COMAH Control of Major Accident Hazards

COMAH Competent Authority

"ALL MEASURES NECESSARY" – Environmental Aspects

(Guidance for Competent Authority Inspectors and officers)

CONTENTS

List of Figures

List of Tables

1 PURPOSE, SCOPE AND GENERAL PRINCIPLES

This document summarises the Competent Authority's (CA)[1] position on "all measures necessary" relating to prevention and mitigation of environmental aspects of major accidents. The guidance sets out how officers/inspectors from the environmental regulators (Environment Agency, Natural Resources Wales and Scottish Environment Protection Agency) should address Regulation 5(1) (all measures necessary [AMN]) decisions for COMAH establishments. The document also provides guidance on some aspects of environmental risk assessment, as applied to AMN decisions.

This document has been developed alongside discussions with industry representatives via the Chemical and Downstream Oil Industry Forum (CDOIF) resulting in the CDOIF Guidelines "Environmental Risk Tolerability for COMAH Establishments"[2].

It should be understood that the CDOIF Guideline "does not explore all possible options for determining environmental tolerability or environmental risk assessment….". Therefore whilst the CDOIF Guidelines are referred to in this document, the requirements of the Regulations may be met by other approaches which may or may not be referenced in this guidance.

This guidance covers:

- general principles;
- As Low As Reasonably Practicable (ALARP) demonstration;
- COMAH good practice;
- proportionality;
    - approach to risk assessment;
    - cost-benefit analysis and gross-disproportion.

This document presumes that the reader has a basic understanding of the requirements of COMAH and the concepts used by the CA to implement it in the UK.

1.1 COMAH 2015[3] Regulation 5(1)

Regulation 5(1) of the COMAH Regulations 2015 states that:

> "Every operator must take all measures necessary to prevent major accidents and to limit their consequences for human health and the environment."

The Health and Safety Executive (HSE) and the appropriate agency[4] work in partnership to meet the Competent Authority (CA) duties under COMAH at each establishment. The HSE will normally lead

[1] As defined in Regulation 4 to COMAH 2015, the competent authority for an establishment is HSE, or the Office for Nuclear Regulation (ONR) for nuclear establishments, together with the appropriate agency. In England the competent authority is HSE or ONR and the Environment Agency (EA); in Scotland it is HSE or ONR and the Scottish Environment Protection Agency (SEPA); and in Wales it is HSE or ONR and Natural Resources Body for Wales (NRW).

[2] CDOIF Guidelines "Environmental Risk Tolerability for COMAH Establishments" (v2, finalised 16 March 2016) http://www.hse.gov.uk/aboutus/meetings/committees/cif/resources.htm

[3] COMAH Regulations 2015 http://www.legislation.gov.uk/uksi/2015/483/pdfs/uksi_20150483_en.pdf

[4] As defined in Regulation 2(1) to COMAH 2015, the appropriate agency is the Environment Agency in England, Natural Resources Wales in Wales, and the Scottish Environment Protection Agency in Scotland.

in dealing with issues concerning the health and safety of people and the appropriate agency on issues concerning environmental protection. As many aspects of prevention, control and mitigation are common to both people and to the environment, close co-ordination and communication between both parts of the CA is essential whilst assessing if all measures necessary have been taken.

It is important to note that Regulation 5(1) only applies to the prevention and mitigation of COMAH major accidents.

Where it has been demonstrated that there is no potential for a Major Accident to the Environment (MATTE) but the site is a cause for concern for other environmental reasons, then other powers subject to the relevant test may be available under other legislation such as the Environmental Permitting Regulations (EPR) in England and Wales, and Pollution Prevention and Control (PPC) or Controlled Activities Regulations (CAR) in Scotland.

In practice, both for safety and the environment, the measures required should be proportionate to the risk. It is important to remember that the assessment is for the risk to a receptor from the whole establishment, not just from a single event or scenario.

The HSE has published a considerable amount of guidance on COMAH and its regulatory decision-making process under the Health and Safety at Work Act (HSWA). The CA believes it is appropriate for the same general principles and guidance to apply to risks to the environment, as they do to persons.

CA guidance relevant to ALARP decisions and environmental risk assessment, to which appropriate agency inspectors should refer, include:

- "ALARP – As low as reasonably practicable"[5];
- "Guidance on ALARP decisions in COMAH" (Health and Safety Executive SPC/perm/37)[6];
- "HID's approach to ALARP decisions" (Health and Safety Executive SPC/perm/39)[7];
- "Environmental Aspects of Safety Report Assessment" (SRAM Appendix 13)[8];
- "Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports"[9] ;
- "A Guide to the COMAH Regulations 2015", L111[10] HSE 2015.

Further guidance on risk management can be found in international standards such as the 31000 risk management series and the 61508 / 61511 functional safety series including:

- BS EN 31010:2010, Risk management : Risk Assessment Techniques;

[5] "ALARP – As low as reasonably practicable" http://www.hse.gov.uk/comah/alarp.htm

[6] "Guidance on ALARP decisions in COMAH" (SPC 37)
http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37

[7] "HID's approach to ALARP decisions" (SPC 39)
http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_39.htm

[8] "Environmental aspects of Safety Report Assessment" (SRAM Appendix 13), COMAH 2015 revised version

[9] "Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports", (COMAH CA, Dec 1999) http://www.sepa.org.uk/regulations/control-of-major-accident-hazards-comah/

[10] L111"A Guide to the COMAH Regulations 2015" http://www.hse.gov.uk/pubns/priced/l111.pdf

- BS EN 61511 series, Functional safety — Safety instrumented systems for the process industry sector (eg Part 3: Guidance for the determination of the required safety integrity levels).

This "All Measures Necessary – Environmental Aspects" guidance provides additional information on environmental risk to supplement the wider CA guidance and standards on ALARP and risk management listed above. Other useful references are referenced in the text of the document or noted in Appendix 4.

1.2 A note on MATTE definition

Within the UK, an important concept for the application of COMAH to the environment is that of a MATTE or Major Accident to the Environment. This is not defined in the Regulations or the Directive, but is a term used in the UK by the CAs and industry to indicate when a major accident has caused serious harm to the environment (or when it has potential to do so):

- a Major Accident which ***could*** **cause serious harm** to the environment (ie lead to serious danger) **is a *potential* MATTE** (ie a Major Accident with MATTE potential);
- a Major Accident which ***has*** **caused serious harm** to the environment ***is*** **a MATTE**.

So, what is serious harm / danger?

The environment is complex with a diverse range of receptors and precise definitions are not practicable. However, guidance on thresholds for MATTE (ie the level of harm that would be considered serious) was published in DETR 1999 "Guidance on the Interpretation of Major Accident to the Environment for the purposes of the COMAH regulations"[11].

Please note:

- The thresholds for MATTE in the DETR guidance are described both in terms of types of incident that might be considered to be a MATTE (see Chapter 4.1 including examples a-k), and tabulated criteria and thresholds for extent, severity and duration of harm to receptors (see Chapter 4.2 and tables 1-12). All receptors (all DETR tables) and the examples require consideration when determining whether an incident or potential accident scenario is a MATTE or potential MATTE. As stated by DETR, all recovery periods are for expected natural recovery, not aided recovery.
- The DETR guidance has been recognised as requiring to be updated, mainly due to the introduction of new legislation such as the Water Framework Directive (WFD) and the Environmental Liability Directive (ELD). WFD introduces a new system of water body classification, whilst ELD and supporting guidance provides definition of the term "environmental damage". The CDOIF MATTE definition work[2] incorporates these changes (for example, damage to land), reflecting the legislation in place in 2015 and should be referred to when determining potential consequences. Operators are advised to consider current relevant legislation (including WFD and ELD) when determining whether an incident or potential incident is a MATTE or potential MATTE.

If issues arise over interpretation of MATTE thresholds, please discuss with appropriate agency Head Office COMAH contacts.

[11] DETR 1999 "Guidance on the Interpretation of Major Accident to the Environment for the purposes of the COMAH regulations" http://www.sepa.org.uk/regulations/control-of-major-accident-hazards-comah/

1.3 COMAH Good Practice

The concept of Good Practice is key to COMAH as in some cases, for example, in the "Broadly Acceptable" region, good practice may be the only measures implemented, and the CA would not normally require further measures unless the law requires it (see section 2.1). It is therefore important to understand what good practice is and how it should be applied.

"A Guide to the COMAH Regulations 2015" (L111[12]) defines Good Practice as follows:

> 84 Relevant good practice should be adopted as a minimum and you should then firstly consider: 'What more can I do to reduce the risks?' And, secondly, explain: 'Why have I not done it?' Good practice represents a consensus between regulators, technical experts, dutyholders and other stakeholders on what constitutes proportionate action to control a given hazard. Among other things it takes account of what is technically feasible and the balance between the costs and benefits of the measures taken. See the HSE website for guidance on ALARP and good practice.
>
> 85 Sources of good practice include Approved Codes of Practice and standards produced by organisations such as the British Standards Institution (BSI), Comité Européen de Normalisation (CEN), Comité Européen de Normalisation Electrotechnique (CENELEC), International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Engineering Equipment and Materials Users Association (EEMUA), the American Society of Mechanical Engineers (ASME), the American Petroleum Institute (API) and HSE.

It should be noted that good practice and best practice have different meanings. The current definition of what the CA regards as 'good' and 'best' practice can be found in the HSE guidance 'Assessing compliance with the law in individual cases and the use of good practice' (known as ALARP 2[13]), . It indicates that a variety of sources of information (whether called guidance, technical notes, etc.) can be regarded as potentially good practice. It is therefore the context of its application within the R2P2 framework ("Reducing Risks Protecting People" – see section 2.1) that becomes relevant, rather than the nature of the information.

In addition to the sources of good practice referenced above the CA regards the following as examples of environmental "Good Practice" that might be relevant in specific circumstances (ie they are good practice for the purposes of any HSE/CA guidance on All Measures Necessary):

- EPR / PPC Guidance (NB: this does not apply to guidance under IPC, as this does not have any specific requirement for accident prevention);
- Pollution Prevention Guidelines (PPGs);
- other generic guidance such as CIRIA C736[14], CIRIA C598[15];
- guidance from trade associations or Institutes (eg CIA winterisation guidance or Energy Institute model codes and guidelines);

---

[12] L111"A Guide to the COMAH Regulations 2015" http://www.hse.gov.uk/pubns/priced/l111.pdf

[13] "Assessing compliance with the law in individual cases and the use of good practice" www.hse.gov.uk/risk/theory/alarp2.htm

[14] CIRIA C736: Containment systems for the prevention of pollution: Secondary, tertiary and other measures for industrial and commercial premises, https://www.ciria.org/Resources/Free_publications/c736.aspx

[15] CIRIA C598: Chemical storage tank systems - good practice. Guidance on design, manufacture, installation, operation, inspection and maintenance

- sector specific regulator / industry guidance (eg the CA containment policy and PSLG[16] final report[17] - Safety and Environmental Standards for Fuel Storage Sites and CDOIF publications).

The CA regard good practice as being subject to the process of continuous improvement and will encourage industry to keep good practice up-to-date as technology advances and societal concern about Major Accident Hazards (MAHs) changes. Where certain Operators are achieving a higher standard ('best practice'), it is reasonable to challenge other Operators engaged in similar activities whether such a standard is now, in effect, good practice[18]. However, it is not true that the best risk controls available are necessarily reasonably practicable or automatically become good practice[19].

For sectors or scenarios where there is no direct "Good Practice" then L111 states that:

> 87 There will be some cases where good practice has not been established. Here, the first step should be to examine the good practice that applies in comparable circumstances, for example that used for a similar process, to determine if it is transferable or can be modified to achieve at least the same level of protection.

This is referred to as "Relevant Good Practice". For example if a sector does not have specific guidance on the design of secondary containment systems, then CIRIA c736 or PSLG final report may be considered "relevant good practice".

In cases where upgrade to current good practice has been demonstrated as not reasonably practicable, there is an expectation that other reasonably practicable risk reduction measures will be assessed and implemented to ensure risk is reduced ALARP[20]. L111 gives guidance on how an Operator might approach this:

> 88 In cases where no suitable standard for good practice exists, you may have to employ a risk management approach to prevention and mitigation based on first principles. The competent authority will require this to be thoroughly justified.

1.3.1 Application of Good Practice

As discussed in R2P2 the CA starts "with the expectation that controls should, as a minimum, implement authoritative good practice precautions (or achieve similar standards of prevention/protection), irrespective of specific risk estimates". However guidance on ALARP (see HSE ALARP suite of guidance[21] and SPCs 37 & 39[6,7]) highlights that it might not be reasonably practicable to implement good practice in given circumstances.

[16] Process Safety Leadership Group

[17] PSLG Final Report on Buncefield http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf

[18] "Policy and guidance on reducing risks as low as reasonably practicable in design" http://www.hse.gov.uk/risk/theory/alarp3.htm

[19] ALARP "at a glance" http://www.hse.gov.uk/risk/theory/alarpglance.htm

[20] ALARP 2 paragraph 3.10

[21] ALARP suite of guidance http://www.hse.gov.uk/risk/expert.htm

Moreover, in some situations (eg higher risk, where residual risk is intolerable or Tolerable if ALARP) the CA would expect further measures to be implemented in addition to good practice to ensure risk is reduced ALARP.

In all cases, where good practice is enshrined in legal requirements, it must be implemented to the extent which will satisfy the law (for example, the management system and emergency plan requirements of COMAH, or the requirements of the oil storage regulations).

1.3.1.1 New Sites

The CA's expectation is that any new sites will be built to include any Good Practice that is appropriate to the risks identified for the site. This is not subject to Cost Benefit Analysis (CBA) but if a specific aspect of Good Practice is not applied a demonstration must be made as to why - for example, the risk does not exist (there is either no source, pathway or receptor) or the proposed installation is new or novel and no suitable standard for good practice exists.

1.3.1.2 Existing Sites

In principle, the use of current good practice applies to both new establishments and existing establishments. However it would clearly not be proportionate behaviour to require upgrading without any consideration of the financial costs and environmental benefits, or consideration of what is a reasonable upgrade time-scale.

The expectation from the CA is clearly stated in the HSE's ALARP 2 guidance:

> 3.4 In judging compliance, HSE expects duty-holders to apply relevant good practice as a minimum. For new plant/installations/situations, this will mean the application of current good practice. For existing plant/installations/situations, this will mean the application of current good practice to the extent necessary to satisfy the relevant law.
>
> 3.5 Where the law requires risks to have been reduced ALARP, HSE:
>
> 1. may accept the application of relevant good practice in an appropriate manner as a sufficient demonstration of part or whole of a risk/sacrifice computation;
> 2. does not normally accept a lower standard of protection than would be provided by the application of current good practice; and
> 3. will, where the duty-holder wishes to adopt a different approach to controlling risks, seek assurance that the risks are no greater than that which would have been achieved through adoption of good practice and so are ALARP for that different approach.

However ALARP 2 also recognises that when assessing compliance against good practice at existing facilities, a proportionate approach should be adopted, ensuring that the duty holder has adopted good practice measures so far as is reasonably practicable.

> 3.10 When reviewing health or safety measures on an existing plant, installation or situation (such as when considering retrofitting, safety reviews or upgrades), duty-holders should compare existing measures against current good practice. The good practice measures set out should be adopted so far as is reasonably practicable. It might not be reasonably practicable to apply retrospectively to existing plant, for example, all the good practice expected for new plant. However, there may still be ways to reduce the risk eg by partial solutions, alternative measures etc.

For existing establishments that do not comply fully with current good practice the CA would expect, as a minimum, the Operator to have carried out a gap analysis between the existing arrangements and current good practice. Subsequently, the Operator should make either a firm commitment to move to current good practice on a reasonable timescale or an appropriate justification, which could well include a CBA, for retaining the existing arrangements, combined with an assessment of what other reasonably practicable measures will be adopted to reduce risk ALARP. The timescale of any upgrade should be proportionate to the circumstances.

In summary, the need to upgrade existing facilities to relevant good practice is not strictly subject to cost-benefit analysis in the ALARP sense, but clearly such upgrading (whether the measures themselves or the time-scales) must be proportionate in the circumstances. If there is deviation from current good practice then the Operator could upgrade to current good practice or should implement equivalent risk reduction by other means where reasonably practicable.

1.3.1.3 Significantly modified sites

For existing establishments that implement modifications that could have "significant repercussions with respect to the prevention of major accidents or the limitation of consequences of major accidents to persons and the environment"[22] the aim should be to incorporate good practice into the modification. Such modifications provide an opportunity to address many issues that would not otherwise be possible, and can make the implementation of good practice easier, and often at lower cost than it would otherwise be. However, whilst many additional measures can be addressed as part of a major upgrade, it may not be reasonably practicable to meet all good practice at existing establishments, even when significant modifications are being carried out (eg it might not be practicable to meet modern layout criteria on an existing plant).

