

Environmental Risk Gap Analysis: Major Accident to the Environment Case Studies

Mike Nicholas, Senior Advisor (COMAH), Environment Agency, Goldcrest House, Alice Holt Lodge, Farnham, Surrey GU10 4LH. email: mike.nicholas@environment-agency.gov.uk

This paper combines two techniques, historic accident review (hindsight) and risk assessment (foresight), to explore the theoretical level of environmental risk posed by establishments that have previously had Major Accidents. It draws on accident reports, published event and failure rate data and the presence and condition of protective measures at the time of the incident to assess potential environmental consequences and determine the theoretical level of environmental risk at the time of the incident. It then explores how much risk reduction could have been delivered by adoption of measures such as those reported in investigation recommendations or subsequently revised good practice and the residual risk that the establishment would have posed had these measures been in place.

The paper reviews the legal requirements for accident review and environmental risk assessment, under the COMAH 2015 regulations (Seveso III directive), along with updates to relevant international standards, environmental protection good practice and the environmental risk tolerability guidelines for Great Britain (GB). This framework for risk assessment and control is illustrated using Major Accident to the Environment (MATTE) case studies that have been selected to illustrate a range of issues relevant to environmental protection.

The paper draws conclusions on the efficacy of current approaches and draws out good practice for environmental risk assessment and environmental protection.

Keywords Environmental Risk Tolerability, COMAH, Major Accident to the Environment, MATTE

Background

Legal drivers for Environmental Protection (within a safety framework)

Major Accidents at industrial establishments have caused serious harm to the environment on several occasions. This has usually been as a result of loss of containment of hazardous liquids (as opposed to the relatively few gaseous release scenarios) and particularly firewater runoff. In Great Britain (GB), for sites regulated under the Control of Major Accident Hazard (COMAH) regulations, the term used to describe a scenario which causes serious harm to the environment is a Major Accident to the Environment (MATTE). A Major Accident which poses serious danger to the environment is a potential MATTE (SEPA, 2016b).

Over the past two decades European safety legislation has been updated to increase the emphasis on protection of the environment, alongside protection of people. With societal concern around MATTEs growing, the Sandoz Warehouse fire in particular had a profound effect in shaping legislation. One important finding from the incident was, at that time "There was weak legislation in place for preventing catastrophic releases of dangerous substances" including inadequacies around incident alert communications, resulting in delayed closure of downstream water intakes (EC, 2013). As a direct result, the Seveso Directive was amended in the 1990s to strengthen the mechanism for protection of the environment, fully incorporating prevention and mitigation of environmental harm into the existing framework for safety of people.

One of the benefits of inclusion of MATTEs into the European framework for Major Accident control has been that MATTEs are investigated to the same depth as those causing harm to people, in so far as identification of causes and root causes, preventive or mitigatory measures and recommendations for future prevention. A further benefit is the improved availability of case study material for accidents resulting in serious environmental harm. This stems from the duties on COMAH operators and Member States within the Seveso Directives, resulting in reporting of the more significant Major Accidents at a European Level. Several authors have tapped into the information available on eMARS (EC, 2017), either directly or by using the database to signpost other accident information. For example the European Commission's Major Accident Hazards Bureau, which has used eMARS data to compile several Lessons Learned Bulletins, including Bulletin No.3 "Major Accidents having significant impact to the environment" (EC, 2013).

Specific requirements of COMAH relating to risk assessment include the necessary content of safety management systems (SMS).

Schedule 2 of COMAH (2015) requires the SMS to include:

> "2. The following matters must be addressed by the safety management system—
>
> ...
>
> (b) the identification and evaluation of major hazards: the adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation, including subcontracted activities where applicable, and the assessment of their likelihood and severity;"

