance on safety performance indicators* OECD
<http://www2.oecd.org/safetyindicators>
- # *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
www.energyinst.org.uk/content/files/guidancemay08.pdf
- # Maremonti M, Russo G, Slazano E and Tufano V 'Post-accident analysis of vapour cloud explosions in fuel storage areas' *Trans. IChemE* 1999 **77** 360–365
- # Yuill J 'A discussion on losses in process industries and lessons learned' in 51st Canadian Chemical Engineering Conference (see <http://psm.chemeng.ca>), Halifax, Nova Scotia, Canada 2001
- # Chang J and Cheng-Chung L 'A study of storage tank incident' *J. Loss Prevention* 2006 **19** 51–59
- # Bai CX, Rusche H and Gosman AD 'Modelling of gasoline spray impingement, Atomisation and sprays' 2002 **12** 1–27

Further information

HSE priced and free publications are available by mail order from HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 Fax: 01787 313995 Website: www.hsebooks.co.uk (HSE priced publications are also available from bookshops and free leaflets can be downloaded from HSE's website: www.hse.gov.uk.)

British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop 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.