Thus prior to implementation of significant changes, the CA expects an Operator to identify the extent to which current good practice will be incorporated within the establishment. If it is not considered reasonably practicable to implement aspects of current good practice, the Operator should make an appropriate justification, which could well include a CBA, for adopting the proposed arrangements, combined with an assessment of what other reasonably practicable measures will be adopted to reduce risk ALARP. The CA will not usually accept a lower standard of protection than would be provided by the application of current good practice (ie the combined proposed measures should reduce risk to a level that would have been delivered using good practice). The CA will be flexible in agreement of upgrade timescales and will usually accept the most cost effective implementation of risk reduction measures.

2 DEMONSTRATION REQUIREMENTS

The Seveso III Directive and COMAH 2015 provide formal definitions of the terms hazard and risk:

> 'hazard' means the intrinsic property of a dangerous substance or physical situation, with a potential for creating damage to human health or the environment;

[22] Revised guidance for operators of top tier COMAH establishments: review and revision of COMAH safety reports (COMAH R01) – COMAH Competent Authority Dec 2009 http://www.hse.gov.uk/comah/report-review.pdf

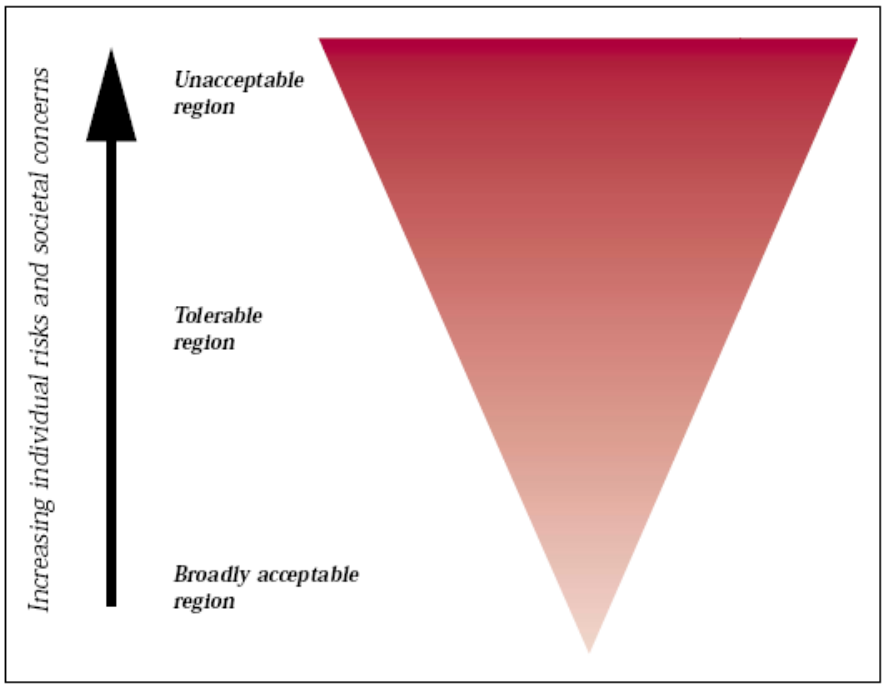
'risk' means the likelihood of a specific effect occurring within a specified period or in specified circumstances.

Risk is thus a combination of **CONSEQUENCE** and the **LIKELIHOOD** (or probability of occurrence) of that consequence. Consequence can be further defined in terms of the **EXTENT** of harm and the **SEVERITY** of harm, and the COMAH Regulations use all these terms (eg Reg 5, Reg 24, Schedule 2 paragraph 2(b) and Schedule 3 paragraph 5). As highlighted by DETR (1999) and CDOIF, a further parameter that influences scale of Consequence is **DURATION** of harm – that is the timescale it would take for natural recovery after the harm has occurred.

2.1 The Tolerability of Risk Diagram

HSE's Tolerability of Risk Diagram, as explained in the document "Reducing Risks Protecting People" (known as R2P2[23]), is used by the CA to define the degree of demonstration required by the Operator.

Figure 2-1 – Tolerability of Risk Diagram



The triangle represents increasing level of "risk" for a particular hazardous activity from the bottom of the triangle to the top (measured by the risk to an environmental receptor, individual risk and societal concerns it engenders).

The dark zone at the top represents an "**UNACCEPTABLE**" or "**INTOLERABLE**" region. For practical purposes, a particular risk falling into that region is regarded as unacceptable whatever the level of benefits associated with the activity. Any activity or practice giving risks falling in that region would, as a matter of principle, be ruled out unless the activity or practice can be modified to reduce the degree of risk so that it falls in one of the lower regions, or there are exceptional reasons for the activity or practice to be retained.

[23] "Reducing Risks Protecting People" http://www.hse.gov.uk/risk/theory/r2p2.htm

The light zone at the bottom, on the other hand, represents a "**BROADLY ACCEPTABLE**" region. For COMAH purposes, risks falling into this region are generally regarded as adequately controlled, however Operators are reminded of the need to comply with all environmental legislation irrespective of site specific risk. When residual risk is deemed Broadly Acceptable, the CA would not usually require further action to reduce risks, beyond adherence to current codes, standards and established good practice so far as is reasonably practicable (see section 0).

For risks shown to be Broadly Acceptable, Operators must reduce risks wherever it is reasonably practicable to do so or where the law so requires it. It is considered that effective design features that are of low cost should always be incorporated to reduce risks, whatever their estimated frequencies.

The zone between the unacceptable and broadly acceptable regions is the "**TOLERABLE IF ALARP"** or "**TifALARP**" region. Risks in this region can be tolerated in order to secure benefits, in the expectation that:

- the nature and levels of the risks are properly assessed and the results used to determine control measures, with the assessment of the risks based on the best available scientific evidence and, where evidence is lacking, on the best available scientific advice;
- the residual risks (ie risk after all protection measures are implemented) are not unduly high and kept as low as reasonably practicable (the ALARP principle); and
- the risks are reviewed periodically to ensure that they still meet the ALARP criteria, for example, by ascertaining whether further or new control measures need to be introduced to take account of changes over time, such as new knowledge about the risk or the availability of new techniques for reducing or eliminating risks.

Within the TifALARP zone there is an expectation that Operators will adhere to codes, standards and established good practice so far as is reasonably practicable, including potentially upgrading if good practice changes. In addition, the Operator will adopt other reasonably practicable risk reduction measures.

It may not be reasonably practicable to retrospectively apply a measure to an existing plant that would be required to reduce risks to ALARP for a new plant (even if that measure has become, in effect, good practice for every new plant). Whether the measure can be applied, or not, will depend on the site-specific circumstances, the risk levels (in terms of site risk compared to tolerability of risk thresholds), and whether the costs of the measure are grossly disproportionate (see section 7.2.3). In cases where upgrade to current good practice has been demonstrated as not reasonably practicable, there is an expectation that other reasonably practicable risk reduction measures will be assessed and implemented to ensure risk is reduced to ALARP, as stated in paragraph 3.10 of the HSE ALARP 2 guidance (see section 1.3.1.2).

2.2 Using the Tolerability of Risk Diagram

COMAH is about ensuring that all measures necessary have been taken to prevent major accidents and to limit their consequences. In environmental terms this requires taking measures that prevent and mitigate against serious harm to environmental receptors [the level of potential harm is informed by source, pathway, and receptor analysis].

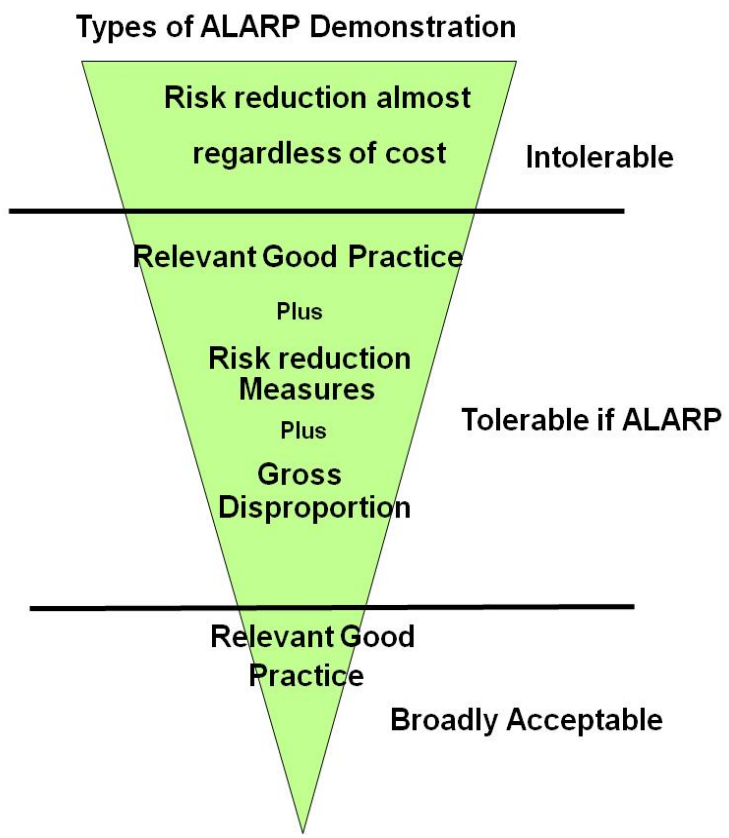
In the same way as the HSE assesses cumulative risk to an individual, the appropriate agencies consider that the cumulative risk to a receptor should be assessed. Typically, in order to do this, each potential MATTE event is assessed and then the likelihood of independent events summed to give the overall likelihood of a MATTE for a receptor from the establishment as a whole.

$$\text{Likelihood}_{\text{receptor}} = \text{Likelihood}_{\text{event1}} + \text{Likelihood}_{\text{event2}} + \ldots\ldots\ldots\ldots\ldots$$

The acceptable frequency of an impact on a receptor will vary depending on the consequence (extent, severity and duration) of impact of the event. The higher the consequences, the lower the acceptable frequency will be (see sections 4.2 and 4.4).

As discussed, the risk from an establishment can be placed within one of the three bands on the "Tolerability of Risk" diagram (see Figure 2-2 below).

Figure 2-2 – Tolerability of Risk Diagram showing expected Risk Reduction Measures



Intolerable Region:

If the risk is in this region then ALARP cannot be demonstrated and action must be taken to reduce the risk almost irrespective of cost.

Tolerable if ALARP Region:

If the risk falls within this region then a case specific ALARP demonstration is required. Relevant Good Practice is expected to be applied (in line with section 1.3.1). Further risk reduction measures must be taken so far as is reasonably practicable (ie upgrade required unless the steps are not practicable at the site or their cost would be grossly disproportionate to the benefits). The extent of this demonstration should be proportionate to the level of risk (see section 7.2).

Broadly Acceptable Risk Region:

If the risk falls within this region, then the all measures necessary demonstration may be based on the application of good practice or equivalent risk reduction measures (see sections 1.3.1 and 2.1).

Details of the consequence and frequencies that would fall into each of the categories above are given in Table 4-3 in section 4.

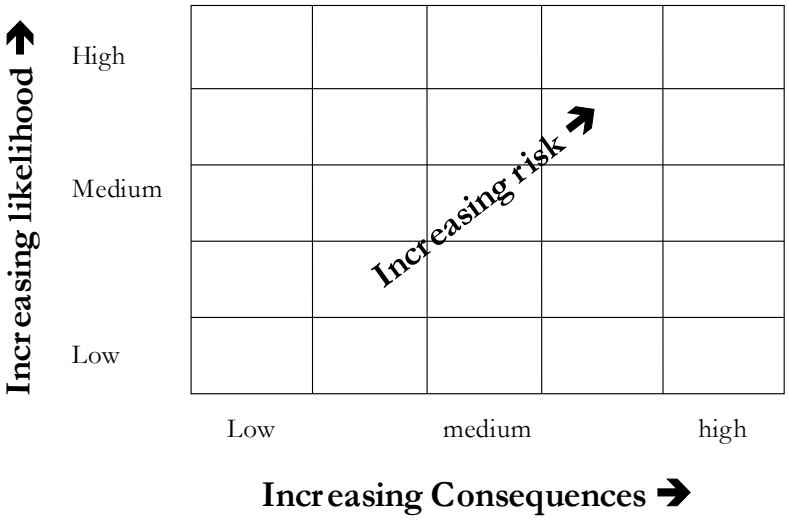
The following sections look at how the risk to a receptor may be assessed and then the tolerability of risk diagram applied.

3 WHAT IS RISK?

As previously discussed risk is a function of both the potential **CONSEQUENCE** (including extent, severity and duration) of an event and the **LIKELIHOOD** of that event happening.

This is normally presented on a risk matrix, for example:

Figure 3-1 – Simplified Risk Matrix



3.1 Risk Assessment and Proportionality

It is the CA's position[6,9,10,24] that the depth of any risk assessment should be proportionate to:

(a) the scale and the nature of the major accident hazards (MAHs) presented by the establishment and the installations and activities on it; and

(b) the risks posed to neighbouring populations and the environment.

That is, the assessment has to be site specific.

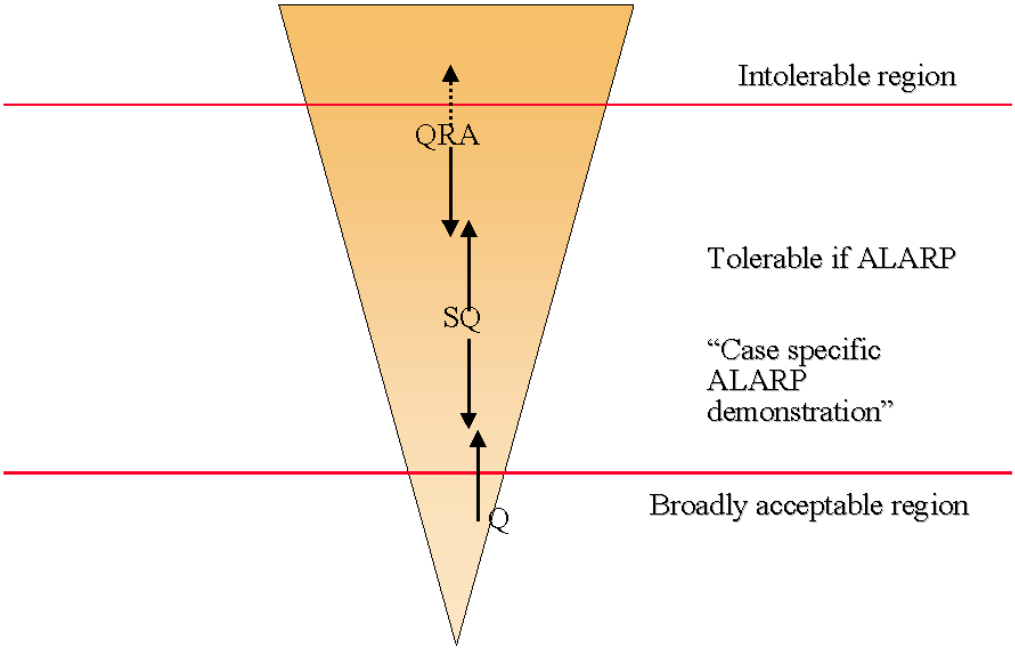
The risks referred to include both individual and societal risks, as well as environmental risks.

The depth of analysis that needs to be present depends on the level of risk predicted before the additional measures are applied. The nearer the risk is to the intolerable boundary the greater the depth of analysis required and the greater will be the depth of demonstration required (eg greater effort needed to determine potential risk reduction measures) to show that those risks are ALARP. There are various kinds of risk assessment that may be used depending on proportionality. These range from qualitative (Q) at the lowest level through semi-quantitative (SQ) up to Quantitative Risk Assessment (QRA) at the highest level.

This is illustrated in Figure 3-2 below.

[24] Preparing safety reports HSG 190 http://www.hse.gov.uk/pubns/books/hsg190.htm

Figure 3-2 – Proportionality of Risk Assessment



The depth of analysis required may vary depending on the pathways and receptors. The HSE will determine whether an Operator's depth of analysis is appropriate for risk to people. The appropriate agencies should similarly determine whether the Operator's depth of analysis is appropriate for the environment considering the worst case scenarios and the sensitivity of environmental receptors. The appropriate agency and HSE may legitimately come to different conclusions on the depth of analysis required.

QRA can be a useful tool to[25]:

- identify those events which contribute most to the risk (ie in identifying the Safety Critical Events or factors); and
- estimate the benefits of proposed risk reduction measures (here the results of the QRA for the existing plant are compared with the results for the plant incorporating proposed risk reduction measures).

Further guidance on the applicability of these techniques and proportionality of assessment is available from SPC/Perm/37[6], or paragraph 2.2 of the CDOIF Guideline[2] – Environmental Risk Tolerability for COMAH sites (or the relevant predictive assessor for a safety report).