Thus all COMAH operators need to establish a procedure within their SMS that will ensure potential MATTEs are identified (alongside other Major Accident Hazards) and an assessment of MATTE likelihood and severity. Schedule 3 of COMAH (2015), applicable to Upper Tier establishments, provides more detail on the expected outputs from the risk analysis process with Schedule 3 (5) describing the data and information to be included in a safety report. This detail remains largely unchanged from COMAH (1999), however significant additions now explicitly require operators to think about accident

causes outside the fence – both "external causes" and "natural causes" – and to review lessons from past accidents and incidents and make "explicit reference to specific measures taken to prevent such accidents". Review of lessons has always been considered a good practice requirement and the Directive itself has evolved on the basis of such lessons. However it is not uncommon to have found that lesson learning has been limited to incidents at the establishment or other establishments of the operator, or the few catastrophic incidents such as Buncefield which stimulate a national paradigm shift in regulatory approach across the regime/sector. COMAH 2015 now explicitly makes the link between lessons from the past and risk analysis for control of Major Accidents of the future and the need to reflectively consider relevant accidents that have occurred at any establishment in Great Britain and internationally (HSE, 2015).

Environment within safety – the International Standards perspective

In addition to the specific risk assessment requirements of COMAH discussed above, Regulation 5 requires "Every operator must take all measures necessary to prevent major accidents and to limit their consequences for human health and the environment." Guidance produced by HSE (2015) indicates that here, compliance is achieved by following the hierarchy for safety. Once inherently safe approaches have been adopted and hazards reduced then remaining risks need to be reduced to a level As Low As Reasonably Practicable (ALARP). Fundamental to this is the expectation that good practice should be adopted as a minimum.

Good practice for risk assessment should include relevant national and international standards. The Author has recently observed that, with regard to inclusion of environmental risks, safety standards have not been developing at the same rate as legislation. Environmental risk assessment was integrated into the regulatory framework during the 1990s, by the Seveso Directive, but international standards are still "catching up".

Specifically, consider functional safety. In the context of BS EN 61508/61511, safety is freedom from unacceptable risk and risk is a function of the frequency/probability of occurrence of harm and the severity of that harm. The scope of the standards highlight they are concerned with safety related systems whose failure could have an impact on the safety of persons and/or the environment. Thus environmental protection should be integral to functional safety. However, the COMAH Competent Authority (CA) has observed that specific environmental based Safety Integrity Level (SIL) determinations are rarely made in practice (this deduced by communications with COMAH officers and HSE Specialist Inspectors). The author is of the opinion that this, until now, has been due to the definition of Harm within the standards.

BS EN 61511_1: 2004 defined harm as follows.

- Harm is "physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment".

Here, harm is related to injury or damage to people and damage to the environment is only of concern if it subsequently causes harm to people (the environment is a vector for hazardous properties indirectly harming people, rather than a receptor on its own). Contrast this with the more recent definition of harm within BS EN 61508 (from 2010) and from this year 61511.

BS EN 61508_4: 2010 (and IEC 61511:2016) define harm differently.

- Harm is "physical injury or damage to the health of people or damage to property or the environment".

Thus harm is not limited to injury or damage to people, but also separately includes damage to property or the environment. SIL determinations based on environmental risk alone should become more common.

For COMAH operators this change should not cause significant issues, since the regulations made the "environment within safety" transition over a decade ago. Operators may however need to review their internal procedures for SIL determination and environmental risk targets in particular, to ensure they are aligned to the COMAH risk assessment procedures and inclusive of the environment. For those sectors outside of COMAH this change will likely be more significant as environmental risk becomes increasingly integrated within functional safety and considered as good practice or a "Best Available Technique". Since the change in definition of harm is aligned to the definition within Guide 51 (ISO/IEC, 2014) which sets out the overarching guidelines for inclusion of safety aspects within standards, integration of environmental protection in its own right within safety is a transition that should become apparent across all safety standards.