[25] Application of QRA in Operational Safety Issues (HSE Research report 025) http://www.hse.gov.uk/research/rrpdf/rr025.pdf

4 HOW MIGHT AN OPERATOR ASSESS RISK?

The risk assessment process can be viewed as addressing seven basic questions[9]:

i) **What can go wrong?** ie identifying potential MATTE scenarios (**hazard identification**);

ii) **What gets out and how much?** ie evaluation of the size of the release from knowledge of the material(s) in question and release rate calculations;

iii) **Where does it get to?** ie dispersion (and deposition) predictions for the release;

iv) Therefore **What are the consequences?** ie an estimate of the potential severity of the accident (consequence assessment);

v) **How often?** ie an estimate of the likelihood of the occurrence (source frequency);

vi) **What is the risk and is this acceptable?** ie determination of risk levels derived from the above analyses, and assessment of their significance; and

vii) **Do any further measures need to be implemented?** ie risk management action.

The following sections discuss commonly used methods by Operators to answer these questions and guidance on the CA's position as regards their appropriate use.

4.1 Identifying potential MATTE event scenarios

The first step is to identify all potential MATTE scenarios.

As discussed in section 1.2, guidance on the thresholds for a MATTE are given in the DETR guidance[11] document and typical MATTE scenarios are given in 4.1 examples a-k. CDOIF has reviewed this guidance, to include consideration of more recent environmental legislation, and where considered necessary has provided clarification and interpretation of some of the terms used. This is summarised in "CDOIF: Guideline – Environmental Risk Tolerability for COMAH Establishments"[2].

It is normal in the first instance to assume that all control and mitigation measures can fail and apply the simple Source-Pathway-Receptor model. The CA Site Prioritisation Methodology[26] provides high level guidance on scoring source, pathways and environmental receptors (see Annex 2 of the site prioritisation methodology for example).

- Source – Identify the hazards; is there a sufficient quantity of material to cause a MATTE if the entire inventory is released to the receptor?
- Pathway – assuming all control and mitigation measures fail, is there a direct or indirect route for the material to get from the Source to the Receptor?
- Receptor – is there a sensitive receptor or high vulnerability receptor? Could incidents cause harm above MATTE thresholds?

[26] CA Site Prioritisation Methodology http://www.hse.gov.uk/comah/guidance/site-prioritisation-methodology.pdf

For each scenario, this allows a quick assessment of each source, pathway and receptor; if any link does not exist or if the maximum potential consequence, based on complete loss of inventory to the receptor, does not exceed a MATTE threshold then it can be stated that a MATTE is not possible and assessment for that scenario can stop.

Note however that care must be taken to ensure that potential scenarios are not dismissed on the grounds that one of the components (source – pathway – receptor) is missing, where this omission is because of the presence of a system or barrier which might fail. For example, a bund might be considered as a method of removing the pathway between the source and the receptor; this would not be a valid reason for concluding that there is no risk of pollution or no risk of a MATTE since there is a possibility that the bund will fail. Also, ruling out a MATTE does not mean that pollution would not occur, but simply that the impact would not be severe enough to be classified as a MATTE.

Where all three components (source – pathway – receptor) exist and the quantity of material involved is sufficient for potential consequence to exceed MATTE thresholds then it must be considered that a MATTE is possible and further assessment of that hazard is required.

4.1.1 Other factors to consider when identifying COMAH scenarios

4.1.1.1 Sites involving an industrial chemical process, that routinely store/use dangerous substances below COMAH thresholds, may still fall within COMAH due to generation of dangerous substances during an incident

As discussed in L111[10] (A Guide to the COMAH regulations, paragraph's 49-58), it is important to understand regulation (2(1)) relating to the inclusion of substances that may be "generated during a loss of control of an industrial chemical process". L111 continues "The inclusion of substances 'generated during the loss of control of a process, including storage activities', may bring within the scope of the Regulations some sites which would otherwise be outside scope or move establishments that may previously have been within the threshold of lower tier into upper tier".

This requirement has its origin in the incident at Seveso in 1976, where a reaction between two relatively innocuous chemicals produced a third (a dioxin) resulting in a major accident. Examples include toxic gases produced during combustion or reaction.

L111 clarifies the terms used and their application in paragraph 56-58:

> 56 Operators should consider substances which may be generated during a loss of control of a process, including storage activities as defined in this regulation. Operators should consider all types of scenarios, including during process and storage, that it is reasonable to foresee may lead to dangerous substances being generated.
>
> 57 The definition is not intended to bring into scope premises which do not manufacture, use or store dangerous substances, solely because of dangerous substances being generated in an accident. For example, a warehouse holding non-dangerous substances is not in scope of the Regulations solely because a fire might generate dangerous substances above threshold quantities.
>
> 58 When considering potential generation of third substances during loss of control, operators should ensure that substances are not double counted. Operators are encouraged to speak to the competent authority for advice in these circumstances.

4.1.1.2 Knock-on effects

As discussed in L111 (A Guide to the COMAH regulations, paragraph 454) "In addition to the direct consequences of major accidents there may be knock-on effects, ie secondary events involving substances which are not dangerous within the terms of COMAH but can be harmful to the environment. For example, milk discharged into a river could have very serious effects on fish and if the release were the result of a major accident it would have to be considered as one of the possible consequences. The safety report should include these where they can be identified." ie knock-on effects will contribute to establishment risk, but only if they are associated with a Major Accident.

4.1.1.3 Domino scenarios

There are specific requirements within COMAH relating to the circumstances whereby the likelihood or consequences of a major accident may be increased because of the location and proximity of establishments within a "domino group". See Regulation 24, as discussed in L111 (A Guide to the COMAH regulations, paragraph 325-334).

4.2 Consequence Assessment

The potential consequence (ie the extent, severity and the duration of harm) of each MATTE scenario should be assessed.

4.2.1 Categorising the consequence of a MATTE

There are a number of approaches that can be used to assess consequence and as with all COMAH determinations the degree of assessment should be proportionate to the risk involved.

Examples of factors that may be relevant/to be considered:

1. What is the mechanism for impact by the substance involved?
    - Is the substance immiscible and may coat the receptor and affect flora and fauna?
    - Will the substance be miscible and be diluted, causing a toxic zone?
2. Is the receptor tidal?
    - Will the substance(s) involved move up and down the receptor?
3. Cumulative impact – can a small leak be present for a period of time before being detected creating a cumulative impact?

If a risk assessment methodology such as developing an event tree is being used, then the impact may have to be reviewed for each of the event tree branches as they may result in different consequences, dependant on the degree of control and mitigation failures identified.

4.2.2 The CDOIF Approach

All information regarding the CDOIF approach has been taken from "CDOIF Guideline – Environmental Risk Tolerability for COMAH Establishments"[2]. It is expected that the guideline (or equivalent) should be used from the date of publication to carry out environmental risk assessments required by COMAH (for example within Safety Reports, SMS risk assessment or any other demonstration of AMN as required by the CA.). Using the guideline will help operators comply with the COMAH, however use of the guideline is not itself a specific legal requirement of COMAH (see Foreword to the guideline).

In order to promote consistency over the description and assessment of environmental risk, CDOIF has developed a risk matrix approach to categorising consequence, which the appropriate agencies consider to be good practice. The approach has been designed as a tool for risk screening and whilst it provides a relatively comprehensive approach for this purpose some outcomes might not have been included in the matrix.

The CDOIF approach assesses consequence as a function of both the severity and the duration of harm resulting from the scenario under consideration, allowing the assessor to determine the appropriate tolerability threshold criteria via look-up tables.

4.2.2.1 Determining the CDOIF Severity of Harm Category

The approach suggested by CDOIF uses the consequence descriptors previously used in IPPC horizontal guidance note H1 and provides an explanation of how the DETR MATTE thresholds fit with that table and further provides examples of increasing severity for each DETR receptor category. It should be noted that CDOIF severity is actually a combination of extent and severity and that the tabulated thresholds in Table 1, Appendix 4 of the guideline are only a summary of the thresholds described in full in section 3.2.

The approach enables a severity of harm level (1, 2, 3 or 4) to be assigned to the scenario:

CDOIF severity of harm categories taken from "CDOIF Guideline – Environmental Risk Tolerability for COMAH Establishments"

Row	DETR Table Ref	Receptor Type	Severity of Harm				Reference to Table 2	Comments
			Significant *While this level of harm might be significant pollution, it is not considered a MATTE.*	Severe *DETR Criteria - the lowest level of harm that might be considered MATTE.*	Major	Catastrophic	*Corresponding Harm/Duration / Recovery row in Table 2*	*The 'Severe' to 'Catastrophic' levels of harm are considered to be included as 'Serious' with respect to the COMAH definition of a major accident.* *Receptors include:*
		Severity Level →	1	2	3	4		
1	1	Designated Land/Water Sites (Nationally important)	<0.5ha or <10%	>0.5ha or 10-50% of site area, associated linear feature or population	>50% of site area, associated linear feature or population	*N/A*	Land or Surface Water	NNR, SSSI, MNR

This is used along with the harm duration category (see section 4.2.2.2) to define overall consequence and thus the tolerability threshold criteria. In this case the severity of harm should be considered as the worst case outcome for the scenario, without mitigation (ie all protection layers fail) or remediation. The extract from the CDOIF table above shows the relevant descriptors for impacts on nationally important designated land / water sites.

Appendix 1 provides further examples of large scale incidents from Seveso type establishments and other causes.

4.2.2.2 Determining the CDOIF Duration of Harm Category

The CDOIF approach then looks at the anticipated time the receptor would take to recover naturally to 80% of the mean level prior to the harm occurring. Different recovery times are allocated to different receptor types reflecting the relative speed of recovery expected for each receptor type.

The approach assigns a harm duration category to the scenario (1, 2, 3 or 4) which is used along with the severity of harm duration category to define the tolerability threshold criteria.

CDOIF duration of harm categories taken from "CDOIF Guideline – Environmental Risk Tolerability for COMAH Establishments" v2

Description	Short term	Medium term	Long term	Very long term
	Harm with such short recovery is not considered a MATTE.			
Harm Duration Category →	**1**	**2**	**3**	**4**
Groundwater or surface water drinking water source (public or private)			Harm affecting drinking water source or SPZ <6 years	Harm affecting drinking water source or SPZ >6 years
Groundwater (except drinking water sources): WFD Hazardous/Non Hazardous Substances	WFD hazardous substances <3 months	WFD hazardous subs >3 months	WFD hazardous subs >6years	WFD hazardous subs >20 years
	WFD non-hazardous substances < 1yr	WFD non-hazardous substances >1year	WFD non-hazardous substances >10 years	WFD non-hazardous substances >20 years
Surface water (except drinking water sources – see above)	< 1year	>1 year	>10 years	>20 years
Land	<3 years or <2 growing seasons for agricultural land	>3 years or >2 growing seasons for agricultural land	>20 years	>50 years
Built environment	Can be repaired in <3 years, such that its designation can be reinstated	Can be repaired in >3 years, such that its designation can be reinstated	Feature destroyed, cannot be rebuilt, all features except world heritage site	Feature destroyed, cannot be rebuilt, world heritage site

4.2.2.3 Determination of the CDOIF Consequence level and tolerability

Once the severity of harm and the harm duration categories are known then a look up table can be used to define the consequence level (A, B, C or D). In qualitative terms, the consequence levels have been developed such that consequence increases from A (locally important events) through B&C (regionally/nationally important events) to D (internationally important events). The A-D consequence level can then be used to determine the tolerability threshold criteria (ie the threshold frequency per receptor per establishment per year) – see section 4.4.

CDOIF Consequence levels and tolerability thresholds taken from "CDOIF Guideline – Environmental Risk Tolerability for COMAH Establishments"

Severity of Harm					
	4		C	D	D
	3		B	C	D
	2		A	B	C
	1	*Sub-MATTE Harm*			
		1	2	3	4
		Harm Duration Category			

Consequence Level	Frequency per receptor per establishment per year	
	Intolerable (greater than)	Broadly Acceptable (less than)
A	1.0 E-02	1.0 E-04
B	1.0 E-03	1.0 E-05
C	1.0 E-04	1.0 E-06
D	1.0 E-05	1.0 E-07

Tolerability of risk to the receptor, from the establishment as a whole, will depend on the aggregate predicted frequency of all independent accident scenarios which could impact a given receptor at or above the respective consequence level. Thus to confirm tolerability at level D then all independent level D predicted incident frequencies should be aggregated. To confirm tolerability at level A, all independent level A, B, C and D predicted incident frequencies should be aggregated.

4.2.3 Other approaches to consequence assessment

Whilst the CDOIF approach will be seen by many Operators as providing a consistent and practical methodology, there is not a legal requirement that it be used. Where an Operator wishes to use an alternative approach they may do so as long as the methodology and any criteria used within it are reasonable and justified. For example, other guidance on consequence assessment can be found in Green Leaves III[27] or DETR (1998)[28].

4.3 Likelihood Assessment

For any scenarios identified as having the potential to cause an impact meeting or exceeding the definition of a MATTE, the likelihood of the MATTE occurring must be assessed and then compared to the tolerability threshold criteria identified in section 4.2.

Often Operators will quote frequencies in a number of different ways, for example:

> A frequency of once every 100 years is equivalent to a likelihood of 1/100 per year (or 0.01 per year or $1x10^{-2}$ per year)

As discussed in section 3.1, the degree of justification should be proportionate to the risk. There are a range of techniques for assessing likelihood ranging from simple qualitative risk matrix descriptors to the more complex QRA (eg event trees).

The following sections discuss some of the more commonly used techniques.

4.3.1 Qualitative

4.3.1.1 Screening

Operators may decide to simply assume all material from a scenario is released as a worst case and place the scenario on the risk matrix – if this is within or close to the broadly acceptable region there may be a case for doing no further assessment.

When considering tolerability it is important to note that risk thresholds are for risk posed to a specific receptor from the Establishment as a whole. Very often Major Accident Hazard Scenarios will be plotted on the risk matrix individually – this is a useful screening technique, as it is self-evident that any event which is intolerable in itself will cause Establishment risk to be intolerable, however scenario risk does not, on its own, demonstrate Establishment tolerability.

Thus, assessors should be aware at this stage that an Establishment which has a number of Broadly Acceptable MAH scenario's may result in an establishment risk in the TifALARP Region and so the Operator will be required to go back and reduce the risk of one or more of these MAH scenarios (so far as reasonably practicable). Similarly a number of TifALARP scenarios may place the

[27] Green Leaves III https://www.gov.uk/government/publications/guidelines-for-environmental-risk-assessment-and-management-green-leaves-iii

[28] "Management of Harm to the Environment: Criteria for the management of unplanned releases" DETR, 1998

establishment risk in the Intolerable region and further measures to control risk would be required almost irrespective of cost.

4.3.2 Semi-Quantitative

4.3.2.1 LOPA

A LOPA (or Layers of Protection Analysis) is a systematic way of presenting risk assessment and identifying the gap between the design proposed and the threshold frequency for a scenario. They are being used increasingly in more complex areas.

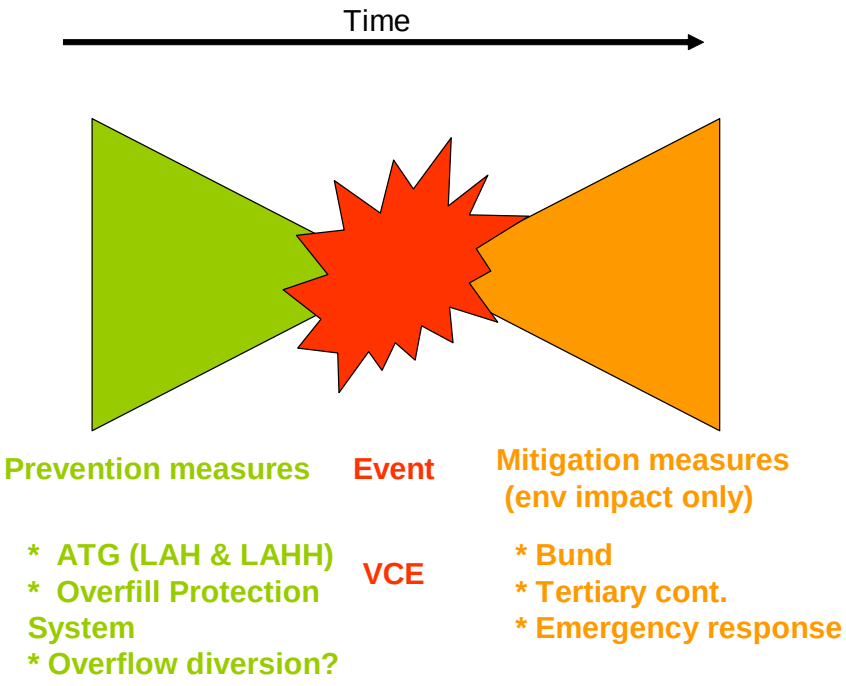
LOPA's are normally presented in a tabular form (see Appendix 2). Whilst on first viewing they may look daunting they are very similar to event trees. Each line represents a scenario, or branch of an event tree.

4.3.3 Quantified Risk Assessment

4.3.3.1 Fault Trees and Event Trees (illustrated by Bow tie diagrams)

One technique used for calculating Scenario and Establishment likelihoods is the use of fault and event trees – which together can be represented as a bow tie diagram. This technique is appropriate for higher risk situations where Quantitative Risk Assessment is required.

Figure 4-1 – Bow Tie for the Hazardous Event (Major Accident Scenario) of Tank Overfill leading to VCE (environment impact only)



In many scenarios, the failures in prevention measures leading to the initiating event (the left hand side of the bow tie) will be the same for both the environmental and the safety assessments. Where this is the case then the same initiating event frequency must be used by all CA assessors.

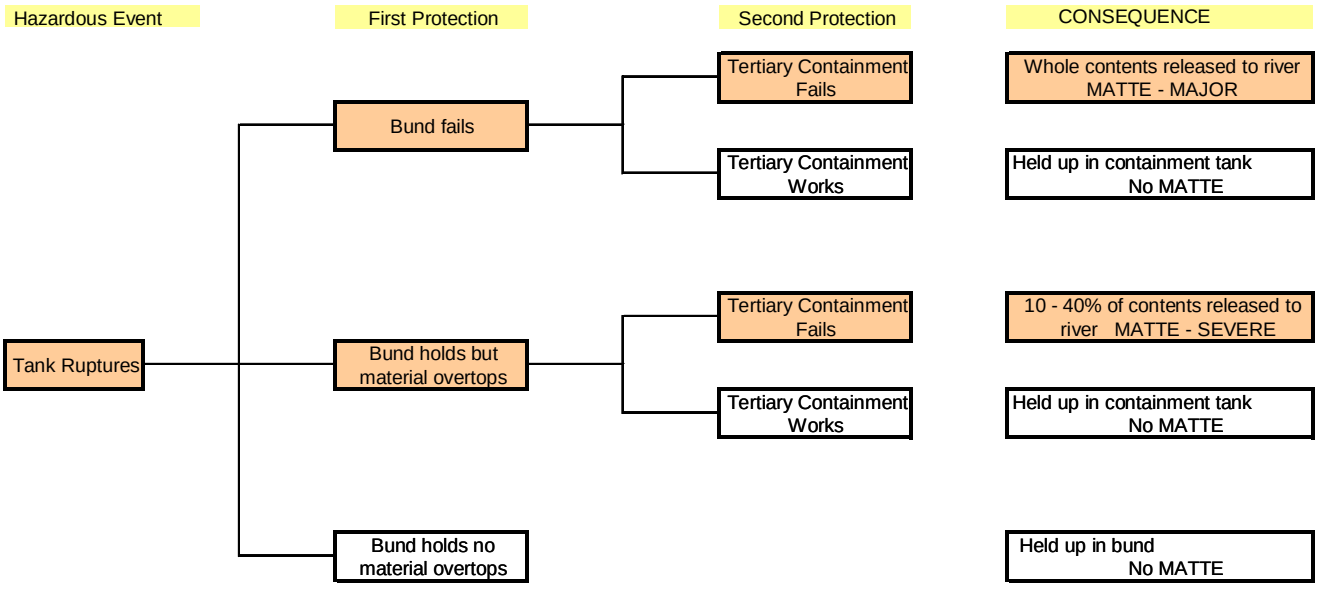
The main differences between the environmental and safety assessments will be the mitigation measures and the receptors (the right hand side of the bow tie). An event tree is essentially a

representation of this right hand side of the bow tie. Further information on environmental event trees can be found in IEC 61511 and Application of QRA in Operational Safety Issues (HSE Research report 025)[25].

To create the event tree the series of circumstances that are required to occur to cause the MATTE are laid out, starting with the initiating event (this could be tank leak, tank rupture, tank overfill etc).

A simple example is given below:

Figure 4-2 – Simple Event Tree Example without Failure Frequencies



The probability of failure is allocated to each mitigation layer. The likelihood of a given outcome occurring per year is then calculated by multiplying the initiating event frequency (the number of times an initiating event occurs per year) with the subsequent probability of failure of the mitigation layers (eg Probability of Failure on Demand – PFD) in each branch of the event tree. It may seem obvious but it is imperative that the likelihoods of fail/don't fail must add up to 1.

In all cases the Operator cannot use mitigation to rule out MATTE potential – mitigation simply reduces the consequences of an incident (and hence reduces the frequency of the more severe outcomes).

Where site specific data is not available, standard rates for typical events can be found in various sources[29].

Table 4-1 provides some typical failure probabilities / frequency data (based on expert judgement) for mitigatory measures with particular environmental relevance. The PFDs are cited as ranges to

[29] http://www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm, http://www.hse.gov.uk/landuseplanning/failure-rates.pdf, the 2010 OGP risk assessment directory http://www.ogp.org.uk/index.asp?main=publications/main.asp. For Human Failures – Discuss with HSE Human Factors Specialist. Other guidance includes EI Guidance on quantified human reliability analysis (QHRA) Nov 2012

emphasise that the likelihood of mitigatory systems failing will differ from scenario to scenario and will depend on many site specific factors (see table notes and further text below). More examples are presented in Appendix 1.

Table 4-1 – Typical Failure Data (see also Appendix 1)

Failure	Typical Likelihoods (PFD unless otherwise stated)
Bund failure on demand – flammables bund with rainwater drain valve (good quality bund to good practice standards where active intervention is required to maintain containment – eg includes rainwater gravity drain valve and/or firewater management requirements)	1 - 0.01 Note 1
Bund failure on demand – non-flammable chemical bund, no rainwater drain (good quality, well maintained bund to good practice standards where system is passive during incident, though some active management of rainwater/spilt chemical recovery will be required)	1 - 0.001 Note 2
Tertiary containment failure (likelihood depends on design of tertiary containment and the available capacity in addition to normal usage)	1 - 0.01 Note 3
Catastrophic loss of containment from a storage tank (ie practically an instantaneous tank rupture with dynamic liquid surge).	5E-06 per tank year Note 4
Major loss of containment from a storage tank (all failure modes, including mechanical failures and operational releases)	1E-04 per tank year
Off-site emergency response fails to mitigate below MATTE thresholds	1 – 0.1 or lower Note 5
Loss of containment from a warehouse fire (includes initiating frequency and subsequent escalation to involve loss of containment of a significant quantity of the hazardous materials stored but no credit for any available secondary/tertiary containment systems)	2E-04 to 9E-04 per year Note 6

Note 1 – Scenario dependent range – PFD = 0.1 is regarded typical for non-catastrophic tank failure events for a flammable liquid bund, upgraded post Buncefield (impermeable, fire-resistant etc), PFD = 1 is regarded typical for catastrophic tank failure (eg even with a bund designed to good practice it is reasonable to assume 50% overtopping unless further qualified). PFD 0.1-0.01 would not be regarded as typical but might be achievable for an actively managed bund with design to best practice.

Note 2 – Scenario dependent range – PFD = 0.01 is regarded typical for non-catastrophic tank failure events for a non-flammable chemical bund designed to good practice (including no drain valve), PFD = 1 is regarded typical for catastrophic tank failure (eg even with a bund designed to good practice it is reasonable to assume 50% overtopping unless further qualified). PFD 0.01-0.001 would not be regarded as typical but might be achievable for a bund designed to best practice.

Note 3 – Scenario dependent range – PFD = 0.1 is regarded typical. PFD = 1 is regarded typical where it is clear a site does not have tertiary containment or where larger scale events would overwhelm any limited tertiary containment available. PFD 0.01-0.001 would not be regarded as typical but might be achievable, in particular when considering smaller scale events in combination with the larger sites that have dedicated, robust tertiary containment (eg transfer systems to containment lagoons and effluent plant).

Note 4 – This data is consistent with HSE LUP guidelines. Please note there is a current EI project to produce a research report reviewing CTF failure rates for atmospheric petroleum product tanks – the data from this needs to be considered once it is published.

Note 5 – Highly case specific - Dependent on Scenario and receptor type, for example releases to groundwater would be very hard to mitigate a MATTE (PFD approaches 1) whereas a release to sewer might readily be mitigated at a treatment works. A release to ground might be readily mitigated for low permeability soils, but not readily mitigated for high permeability soils. A PFD lower than 0.1 would not be typical.

Note 6 – The figures cited are from CPR-18E "Guidelines for QRA – Purple book". Values of one or two orders of magnitude lower than those stated might be expected for a warehouse with fire detection and sprinkler / other fire extinguishing system, dependent on the fire system integrity. Conversely, this figure is for a single warehouse so higher rates might be expected if the warehouse is not standalone, but surrounded by other fire initiators (eg process plant).

4.3.3.2 Choice of PFD for environmental mitigation

Much of the information used in risk assessment is likely to be common for risks to people and the environment; hence HSE experts can be consulted to validate much of the failure rate data. For example, during routine operations a PFD between 0.1 and 0.01 might be considered appropriate for the circumstance of an operator who fails to react to an alarm or forgets to close a valve (likelihood depends on level of competence, training etc.) – such values should be discussed with HSE predictive and/or human factors specialists.

The appropriated agencies will need to take a view on the level of mitigation to the environment.

PSLG final report[17] pp.101–104 discusses how to include mitigation layers in a risk assessment. The bund or the tertiary containment and other emergency response measures need to be considered as a layer of protection (in this case mitigation since primary containment has been lost) and each needs to be assigned a probability of failure on demand (PFD).

The PSLG final report does not give PFDs, but says this requires a realistic case-by-case assessment which may take into account the extent to which measures comply with current good practice, the means of recovery of spilt material (if it is safe to do so) and the extent to which loss of integrity may occur for the event being considered. So, where the measures in place deviate from good practice (are of a lower standard), higher PFDs might be expected and conversely lower PFDs might be expected by going beyond good practice (to adopt best practice).

The values used need to be explained and justified for each case. Detailed justification will be expected where failure rates used are at the lower end of the PFD ranges in Table 4-4.

Bunding: There are several factors which might influence the choice of PFD for bunding:

- A bund for storage of flammables might have a generally higher PFD than a non-flammables bund (greater range of failure modes and more complexity involved – managing firewater for example).
- As a bund deviates further from good practice, PFD is expected to increase (eg a bund not designed to minimise risk of failure from jetting (spigot flow) might have higher PFD than one with sufficient spacing between the tank and bund wall). Thus higher PFDs

might apply if an operator had identified deviation from current good practice but had made a demonstration that upgrade of the bund is grossly disproportionate.

- As severity of scenario increases, PFD is expected to increase (eg some operators claim no credit for a VCE for concrete bunds and use PFD = 1, conversely a lower PFD might be expected for a small spill).
- If primary containment is not designed to good practice, this might increase the PFD of secondary containment:
  - example 1: if there are no ROSOVs on tank inlet and outlet then a VCE or escalating pool fire might damage pipes outside the bund and subsequent tank drain down through product pipes might bypass the bund, making the bund ineffective for secondary containment – the bund would cease to function as an independent protection layer;
  - example 2: if tank separation distances are below standard then there might be a higher likelihood of escalation and thus higher likelihood of bund failure through greater severity of incident, as explained above.

Tertiary containment: Due to the complexities of tertiary systems and multiple potential failure modes then tertiary containment PFDs below 0.1 are thought to be unlikely, though might be achievable, in particular when considering smaller scale events in combination with the larger sites that have dedicated, robust tertiary containment (eg transfer systems to containment lagoons and effluent plant). Factors that might influence choice of PFD for tertiary containment include:

- Natural topography of a site might favour containment on site (eg where on-site surface flows follow pathways to a natural depression, which can then be adapted for containment purposes).
- A tertiary system which requires emergency responder intervention during an incident (eg to transfer liquids from one location to another or to respond to alarms and close effluent plant valves) might have a higher PFD than an automated or fully passive system.
- A tertiary system reliant on pumping of liquids between one location and another might have a higher PFD (due to vulnerability to pump failure, loss of power etc) than a gravity based system.
- A system reliant on underground drainage might be considered more difficult to inspect and maintain and thus have a higher PFD than an above ground / open channel drainage system.
- The larger the scale of event, the more likely it will be to overwhelm tertiary containment systems and thus the higher the PFD (subject to the Major Accident scenarios considered in the tertiary containment design process).

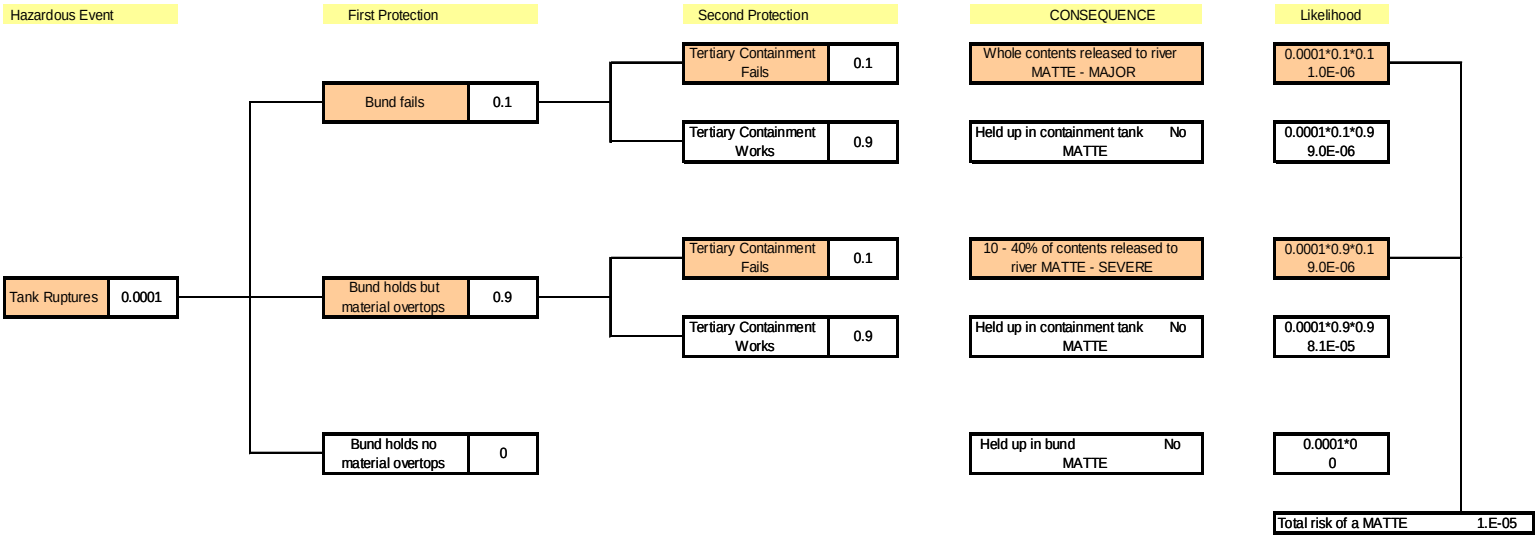
Emergency Response: These measures are mostly considered to be mitigation and as with other mitigatory measures, the likelihood of successful mitigation by emergency response will be scenario specific, but is unlikely to have PFD lower than 0.1 (0.5 might be a typical credit claimed for larger events). It is necessary for any credit chosen to be fully justified, including independence from the failings which have led to the release. If credit has been claimed for emergency response it should be considered whether the actions will completely avoid damage, or reduce the severity of damage

(eg emergency response might mitigate sufficiently for a catastrophic accident to be avoided, but the accident might still have a Major or Severe outcome and thus contribute to overall establishment or scenario risk for these lower consequence thresholds).

Factors that might influence choice of PFD for emergency response might include:

- Emergency response to a small scale event (small spill) might have a lower PFD compared to a larger event (warehouse fire / explosion) where emergency response PFD will be high (or conservatively assumed to equal 1).
- Emergency response actions are considerably more difficult to implement when mitigating impact to groundwater, compared with surface waters (thus PFD of mitigation to groundwater might be considered to be high, or conservatively assumed to equal 1).
- Emergency response actions are more likely to be successful (lower PFD) when carried out by dedicated emergency responders who have been involved in planning and exercising the specified accident scenario.
- If third party, off-site facilities are available (eg third party resources/assets available through mutual aid or similar agreements) then emergency response might be less likely to fail to mitigate.

Figure 4-3 – Simple Event Tree with Failure Rates

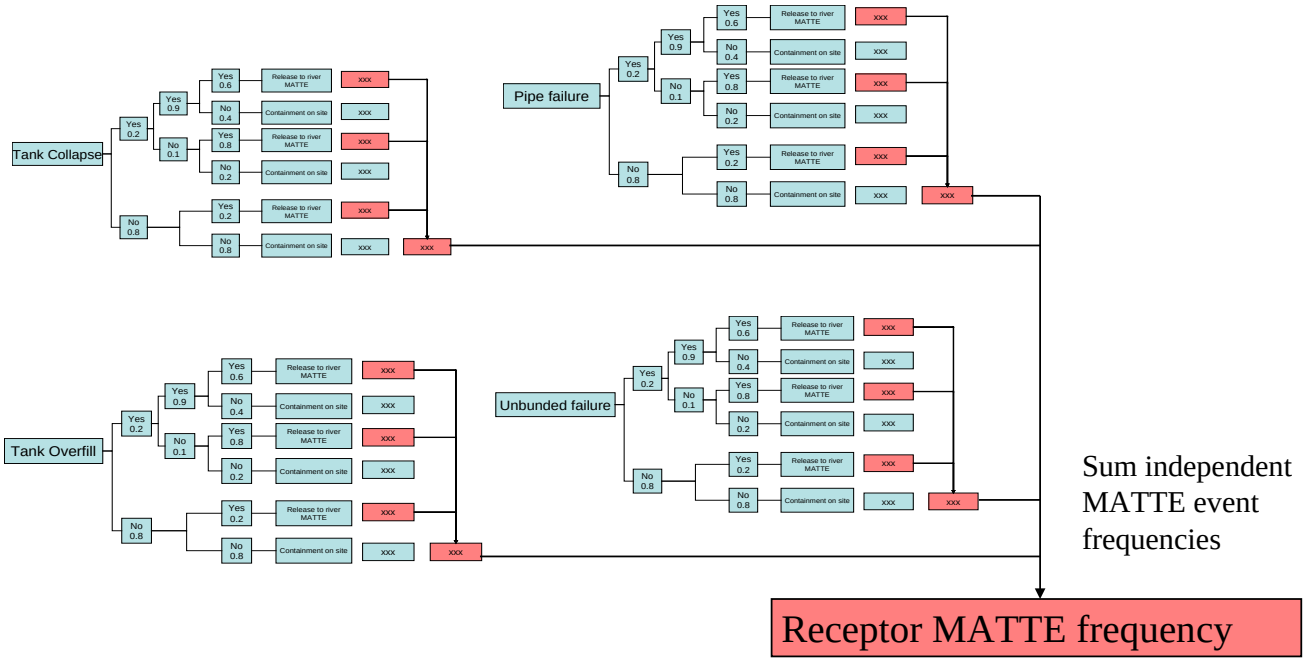


All branches on the tree with the consequence of a MATTE to a given receptor then need to be identified and the likelihoods summed to get the overall likelihood of the hazardous event leading to a MATTE to the receptor (likelihood of MATTE to different receptors should not be summed since this might cause double counting of initiating events).

At this stage, the independent scenarios are often plotted on a risk matrix to identify the scenarios with the biggest impact, where further measures would give the greatest benefit.

Finally all the independent initiating events / hazardous events which could cause a MATTE for a specific Receptor can be summed to get the Establishment likelihood for that Receptor.

Figure 4-4 – Summation of MATTE Likelihood across Independent Hazardous Event Trees



Repeat process for various pathways (air, land, water) and receptors to identify receptor(s) at greatest risk

The Establishment risk is normally then plotted on a risk matrix to assess if further measures may be required to be considered. By repeating this for all receptors the receptor most at risk can be identified (and risk reduction targeted to be most cost effective).

Where tolerability thresholds vary depending on level of harm then Establishment likelihoods need to be evaluated separately for the different consequences. CDOIF has proposed four different levels of MATTE consequence, with 4 separate tolerability bands (see section 4.2.2.3). The tolerability of these different scale consequences should be considered independently.

Thus risk needs to be evaluated for each consequence level. This involves the aggregation of risks from scenarios with consequences at or above the consequence level being assessed. For example, to ensure risk at or above consequence level C is ALARP then the frequencies with accident outcomes level C and D would be aggregated (they both exceed consequence C) and compared to the tolerability criteria established for consequence C.

4.4 Assessing the Acceptability (Tolerability) of Risk

The CA considers that, with respect to the tolerability of MATTE risk, the threshold frequencies for the Intolerable and Broadly Acceptable regions will vary for different levels of consequence. The CA also considers the most appropriate approach to determining environmental tolerability is through assessment of the risk posed by the whole establishment to a specific receptor ie the sum of the likelihood of all independent events which could lead to a MATTE affecting the same receptor.

Please note, the boundaries between the intolerable, TifALARP and Broadly Acceptable regions are not a sharp delineation of legal duty – they are presented in order to guide what is necessary to manage risk.

4.4.1 Establishment environmental risk thresholds

To assist in considering the need to apply Risk Reduction Measures, threshold frequencies can be presented in matrix or graphical format.

As discussed previously (see section 4.2.2) CDOIF has published guidance on definition of MATTE and on establishment environmental tolerability. Within this guidance tolerability criteria are presented for four different MATTE consequence levels. Consequence levels A-D represent low level MATTE (A) through to high level MATTE (D) and are determined by consideration of receptor type and extent, severity and duration of harm. From these parameters CDOIF look-up tables can be used to classify potential consequence.

The CDOIF establishment environmental tolerability criteria, presented in Figure 4-5 are viewed by the CA as good practice and any operator deviating from these might expect a higher level of scrutiny from the CA.

4.5 Summary

To confirm risk from the establishment is ALARP it is necessary for the operator to:

- Identify all MATTE scenarios (source–pathway–receptor screening). For large sites a representative set might be appropriate, but it will be necessary to estimate what proportion of the overall establishment risk is represented.
- For each MATTE, identify the worst case (no mitigation/remediation) MATTE consequence level, A to D, based on receptor specific extent, severity and duration predictions.
- Determine MATTE frequencies/consequence levels considering success/failure of mitigation (ie residual risk). Event trees have been seen to effectively enable this.
- For each receptor and each consequence level compare the aggregate frequency of all predicted establishment outcomes that remain at or exceed that consequence level (whether or not these are included in the representative set) with the appropriate tolerability criteria to determine whether risks have been reduced ALARP.
- Adopt any further control measures as necessary and re-iterate the process to demonstrate residual risk is ALARP.

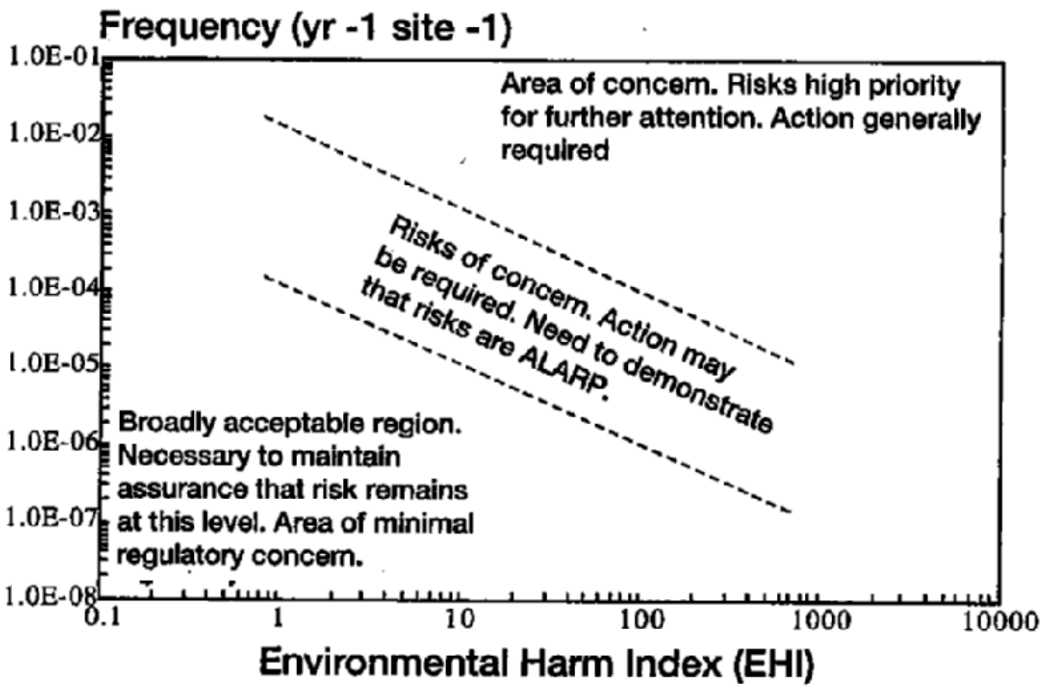
Figure 4-5 – CDOIF Establishment Risk Criteria presented in Matrix Format

	Frequency per establishment per receptor per year						
CDOIF Consequence Level	10^{-8}–10^{-7}	10^{-7}–10^{-6}	10^{-6}–10^{-5}	10^{-5}–10^{-4}	10^{-4}–10^{-3}	10^{-3}–10^{-2}	>10^{-2}
D - MATTE						Intolerable	
C - MATTE							
B - MATTE				TifALARP			
A - MATTE	Broadly Acceptable						
Sub MATTE	Tolerability not considered by CDOIF						

Note: conclusions on tolerability based on CDOIF consequence levels cannot be made without also referring to the CDOIF severity and duration tables used to classify MATTEs A-D (see section 4.2)

Other publications have also proposed benchmarks for establishment tolerability. Below are the establishment risk criteria in graph format, as proposed by DETR (1998)[28]. This approach is also acceptable for COMAH and represents a more detailed assessment of risk to surface water systems, compared to the CDOIF approach and might be appropriate where risks are high. For a summary of how EHI is calculated see Vince (2008) "Major Accidents to the Environment".

Figure 4-6 – Establishment Risk Threshold Frequencies (per receptor) presented in Graphical Format (DETR, 1998)



(fig 8.1, from "Management of Harm to the Environment: Criteria for the management of unplanned releases" DETR, 1998. Here EHI is a function of extent, severity and duration of harm to a receptor and a predicted EHI is thus an indicator of the level of potential harm - the uncertainties in the quantification process need to be recognised. Incidents with predicted EHI>100 should be regarded as having MATTE potential whilst a predicted EHI>1 should be regarded as significant).

4.5.1 Establishment risk vs scenario / safety critical event risk

When carrying out an assessment for a specified scenario, operators need to ensure the required tolerability criteria, for the establishment as a whole are met. As outlined above this is done by adding residual risk from all independent Major Accident events (including those not directly assessed as a representative scenario) and comparing this total establishment risk to the tolerability criteria (eg for a description of this process in SIL determination see BS EN 61511_3 Annex F13 – Total Risk). This type of demonstration is suited to safety reports or demonstrations of all measures necessary within a MAPP & SMS.

However, for many day-to-day management of change/risk review decisions it would be too time consuming and disproportionately onerous to review and revise total establishment risk on each occasion that a change is proposed. For that purpose risk targets can be modified / calibrated so that a fraction of the tolerable frequency is allocated, as appropriate, to the area of the installation being assessed. This could be done for example:

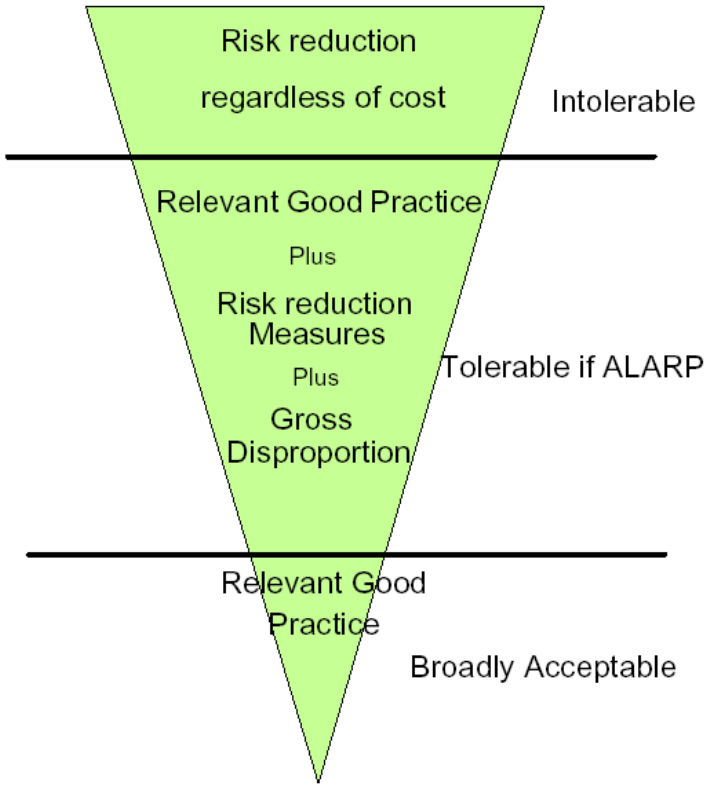
- by dividing the establishment risk target by the number of Major Accident scenarios and comparing to individual scenario residual risk (eg for individual risk it is common to assume an individual might be simultaneously exposed to 10 hazards, thus the individual risk targets are often divided by 10 to allow scenario assessment);
- by allocating target risk to a scenario / installation / plant item pro-rata and comparing to scenario residual risk;
- by calibrating a risk graph (eg BS EN 61511_3 Annex D.3).

If residual scenario risk exceeds the modified scenario target it does not mean that establishment risk is Intolerable (since other scenarios may be controlled to well below their allocated risk targets) however it should signal the need for a more thorough assessment of establishment risk and the method of allocating scenario risk thresholds. Of course, if residual scenario risk exceeds the establishment intolerable threshold then the establishment risk is also intolerable

This process is illustrated in figure 4-7, and can be applied equally to calibration of an entire risk matrix to provide a scenario risk matrix.

Figure 4-7 – Tolerability of risk: Example of Establishment vs Scenario Thresholds

If the scenario (Safety Critical Event) being assessed is 1 out of 20 possible CDOIF consequence level C MATTEs at the establishment then scenario tolerability thresholds can be estimated as 1/20th establishment thresholds



Establishment thresholds	Scenario thresholds
MATTE likelihood to a Receptor of $\geq 10^{-4}$ per year is intolerable for an accident of CDOIF consequence C	If scenario MATTE likelihood to a Receptor **$\geq 5x10^{-6}$** per year for an accident of CDOIF consequence C then need more assessment to determine establishment risk is not intolerable
MATTE likelihood to a Receptor of $\leq 10^{-6}$ per year is broadly acceptable for an accident of CDOIF consequence C	If scenario MATTE likelihood to a Receptor **$\leq 5x10^{-8}$** per year for an accident of CDOIF consequence C then establishment risk likely to be broadly acceptable
	Figures in bold are case specific for 20 MATTEs at the site

4.5.2 More detailed approaches to assessing the acceptability of risk

It must always be remembered that Risk Assessment is not an exact science and does not give an absolute answer. Therefore the outcome of the Risk Assessment will always require some degree of professional judgement based upon, for example:

- The degree to which data and judgements made within the risk assessment are optimistic or conservative (eg (i) a scenario just placed within the lower end of the Tolerable if ALARP region with an extremely conservative assessment may be considered to be Broadly Acceptable, (ii) a scenario just placed within the upper end of the Tolerable if ALARP region with an extremely optimistic assessment may be considered to be intolerable).
- Sensitivity analysis – how close to the region boundary is the event placed in relation to the accuracy of the data provided.

5 HOW MIGHT AN OPERATOR APPROACH REDUCING RISK?

5.1 Reduce the Likelihood

Further mitigations or protective layers may be installed to reduce the likelihood of a MATTE (eg upgraded Safety Instrumented Systems (SIS), improved secondary or tertiary containment etc.). Measures should be considered in accordance with the established good practice, the pollution control hierarchy (eg PPG 22) and the safety hierarchy (eg HSG190[24] para 340-349).

At this stage it is worth considering the wider benefits of any reductions proposed. For example improved tertiary containment may reduce risk of a number of scenarios, giving greater benefit – whereas an increased SIL may only impact on one scenario, giving limited benefit. If an approach such as an event tree or a LOPA has been used, it should be relatively easy to spot which particular scenario's drive the outcome (ie which contribute the greatest to the likelihood), and risk reduction measures that affect these should be considered first.

5.2 Reduce the Consequence

In some circumstances, it may be cheaper and easier for the Operator to simply reduce the potential extent and/or severity of a MATTE by adopting principles of inherent safety; for example:

- reduce the inventory of the Dangerous Substance on site – in some cases this might move the Operator down a region without spending any capital;
- substitute a dangerous substance on the site for a less hazardous material – where possible, this would also include changing the concentration of a substance preparation.

Alternatively, if all inherently safe measures have been adopted (so far as is reasonably practicable) alternate approaches to reducing the consequence include mitigation (mitigation reduces the frequency of higher consequence outcomes). For example, emergency response measures - though these might not always be successful or in some cases practicable and thus they have their own associated PFD. Again measures should be considered in accordance with the established good practice, the pollution control hierarchy (eg Section 7 of PPG 22) and the safety hierarchy (eg HSG190 para 340-349).

6 COMMON MISTAKES WHEN ASSESSING RISK

6.1 Common Mode Failure

Common mode failure is when the failure of one part of a system causes a number of others to fail – this is sometimes not recognised in risk assessment. This cannot happen when protection layers are independent.

Table 6-1 – Comparison of an overfill protection system designed with a common mode failure and one designed with independent loops

Example 1 – system designed with the potential for common mode failure	Example 2 – system designed with independent loops to provide higher reliability
L_H alarm and L_{HH} alarm and trip off a common level sensor	L_H alarm and L_{HH} alarm and trip off independent sensors
Here if the level sensor fails then neither the L_H alarm and L_{HH} alarm and trip will operate, ie there is a potential common mode failure – in this case either both are working or both are not working. Credit can only be taken for one protective layer. If the L_H alarm sensor fails to sound because the sensor is not working then the L_{HH} alarm and trip will not operate either.	Here if the L_H alarm sensor fails then the L_{HH} alarm and trip is unaffected. Credit can be taken for two protective layers. If the L_H alarm sensor fails to sound then it is possible that the L_{HH} alarm and trip may still operate and prevent overfill.
This type of system is obviously cheaper and easier to install only one port into a tank is required for the single sensor. This design may be appropriate where the loop is installed for operational or financial reasons.	Providing higher reliability, this design will be typical of that installed where the loop is part of a Safety Critical System.

Examples of similar issues include:

- control systems operating off a common power supply without suitable back-up (eg Uninterruptible Power Supply);
- if a plant operative has not responded to an alarm – why would he operate a manual valve?

6.2 Ruling out MATTE due to Mitigation Layers

It is often claimed that presence of a mitigation layer such as bunding or emergency response removes potential for a MATTE when in fact mitigation only reduces likelihood of MATTE (mitigation reduces the frequency of higher consequence outcomes).

7 DEMONSTRATION THAT ALL MEASURES NECESSARY HAVE BEEN TAKEN.

The CA considers all measures necessary to be in place when:

a) the risks are demonstrated to either Broadly Acceptable or ALARP; and

b) that demonstration has been accepted and verified.

All measures necessary must be in place for each separate major accident, whether the major accident is included as a representative scenario for risk assessment / demonstration purposes or not.

Regulation 5(2) requires that "Every operator must demonstrate to the competent authority that it has taken all measures necessary as specified in these Regulations."

This means that both Upper Tier (UT) and Lower Tier (LT) establishments are required to make such demonstrations: for UT establishments most of this demonstration should be within the Safety Report; at LT establishments the demonstration will normally be requested through a site inspection.

7.1 Broadly Acceptable Region

In this region the CA starts with the expectation that "good practice" will be implemented (so far as is reasonably practicable) in line with section 0.

Appropriate implementation of "good practice" is particularly important in this region as they may be the only measures implemented.

7.2 Tolerable if ALARP (TifALARP) Region

7.2.1 ALARP Demonstrations

It is expected that for any risks that fall within the TifALARP region the Operator will adopt good practice (so far as is reasonably practicable) and carry out an ALARP assessment to determine what more could be done to reduce risk.

The case specific demonstration in the TifALARP region is essentially a simple concept, which can be satisfied by the operator answering two fundamental questions in relation to identified Major Accident Hazard (MAH) scenarios.

- **What more can I do to reduce the risks?**
  - The Operator should look systematically at the risks from his operations and draw up, in a proportionate way, a list of measures which could be implemented to reduce these risks. Only in a minority of circumstances will there be nothing further that the operator could do. However the need to act is determined by answering the second question.
- **Why have I not done it?**
  - The answer to this may be qualitative or quantitative in nature depending on the predicted level of risk prior to the implementation of those further measures. Whatever way the question is answered, if the measures are reasonable based on engineering considerations

and it cannot be shown that the measures are grossly disproportionate to the benefit to be gained, then the operator is duty bound to implement that measure.

The meaning of grossly disproportionate is discussed in section 7.2.3.

A simple tabulated format for presentation of an ALARP demonstration is given in Table 7-1.

Table 7-1 – ALARP demonstration template

What more can I do to reduce the risks?			**Why have I not done it?**			
Scenario	Options to reduce risk	Benefit(s) achieved	Cost of option	Is the cost grossly disproportionate? (YES/NO – if YES state reason)	Will the option be implemented?* (YES/NO – if NO state reason)	Proposed implementation date (enter date or N/A)

* If the option to reduce risk is current good practice and it is not intended to implement it then a more in depth justification is required, combined with an analysis of what other reasonably practicable measures can be adopted to achieve an equivalent level of risk reduction.

7.2.2 Proportionality

Proportionality must be considered for at least two aspects of the assessment:

- the rigour or robustness or depth of risk assessment and demonstration (as discussed in section 3); and
- the level of gross disproportion appropriate in the ALARP region.

7.2.3 Cost Benefit Analysis and Grossly Disproportionate

Proportionality is also relevant to demonstration of all measures necessary. The higher the risk is within the "tolerable if ALARP" region, the greater the costs that should reasonably be incurred to reduce the risk. This is assessed by cost-benefit analysis (CBA) with the presumption that additional measures must be taken unless the cost is "grossly disproportionate".

For a measure to be necessary the costs do not simply have to outweigh the benefits; the costs must be grossly disproportionate to the benefits. Here the judgement needs to be on the basis of including all costs and all benefits.

To assist in determining this, the CA (building on work of HSE[30] has proposed a framework for cost benefit analysis using a "disproportion factor" which is a benchmark for the ratio of costs to benefits.

[30] Cost benefit analysis http://www.hse.gov.uk/risk/theory/alarpcheck.htm

If the ratio of costs to benefits exceeds the disproportion factor then the costs can be said to be grossly disproportionate.

A measure is reasonably practicable unless

Costs / Benefits > Disproportion Factor (DF)

In carrying out this calculation the CA interprets benefits to be all benefits arising from reduction of risk (to include avoiding fatality, avoiding environmental harm and other benefits.

This approach is underpinned by a benefit of avoiding a statistical fatality of approximately £1.8M (2013)[31]. HSE has proposed a disproportion factor between 1 and 10 in the ALARP region (ie cost per avoided fatality could range from £1.8M to £18M), but the relationship has not been more precisely defined.

For MATTEs, there are no commonly agreed values for preventing a MATTE similar to the £1.8M value of avoiding a human fatality. The value of preventing or mitigating a MATTE will be dependent on the value of the specific receptor and associated clean-up and restoration costs and can run into £10sM. Thus unlike single fatalities, which have equal impact and value, a MATTE can have variable impact and value depending on a number of factors including:

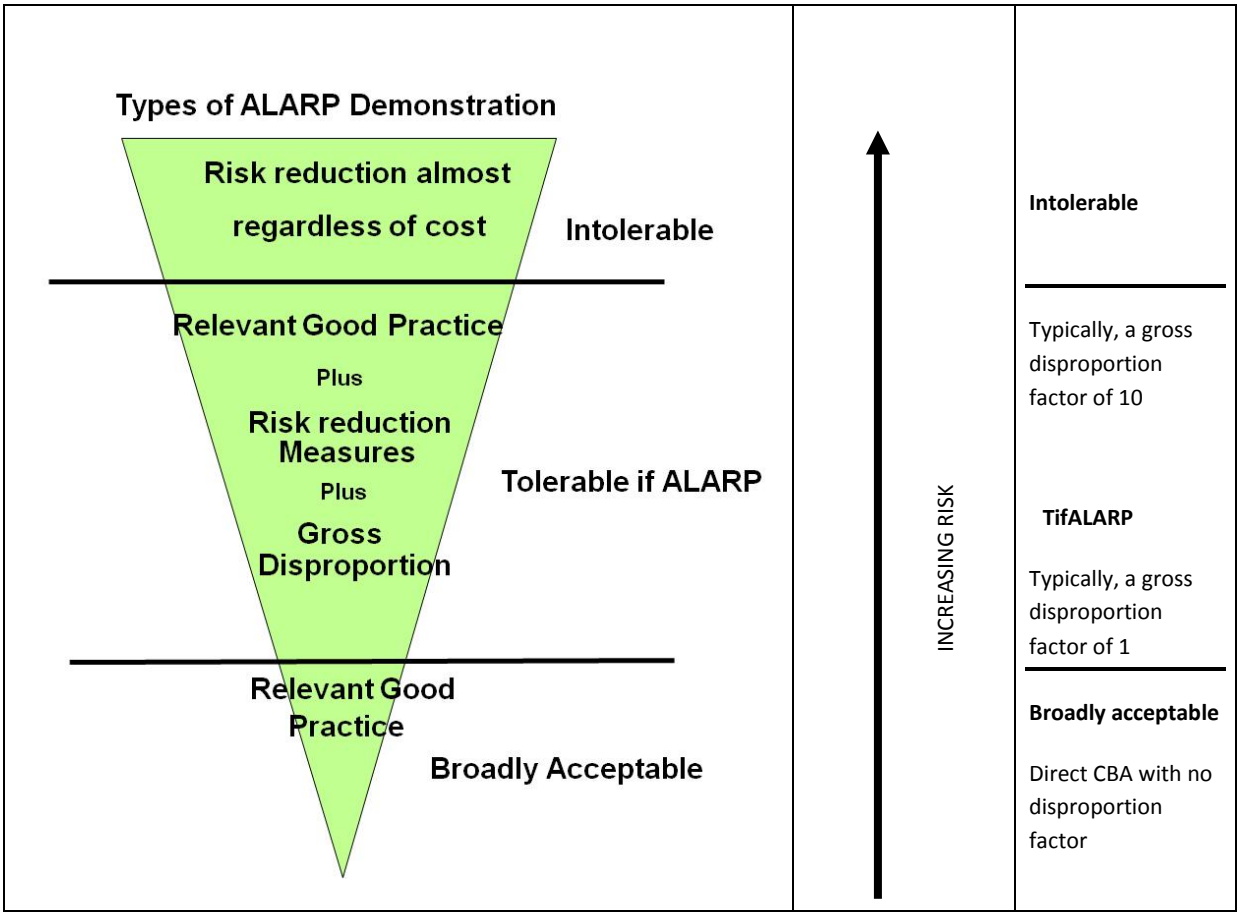
- How much of the receptor has been affected?
- How many of the species have been affected and what proportion of the population is this?
- How long will it take the receptor or species to recover?
- Is there any direct economic loss, such as loss of abstraction?
- How much will clean-up and restoration cost (to include action to remove the dangerous substance from the environment and remedial measures such as restocking and restoring habitat)?

Thus predicting the cost of a MATTE is difficult – some historical costs are provided in Appendix 1.

The COMAH regulations define an EC reportable incident and as such the listed criteria are taken as equivalent. Therefore the starting point for an environmental assessment is that it is reasonable to assume a proportion factor between 1 and 10 in the ALARP region (see Figure 7-1). Thus for any given scenario it is necessary to understand the tolerability thresholds appropriate to the consequences and where in the TifALARP zone the establishment lies in order to select an appropriate disproportion factor.

[31] ALARP guidance quotes £1.3M (2003), and HSE EAU £1.6M (2010) http://www.hse.gov.uk/economics/eauappraisal.htm

Figure 7-1 – Tolerability of Risk Diagram with Typical Gross Disproportion Factors



In the Broadly Acceptable region measures can be assessed on the basis of a direct balance between costs and benefits (proportion factor = 1).

However the assessor must then consider the questions raised above and consider what is reasonable in the circumstances:

- where a receptor will recover quickly and/or its loss will not have a knock on effect on other species then this proportion factor could possibly be reduced;
- where a significant proportion of the population of a species has been affected and/or recovery will be slow (or recovery will not occur) then the full factor should be applied.

At this point it is re-emphasised that CBA only strictly applies to measures in addition to all relevant good practice and appropriate agency inspectors should take this line for all new build or significant changes at existing establishments. With respect to existing establishments, any deviation from current good practice where upgrade is not proposed requires in depth justification from the operator and similarly requires the appropriate agencies to challenge this position in depth (what alternatives are available to reduce risk? Are costs and benefits truly representative? Have risk assessment and CBA methodologies been correctly followed?). Appropriate agency inspectors should only accept a deviation from good practice after full CA assessment of Operator demonstrations and inspection of the measures in question and the CA will not usually accept a lower standard of protection than would be provided by the application of current good practice -

further advice should be sought from specialists, including EA technical advisor or SEPA COMAH Lead.

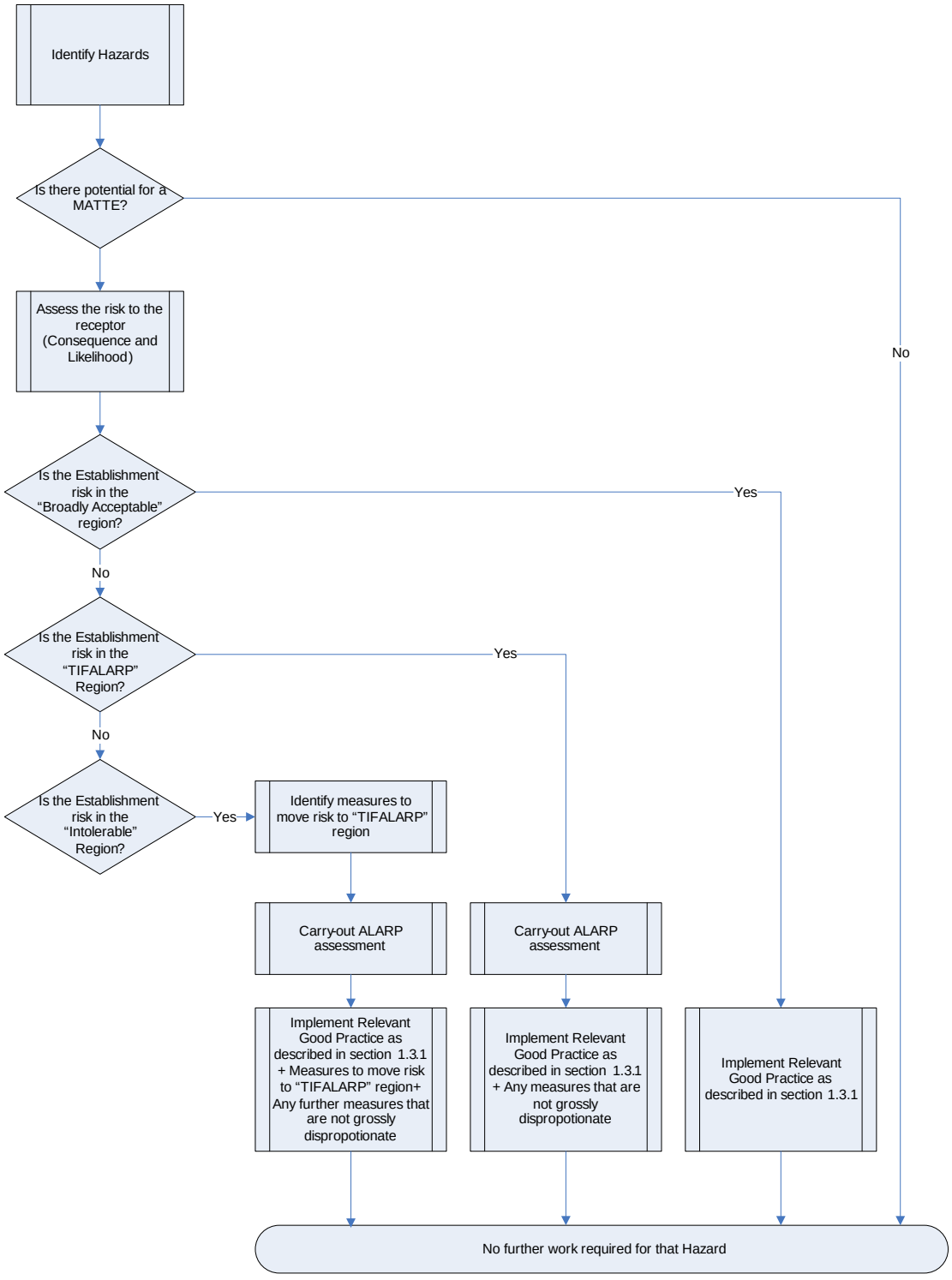
7.3 Intolerable Region

As discussed above if the scenario or establishment falls within this region, then the Operator must identify further improvements to reduce the risk and these should be implemented almost irrespective of cost. Only once the proposals identified would move the risk of the scenario/establishment into the TifALARP region can an ALARP assessment be completed to decide if it is appropriate to carry out further improvements above and beyond those required to move into the TifALARP region.

8 APPROACH TO SAFETY REPORT ASSESSMENT

The basic COMAH assessment process is reasonably straightforward and is summarised in Figure 8-1. All statements referring to implementation of risk reduction measures are subject to ALARP principles, including that of risk reduction So Far As Is Reasonably Practicable.

Figure 8-1 – Summary of COMAH Assessment Process



9 CONCLUSIONS

As described in section 1.3, in-line with the ALARP 2 guidance[5], the CA's expectation is that:

a) COMAH operators will "apply relevant good practice as a minimum";

b) it is also recognised that "it might not be reasonably practicable to apply retrospectively to existing plant, for example, all the good practice expected for new plant"; in these circumstances however "there may still be ways to reduce the risk eg by partial solutions, alternative measures etc."

The need to upgrade existing facilities to relevant good practice is strictly not subject to cost-benefit analysis in the ALARP sense but clearly such upgrading (whether the measures themselves or the time-scales) must be proportionate in the circumstances. If there is deviation from current good practice then the operator could upgrade to current good practice or otherwise should implement equivalent risk reduction by other means where reasonably practicable (deviation from good practice will require justification). Inspectors can consult an EA Senior Advisor or SEPA/NRW COMAH lead prior to reaching agreement on upgrade time-scales or where considering operator proposals which would not lead to the full implementation of relevant good practice.

Decisions on All Measures Necessary are guided by consideration on the tolerability of risk:

- if risk is in the **Intolerable** region then ALARP cannot be demonstrated and action must be taken to reduce the risk almost irrespective of cost;
- in the **TifALARP** zone, all reasonably practicable risk reduction measures should be adopted in addition to relevant good practice. These additional measures to reduce risk need to be based on local site considerations: the requirement to undertake such measures is subject to cost-benefit analysis and the test of "gross disproportion";
- when risk is controlled to a level that is **Broadly Acceptable**, we as regulators would not usually require further action to reduce risks, beyond adherence to codes, standards and established good practice so far as is reasonably practicable.

APPENDIX 1 – Environmental QRA data and MATTE case studies

Note 1 – the following data has been compiled from literature based on historical information and thus may not be fully representative of an establishment designed, built and operated to present day good practice. See final page of this document for references to Appendix 1.

Note 2 – this data can be used as a comparator for scenario data presented by operators, but site specific circumstances may mean that individual establishment data may deviate from this information and specialist advice should be sought before drawing conclusions.

FUEL TANK FARMS - SCENARIO DATA

The data below is a summary – more info can be found from International Association of Oil and Gas Producers (IOGP), see the risk assessment data directory published in 2010 for example[32].

Tank events

Spill on roof [1]	1.6 E-3 per tank year
Sunken roof [1]	1.1 E-3 per tank year
Roof failure (AST > 450m^3) [2]	2.0 E-3 per tank year
Major Release (AST > 450m^3) [2]	1.0 E-4 per tank year
Minor Release (AST > 450m^3) [2]	2.5 E-3 per tank year
Release outside shell – all modes & scales [1]	2.8 E-3 per tank year
Breakdown of failure modes for release outside shell [1]	
Tank bottom corrosion	4 E-4 per tank year
Failure of roof leg pads	0.3 E-4 per tank year
Bottom annular plate corrosion	1 E-4 per tank year
Steam coil failure	0.9 E-4 per tank year
Drain Failure	4 E-4 per tank year
Mixer leak	3 E-4 per tank year
Leak from pipework, etc	5 E-4 per tank year
Overfill	4 E-4 per tank year
Catastrophic failure rate (AST > 450m^3) [2]	5 E-6 per tank year
Catastrophic failure rate [9]	3 E-6 per tank year

N.B. HSE does not support the derivation or use of the catastrophic failure rates discussed in the paper *'IChemE 139 - bund effectiveness in preventing escalation of tank farm fires'*.

[32] Risk Assessment Data Directory – Guide to finding and using reliability data for QRA http://www.iogp.org/pubs/434-20.pdf
Risk Assessment Data Directory – Storage incident frequencies http://www.iogp.org/pubs/434-03.pdf
Risk Assessment Data Directory – Process release frequencies http://www.iogp.org/pubs/434-01.pdf
Risk Assessment Data Directory – Human factors in QRA http://www.iogp.org/pubs/434-05.pdf

Tank Fires

Spill on roof fire [1]	3 E-5 per tank year
Full surface fire [1]	3 E-5 per tank year

Bund fires

Small bund fire [1]	9 E-5 per tank year
Large bund fire [1]	6 E-5 per tank year

All sizes

Highly flammable liquid [3]	1.2 E-4 per tank year
Flammable liquid [3]	1.2 E-5 per tank year

Fire escalation probabilities

Small bund fire escalation [1]	negligible
Large bund fire impingement causing rim seal fire [1]	0.5
Large bund fire impingement causing full surface fire [1]	0.5
Large bund fire impingement causing tank fire [1]	→ 1 (ie highly probable)
Rate of spread to other tanks in common bund [3]	→ 1 (ie highly probable)
Tank in single bund, failure rate if involved in bund fire [3]	0.5

Bund Failure Probabilities (fuel tank farms – fire scenarios)

All scenario FoD [3]	0.4
Multi tank bund FoD [3]	0.8
Single tank bund FoD [3]	0.3

(NOTE these figures are based on pre-Buncefield incidents and it is anticipated bund failure PFD will be reduced to say 0.1 for an upgraded bund meeting PSLG / containment policy).

Bund failure – HFLs general

Bund overtopping following catastrophic tank failure (50% lost)[4]	1 (ie assume 50% overtopping with CTF)

(Note – whilst the HFL SRAG suggests the assumption that all CTFs will result in 50% loss from the bund, there is a growing body of literature citing incidents and experimental observations with regard catastrophic tank failures. Overtopping fraction lost may vary due to bund general arrangement relative to tank dimensions. Overtopping fractions are cited in the literature in a range of up to 70%. Estimates made following actual incidents have calculated overtopping fractions in the range 25% and 50%. Some bunds, however, may not withstand the hydrodynamic load of liquid or force of tank impact and thus loss could approach 100%)

NON-SUBSTANCE SPECIFIC DATA

See SRAGs for predictive criterion guidance http://www.hse.gov.uk/comah/srag.htm

HSE has published Generic Failure Rate and Event Data for LUP (noting it can be used for COMAH if site specific data is lacking) [2] http://www.hse.gov.uk/landuseplanning/failure-rates.pdf

See Purple book for comprehensive listing of failure rate data[5]

See BSA website for info on sprinklers http://www.business-sprinkler-alliance.org/

Tank failure

LOC AST Instantaneous [5]	5E-6 per tank year
LOC AST over 10 mins [5]	5E-6 per tank year
LOC AST 10mm diam [5]	1E-4 per tank year
Catastrophic / complete tank failure rate [6]	5 E-6 per tank year
Catastrophic tank failure - probability of escalation to involve adjacent tanks [6]	0.2

Bund Failure

All bunds, all modes (passive containment and adequate watertightness & capacity) [7]	0.01-0.001

(Note – this rate is considered very low and not applicable for fire scenarios where active firewater management is required and for bunds with active management of rainwater drain valves. In these cases 0.1 might be the lowest PFD expected unless best practice was adopted and then PFD might be no lower than 0.01)

All modes, wet test FoD [8]	0.5

(Note, whilst this is an actual survey result it is hoped that CA focus on bunding as safety critical will reduce PFD)

Relative failure modes for bunds failing wet tests[8]	Pipe hole 6% Drain hole 18% Crack in base 27% Crack in wall 31% Poor construction 18%
Bund overtopping following catastrophic tank failure (50% lost) [9]	1 (ie assume 50% overtopping with CTF)

(Note – whilst the HFL SRAG suggests the assumption that all CTFs will result in 50% loss from the bund, there is a growing body of literature citing incidents and experimental observations with regard catastrophic tank failures. Overtopping fraction lost may vary due to bund general arrangement relative to tank dimensions. Overtopping fractions are cited in the literature in a range of up to 70%. Estimates made following actual incidents have calculated overtopping fractions in the range 25% and 50%. Some bunds, however, may not withstand the hydrodynamic load of liquid or force of tank impact and thus loss could approach 100%).

Relative failure modes for incidents with on/off-site impacts [10]	Bund leak or overfill 56%, Bund incomplete or absent 32%, Bund collapse or materials in bund area 6%, Spigot flow 6%

Warehouse fire

Useful data from on VCE potential from aerosol warehouses the HSL report http://www.hse.gov.uk/research/rrhtm/rr916.htm. Whilst focusing on the top end event (and estimating this to have very low frequency) it does have useful data for other fire events, initiation and escalation/mitigation (eg see table 6 & 7 appendix D).

Loss of Containment for substances in:

Warehouse fire - rate [5]	1.8 - 8.8 E-4 per year
Initiation of fire - rate [11]	1 E-2 per year
PFD sprinklers – failure to control / extinguish [12]	0.03 (10 yrs European data)

MATTE case studies (and other Major / Catastrophic incidents of note)

ref	Year	Place	Accident	Substance	Amount released	Impact	Costs (not date adjusted)	Lessons
[xiii] & [xiv]	1976	Seveso Italy	Seveso	Dioxin (TCDD)	1 / few kg	10 sq miles land and vegetation contaminated. Many animal deaths 600 people evacuated, 2000 people treated for dioxin poisoning	>$10 billion clean-up and compensation	Seveso Directive
[xv] & [xvi]	1986	Switzerland	Sandoz warehouse fire	Flammables, Toxics & R50/53 Pesticide & firewater	Est. <30 tonnes dangerous substances (out of 680 tonnes total) in firewater	Extensive cross border to Rhine killing most aquatic life over 100s km & many years recovery	€90M total €24M remediation €27M compensation €39M damage to premises	Pollution could have been reduced by: Sprinklers (reduce vol. of water) Better containment (warehouse and drainage) Firewater management plans
xv & xix	1989	Prince William, Alaska	Exxon Valdez (tanker)	Crude Oil	38,000 tonnes	Pollution of 1090 miles coastline, large kill of otters, seabirds. Long term recovery (half species recovered after 10 years)	$1-2B clean-up $100M ecological recovery	
xv & [xvii]	1992	Bradford UK	Allied Colloids fire	Oxidising & flammable raw materials warehouse & external drum store	Some of the 16M litre of firewater runoff	10 - 20,000 fish killed over 50 km stretch of river		New warehouse – high fire prevention standards, sprinklers, segregation. New £4M water supply, drainage and containment system installed with boundary walls and retention basin (see CIRIA 164 p.65 on for more detail).

ref	Year	Place	Accident	Substance	Amount released	Impact	Costs (not date adjusted)	Lessons
[xviii]	1996	Millford Haven UK	Sea Empress (tanker)	Oil & fuel	72,000 tonnes crude and 370 tonnes HFO	Pollution of 200km coastline. Beach closures, temporary fishing bans. Wildlife recovery within 2 years	$60M total $36M clean-up	
[xix] & [xx]	1998	Portugal	Porto refinery spill, followed by flow off-site and ignition on beach	Crude oil	230 m^3	One fatality, human injuries, water contamination	€20M (material loss)	Motorise block valves to reduce response times, Improve onsite drainage systems and procedures to minimise risk of hydrocarbon release through outfall
xv	1998	Spain	Aznalcollar tailings dam, Donana lowlands	Tailings, acidic & heavy metals	5 – 7 million m^3 (incl. 2 million m^3 mud)	5000 ha agricultural land destroyed Aquatic life killed over first 40km of spill (30 tonnes dead fish)		
xix	2000	Sweden	Gällivare, Tailing dam failure	Tailings		Material loss, ecological harm		
xv	2000	Romania	Baia Mare tailings dam	Inc. cyanide	100,000 m^3 tailings water	Extensive cross border >1000km rivers 1240 tonnes dead fish in Hungary alone Drinking water interruptions to 2.5M people		
[xix]	2000	France	Haguenau, Large fire in a glues and resins factory			Ecological harm	>15 million Euro (material loss)	

ref	Year	Place	Accident	Substance	Amount released	Impact	Costs (not date adjusted)	Lessons
[xix]	2004	Italy	Ancona Explosion and fire in a storage facility during loading			One fatality, three people injured, ecological harm	€6.5M (material loss) €56M (costs for renovation and disrupted production)	
[xxi]	2005	Milford Haven	Petroplus tank bottom leak	Kerosene	~650 tonnes	>1ha groundwater contaminated.	> £3 million clean-up	Pollution could have been avoided / reduced by: Inspecting to standards (API 653 / EEMUA 159) Impermeable tank bases Inclusion of tank bottom leakage as Major Accident Scenario
[xix]	2005	Belgium	Kallo, Major leak in a storage tank			Soil contamination		
[xxii]	2005	Buncefield	HOSL, Buncefield explosions and fire	Fuels	1000s tonnes fuel and firewater (68 million litres used)	>1ha groundwater contaminated. Extensive damage to property on and off-site	£1 Billion total Site clean-up estimated to be £30-50M with ongoing remediation adding to this	See publications of MIIB / PSLG & CA Containment Policy and Buncefield : Why did it happen?
EA	2006	Andoversford UK	Biolab fire	Swimming pool / water treatment chemicals	> 40 tonnes R50 involved	~2500 fish killed over 6km river with 4-7 yr recovery time predicted. Road closures and business disruption		Pollution could have been reduced by: Better containment & knowledge of drainage pathways on and off site.
[xxiii] [xxiv]	2006	Louisianna, USA	Hurricane Katrina, Murphy	Mixed Arabian Crude	25,000 bbl	City canals and over 1 sq mile of neighbourhoods	$50M fine $70M clean-up	Pollution could have been reduced by:

ref	Year	Place	Accident	Substance	Amount released	Impact	Costs (not date adjusted)	Lessons
[xxv]			Oil tank failure - flooding			oiled	$30k per home compensation	filling tank before flooding so it did not float; Query adequate bund? Flood risk assessment?
	2008	Dormagen, Germany	Ineos Explosion & fire after pipeline rupture	Ethylene – escalation to acryl nitrile		on-site and environmental damage	€3.2M (on-site & environmental damage) €40M (material loss)	

For more examples see eMARS.

There are 10,000 Seveso sites in Europe. 339 major accidents were reported under the MARS (Major Accident Reporting System) scheme for the period 1998–2009 (MARS, 2010), with 22 incidents had impacts on the environment exceeding reportable thresholds.

APPENDIX 2 – EXAMPLE OF A LOPA ASSESSMENT USING A STANDARD TEMPLATE

Frequencies are in events per year, other numerical values are probabilities.

1	2	3	4	5	6	7	8	9	10	11	13	14	15	16	17	18	19	20
	Select severity cell below and choose a severity level from the drop down list		Enter 1 if none or if constantly present. Note: enter description of enabling event in comments box	Enter nothing if no IE	Enter 1 if no credit claimed. BPCS includes all equipment and people required to perform basic process control. This may vary with each scenario	Enter 1 if CM not relevant or always present for associated IE. CM values are probability of success therefore care is needed in how CM is worded					Protection layers (PLs) and Mitigation layers (MLs) PFD Enter 1 if no credit is claimed for IPL or IML relevant to each IE. **Figures represent PFD**			IE frequency /yr multiplied by the enabling event and any conditional modifiers ((5*(4*7*8*9*10*11))	LOPA ratio Risk target frequency divided by residual risk frequency	User proposed SIF value must be entered as a PFD Enter 1 if non chosen	**Residual risk without proposed SIL**. This columns equates to the scenario frequency multiplied by the existing protection layers (16*(6*13*14*15))	**Residual risk including the user proposed SIL**. This columns equates to (18*19)
Scenario Description for SCENARIO A	***Select Severity Level (company specific) from pull down list below***	***Initiating Event identifier***	***Enabling Events (e.g. fill operations per year or % of yr present)***	***Initiation Event Frequency (freq / yr)***	***BPCS dangerous failure rate per hour***	***CM1 probability of ignition***	***CM2 probability of person on site raising alarm***	***CM3 probability of calm weather***	***CM4 probability operator is in hazard zone***	***CM5 probability of fatality***	***IPL 1 ATG Alarm***	***IPL 2 e.g. existing shutdown system***	***IMLs e.g. Overfill detection fails***	***Frequency of unmitigated consequence***	***Level of risk reduction required to meet stated risk target***	***User Proposed SIF Integrity Level (PFD)***	***Intermediate Event frequency (events/yr)***	***Frequency of mitigated consequence***
Gasoline bulk storage tank overfill leading to vapour cloud explosion.	**(S) Serious**	***IE1***	1	10	1.00E-07	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E-01	8.00E-01	5.84E+01	4.00E-03	8.00E-10	3.20E-12
		IE2	1	2	1.00E-03	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E-01	1.60E-01			1.60E-06	6.40E-09
		IE3	1	50	1.00E-03	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E-01	4.00E+00			4.00E-05	1.60E-07
		IE4	1	0.05	1.00E-02	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E-01	4.00E-03		SIL2	4.00E-07	1.60E-09
		IE5	1	0.1	1.00E-03	0.8	1	0.1	1	1	1.00E+00	1.00E+00	1.00E-01	8.00E-03	NO SIL REQUIRED		8.00E-07	3.20E-09
Company Risk Target	1.00E-05													4.97E+00			4.28E-05	1.71E-07
Inputs														**Outputs**				

Each line represents a scenario, or branch of an event tree.

1	2	3-6	7-11	13-15	16	17	18	19	20
defines the scenario considered.	defines the severity of the outcome (this sets the risk threshold).	calculates the likelihood of the initiating event (or IE) occurring (eg loss of containment from a tank due to over fill, or loss of containment from a tank due to catastrophic failure)	This section describes the condition modifiers (or CM) which apply. These are NOT protection layers but factors that would affect the likelihood of the outcome occurring – for example the probability of low wind speed so that a vapour cloud is not dispersed, or the probability that a bird species in present on a receptor (if an over-wintering bird – this may not be for 100% of the year). The probability of the modifier occurring is recorded eg if the vulnerable species is present all year round then a factor of 1 would be used or there is an 80% chance that the cloud will not be dispersed so a factor of 0.8 would be used.	This section describes the independent protection or mitigation layers (IPL's or IML's) that are present. For example, trips, secondary and tertiary containment. The probability of failure on demand (or PFD) is recorded for each.	This is the frequency of the unmitigated consequence ie ignoring any protective or mitigation layers P(IE) x CM1xCM2….	This the LOPA ratio – ie risk target/ residual risk obviously anything greater than 1 requires further analysis	If the further mitigation proposed is an increase in the reliability of a Safety Instrumented System (SIS), then the relevant factor can be entered here.	This is the frequency of the mitigated consequence ie Column 16 multiplied by the IPL and IML factors	This is the frequency of the mitigated consequence taking account of any proposed improvements in column 18 ie Column 19 multiplied by the factor in column 18. If no improvements to SIS are proposed then this value will be the same as Column 19.

COMMENTS

Company Name: ***Name of LOPA Site***
LOPA Overview: ***Why the LOPA has to be verified.***
Date:
Assessor:

Output Summary	
Freq of unmitigated consequence	**8.2E-03**
Freq of mitigated consequence	**8.2E-07**
Risk target met?	**Yes**
Risk gap to meet target (PFD)	
Risk gap to meet target (RRF)	
Required SIF SIL for risk gap	**NO SIL REQD**

The suggested risk targets below may be considered conservative but may be used; alternativly the company can enter their own risk targets.

Severity Level	Safety Consequence	Environmental Consequence	Maximum Frequency of Mitigated Event Likelihood per
(M) Minor	Serious Injury	Sub MATTE	**1.0E-05**
(S) Serious	Possible fatality	MATTE	**1.0E-06**
(E) Extensive	Between 1 and 20 fatalities	MATTE exceeds EC reporting	**1.0E-07**
(U) User Defined	User defined RTC	User defined	

	Low demand SIL ranges		High demand SIL ranges	
Target SIL	**Max**	**Min**	**Max**	**Min**
SIL1	1.0E-01	1.0E-02	1.0E-05	1.0E-06
SIL2	1.0E-02	1.0E-03	1.0E-06	1.0E-07
SIL3	1.0E-03	1.0E-04	1.0E-07	1.0E-08
SIL4	1.0E-04	1.0E-05	1.0E-08	1.0E-09
Select SIL Demand Rate (high/low) from cell below				
Low				

Combiner tool.

This is **not** part of the LOPA calculation. It is a **tool to help** combine CM OR IPL values.

CM Combiner		IPL Combiner	
CM1	1.0	IPL1	1.0
CM2	1.0	IPL2	1.0
CM3	1.0	IPL3	1.0
CM4	1.0	IPL4	1.0
CM5	1.0	IPL5	1.0
Product CM	**1.0**	**Product IPL**	**1.0**
Set unused CM to 1		Set unused IPL to 1	

APPENDIX 3 – EXAMPLES OF COST/BENEFIT ANALYSIS

Microsoft Office
Excel Worksheet

CBA examples - justified spend estimates

see http://www.hse.gov.uk/risk/theory/alarpcheck.htm for methodology

see SPC/PERM/37 & 39 for COMAH guidance including selction of disproportion factor
http://www.hse.gov.uk/foi/internalops/hid/spc/permissioning.htm

These examples show how CBA may be applied to inform an ALARP decission (see ALARP guidance above for when this is appropriate). Here the course screening method is used to determin justified spend (inclusive of disproportion factor). Thus if cost exceeds justified spend then the project is likely grossly disproporiotnate. More detailed methods adopting cost discounting approaches are also valid.
N.B. risk figures and costs need to be site specific - those provided here are for illustration

Example 1

3 tanks in bund, with tertiary containment discharge to river

What is the justified spend for removing a gravity drain cf blind pumped sump to reduce MATTE risk?
Assume single outcome CDOIF category C and no other category C scnearios at establishment

From LOPA it is estimated total risk to off-site river, per tank, associated with major loss of primary containment (10-4 per tank yr), flow through gravity drain (0.1 PFD), and loss of tertiary containment (0.1 PFD) =						1.00E-06	per tank year	(so establishment risk without blind sump is 3E-06 per year)
From LOPA it is estimated total risk to off-site river, per tank, associated with loss of primary containment (10-4 per tank yr), flow through oil interlocked pumped sump (0.01 PFD), and loss of tertiary containment (0.1 PFD) =						1.00E-07	per tank year	(so establishment risk with blind sump is 3E-07 per year)
				Tanks in bund =		3		
			At risk low end of TifALARP, disproportion factor DF =			2		
					To normalise, take benefit =	1000000	pounds	
					Life of blind sump, limited due to life of pump / oil sensor etc =	25	years	
Justified spend =	No of tanks	x benefit	x risk gap	x DF	x plant life			
	3	1000000	9.00E-07	2	25	£135.00	per £1M of benefit per bund	

Thus if benefits are £10M (e.g. avoided clean-up & recovery only), total justified spend = £1,350 per bund
Justified spend would likely increase further when risk to persons and property, on and off-site is included.
This would need further risk assessment & CBA to include factors such as ingnition probabilities or time at risk.
Example 4 shows how this can be done.

Example 2

3 tanks in bund, no tertiary containment, drainage to river

What is the justified spend for removing a gravity drain cf blind pumped sump to reduce MATTE risk?
Assume single outcome CDOIF category C and no other category C scnearios at establishment

From LOPA it is estimated total risk to off-site river, per tank, associated with loss of primary containment (10-4 per tank yr), flow through gravity drain (0.1 PFD) =						1.00E-05	per tank year			(so establishment risk without blind sump is 3E-05 per year)
From LOPA it is estimated total risk to off-site river, per tank, associated with loss of primary containment (10-4 per tank yr), flow through oil interlocked pumped sump (0.01 PFD) =						1.00E-06	per tank year			(so establishment risk with blind sump is 3E-06 per year)
Tanks in bund =						3				
At risk mid TifALARP, disproportion factor DF =						5				
To normalise, take benefit =						1000000	pounds			
Life of blind sump, limited due to life of pump / oil sensor etc =						25	years			
Justified spend =	No of tanks	x benefit	x risk gap	x DF	x plant life					
	3	1000000	9.00E-06	5	25	£3,375.00	per £1M of benefit per bund			

Thus if benefits are £10M (e.g. avoided clean-up & recovery only), total justified spend = £33,750 per bund
Justified spend would likely increase further when risk to persons and property included.
This would need further risk assessment & CBA to include factors such as ingnition probabilities or time at risk.
Example 4 shows how this can be done.

Example 3

30 tanks in bunds, with gravity drain, no tertiary containment, drainage to river

What is the justified spend for installing tertiary containment to reduce MATTE risk?
Assume single outcome CDOIF category C and no other category C scnearios at establishment

From LOPA it is estimated total risk to off-site river, per tank, associated with loss of primary containment (10-4 per tank yr), and loss from bund (0.1 PFD) =						1.00E-05	per tank year			(so establishment risk without 3ry cont. is 3E-04 per year)
From LOPA it is estimated total risk to off-site river, per tank, associated with loss of primary containment (10-4 per tank yr), and loss from bund (0.1 PFD) and loss from tertiary containment (0.1PFD) =						1.00E-06	per tank year			(so establishment risk with 3ry cont. is 3E-05 per year)
Tanks =						30				

N.B. At this point it sould be recognised total risk to river from tanks exceeds 1E-04 thus risk is intolerable and improvement measures required almost irrespective of cost. Thus justified spend calcs are illustrative only to show outcome when risk is bordering intolerable

At risk approaching intolerable, disproportion factor DF =						10				
To normalise, take benefit =						1000000	pounds			
Life of tertiary containment =						50	years			
Justified spend =	No of tanks	x benefit	x risk gap	x DF	x plant life					
	30	1000000	9.00E-06	10	50	£135,000.00	per £1M of benefit			

Thus if benefits are £10M (e.g. avoided clean-up & recovery only), total justified spend = £1,350,000
Justified spend would likely increase further when risk to persons and property included.
This would need further risk assessment & CBA to include factors such as ingnition probabilities or time at risk.
Example 4 shows how this can be done.

Example 4 (to illustrate multiple outcomes of different severity)

1 tank in bund with underfloor pathway to groundwater + risk of fuel migration via ground/groundwater to control room resulting in an explosive atmosphere in control room

For credibility of this scenario see case study of Petrol leak at Strath Services (operated for ConocoPhillips), Mayflower Terminal, Plymouth. July 2007" in paper "Bunding at Buncefield: Successes, failures and lessons learned" IChemE Loss Prevention Bulletion 205 pp19-25

What is the justified spend for lining under a tank with a permiable base to reduce risk to persons and the environment?

Assume CDOIF category C outcome for large LoC and CDOIF category A outcome for small LoC (both are MATTE)

Lastfire cites total tank bottom failure rate of 4E-4 per tank year - assume 1/4 of these are large (N.B. this ratio might be reduced further by wet stock reconciliation / leak detection techniques but this will only detect a leak and reduce its severity, rather than reduce overall leak rate)

For illustration in this case a Large LoC might also lead to explosive atmosphere in nearby control room (LOPA gives this risk after considering ignition probability and 5 person occupancy rate as 5E-6 per tank year)

From LOPA it is estimated total risk to groundwater, per tank, associated with large loss of primary containment (10-4 per tank yr) =	1.00E-04	per tank year	(This is borderline intolerable for cat C)
From LOPA it is estimated total risk to groundwater, per tank, associated with large loss of primary containment (10-4 per tank yr) and through a failed liner (0.01 PFD) =	1.00E-06	per tank year	
From LOPA it is estimated total risk to groundwater, per tank, associated with small loss of primary containment (3*10-4 per tank yr) =	3.00E-04	per tank year	(This is low-mid TifALARP for cat A)
From LOPA it is estimated total risk to groundwater, per tank, associated with small loss of primary containment (3*10-4 per tank yr) and through a failed liner (0.01 PFD) =	3.00E-06	per tank year	
From LOPA it is estimated total risk to building and persons in it, per tank, associated with large loss of primary containment =	5.00E-06	per tank year	(This is low-mid TifALARP for individual risk)
From LOPA it is estimated total risk tobuilding and persons in it, per tank, associated with large loss of primary containment (10-4 per tank yr) and through a failed liner (0.01 PFD) =	5.00E-07	per tank year	

At risk approaching intolerable, disproportion factor DF =	10	
At risk low-mid TifALARP, disproportion factor DF =	3	
Benefit (large LoC - from petroplus 2005) =	3000000	pounds
Benefit (small LoC) =	100000	pounds
Benefit 5 persons (£9M) and building (£10M) =	19000000	pounds
Life of tank & liner =	50	years

Justified spend =	benefit	x risk gap	x DF	x plant life		
Large LoC - groundwater	3000000	9.90E-05	10	50	£148,500.00	
Small LoC - groundwater	100000	2.97E-04	3	50	£4,455.00	
Large LoC - building & persons	19000000	4.50E-06	3	50	£12,825.00	
				Total	£165,780.00	per tank

Note the petroplus (2005) incident cost £3M in remediation alone so total benefits for large tanks might significantly exceed those cited in this example, especially if long term loss of abstraction or terminal closure folowing explosion are factors.

APPENDIX 4 – USEFUL GUIDANCE AND REFERENCES

CA guidance relevant to ALARP decisions, to which Agency inspectors should refer, include:

"ALARP – As low as reasonably practicable" http://www.hse.gov.uk/comah/alarp.htm

"Guidance on ALARP decisions in COMAH" (Health and Safety Executive SPC/perm/37)
http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37

"HID's approach to ALARP decisions (Health and Safety Executive SPC/perm/39)
http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_39.htm

- "Guidance for environmental aspects of COMAH Safety Reports" (Competent Authority SRAM section 13)
- "Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports" (COMAH CA, Dec 1999)
- "A Guide to the COMAH Regulations 1999", L111 HSE 2006.
- DETR 1999 "Guidance on the Interpretation of Major Accident to the Environment for the purposes of the COMAH regulations"

For EC Major Accident information see Minerva - https://minerva.jrc.ec.europa.eu/en/minerva and also the databases http://enatech.jrc.ec.europa.eu/Home and https://emars.jrc.ec.europa.eu/

References to Appendix 1

[1] Lastfire June 1997 – N.B this is for large tanks >40m diameter
[2] HSE Failure Rate and Event Data for Land Use Planning Risk Assessments (notes not originally intended for COMAH but can be used as starting point for COMAH in absence of site specific data) http://www.hse.gov.uk/landuseplanning/failure-rates.pdf
[3] "Bund effectiveness in preventing escalation of tanks farm fires", Davies, Harding, MaKay, Robinson and Wilkinson, IChemE symposium series No 139. Also published as Process safety and environmental protection, Trans IChemE vol. 74, n°2, pp. 88-93, 1996
[4] "SAFETY REPORT ASSESSMENT GUIDE: HFLs", HID, 09 July 2001
[5] CPR-18E "Guidelines for QRA – Purple book" Committee for the Prevention of Disasters First edition 1999
[6] Thyer et al "A review of catastrophic failures of bulk liquid storage tanks" IChemE LPB 205 Feb09
[7] ARAMIS - ACCIDENTAL RISK ASSESSMENT METHODOLOGY FOR INDUSTRIES IN THE CONTEXT OF THE SEVESO II DIRECTIVE – User guide
[8] Bund survey reveals many bunds in poor state – http://www.enviro-solutions.com/features/bund-survey.htm
[9] " SAFETY REPORT ASSESSMENT GUIDE: HFLs", HID, 09 July 2001
[10] Bugler et al "Guidance on the bunding of bulk chemical storage vessels" HSE Specialist Inspector Report 39
[11] " SAFETY REPORT ASSESSMENT GUIDE: Chemical warehouses", HID, v6 26 June 2002
[12] http://www.business-sprinkler-alliance.org/about-sprinklers/quick-facts/
[xiii] http://ec.europa.eu/environment/seveso/index.htm
[xiv] http://web.bryant.edu/~aboggio/boggio_seveso.pdf
[xv] I Vince "Major Accidents to the Environment" Elsevier 2008
[xvi] Fire and Rescue Manual – Vol2 Fire service operations Environmental Protection, The Stationary Office (2008).
[xvii] CIRIA 164 Design of containment systems for the prevention of water pollution from industrial incidents (1997) [note: R164 was replaced in 2014 by CIRIA C736]
[xviii] ITOPF http://www.itopf.com/spill-compensation/cost-of-spills/ & http://www.itopf.com/information-services/data-and-statistics/case-histories/index.aspx
[xix] Mapping the impacts of natural hazards and technological accidents in Europe An overview of the last decade, EEA Technical Report 13 (2010)
[xx] eMARS https://emars.jrc.ec.europa.eu/
[xxi] Whitfield & Nicholas "Bunding at Buncefield: Successes, failures and lessons learned" Loss Prevention Bulletin 205, IChemE Feb 2009
[xxii] http://www.hse.gov.uk/comah/buncefield/response.htm and http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf
[xxiii] https://archive.epa.gov/katrina/web/html/index-6.html
[xxiv] http://www.corpwatch.org/article.php?id=14029
[xxv] Atherton & Ash, REVIEW OF FAILURES, CAUSES & CONSEQUENCES IN THE BULK STORAGE INDUSTRY Liverpool John Moores University (downloaded from http://lightningsafety.com/nlsi_lls/Causes-of-Failures-in-Bulk-Storage.pdf)