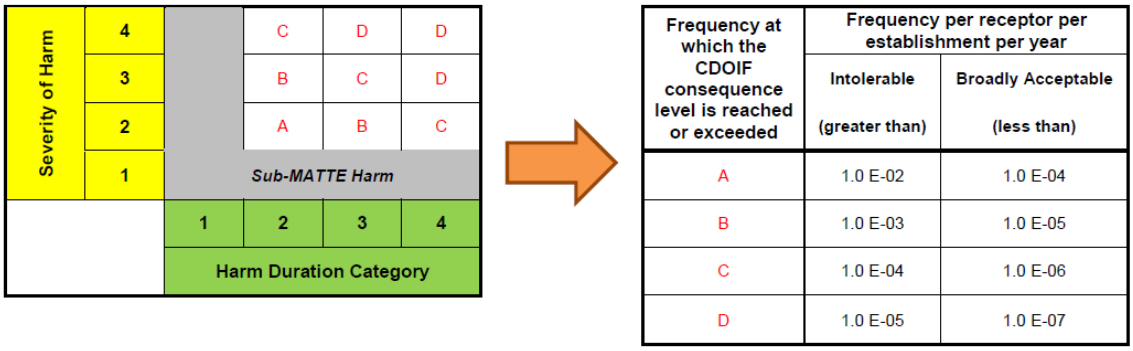
The environmental risk problem – How safe is safe enough (if you're a fish)?

Both Operators and Regulators need to understand and agree the thresholds for environmental tolerability to manage environmental harm within the ALARP framework for safety. Whilst there had been work to address this from the late 1990s onwards, consensus on environmental risk tolerability in GB had not been reached by 2010. Following Buncefield and other Major Accidents that occurred between 2005 and 2010 regulators and industry agreed there was a need to build consensus on environmental tolerability for COMAH establishments. Nicholas et al (2014) outline the work in this area in more detail and explain that in 2010 the Chemical and Downstream Oil Industry Forum (CDOIF) established a working group to address this gap. In 2013 a guideline on "Environmental Risk Tolerability for COMAH Establishments" (HSE, 2013a) was published.

The CDOIF guideline provides guidance on how to approach environmental risk assessment, but the most important aspect is that it establishes risk tolerability criteria for different levels of environmental consequence. Through considering the severity and duration of harm to differing receptor types and classifying each using the guideline's 1-4 scaling system it is possible to qualify "Unmitigated consequences" as sub-MATTE or MATTE A-D. CDOIF then worked to agree frequencies

on a "per receptor per establishment per year" basis for each level of consequence to set the Intolerable and Broadly Acceptable boundaries of the recognised ALARP framework. These are presented in Figure 1 below.

Figure 1. Extract from CDOIF guideline, Appendix 4 : Table 3, Matrix for deriving receptor tolerability for MATTE (HSE, 2013a).



Frequency at which the CDOIF consequence level is reached or exceeded	Frequency per receptor per establishment per year	
	Intolerable (greater than)	Broadly Acceptable (less than)
A	1.0 E-02	1.0 E-04
B	1.0 E-03	1.0 E-05
C	1.0 E-04	1.0 E-06
D	1.0 E-05	1.0 E-07

The guideline does not resolve all issues. For example, whilst it provides a framework within the established source-pathway-receptor model, it does not discuss the detail of different techniques for qualifying / quantifying environmental harm. Also, whilst it provides direction on how to approach an evaluation of costs and benefits within a COMAH Cost Benefit Analysis (CBA) it does not indicate where a user can source environmental valuation material. In fact both environmental modelling and environmental valuation / economics are fields in their own right and CDOIF recognised that the guideline would never provide full answers to all the challenges faced. Work continues to be carried out to clarify some knowledge gaps, such as work soon to be published by the Energy Institute on consideration of duration of environmental harm (EI, 2016) and no doubt further work will continue as operators continue to discuss environmental risk assessments. However in its first years of use, the guideline has proved invaluable in establishing a common approach for operators and the regulator to explore the tolerability of environmental risk. In many cases, discussions on "All Measures Necessary" have been resolved through understanding environmental risk, within the ALARP framework, and then adopting ALARP principles. After all, the ALARP framework was developed as a tool designed to be useable in the context of the uncertainties surrounding evaluation of risks to people. To date, most users agree that the frequency thresholds established feel "about right". This is hugely encouraging and stems from the fact that they have been borne through expert discussions amongst a variety of stakeholders, not simply about how much the metaphorical fish is worth (pounds and pence), but by thinking about safety from a holistic viewpoint. The "value of life" for a specific fish species might come into the equations at some point – and there are values the Environment Agency can provide for this if necessary. However, tolerability of risk is wider and the thresholds have been set in the context of matters such as public perception associated with killing the fish, shareholder confidence, total incident costs etc. These are all notoriously difficult to quantify precisely, but when taken together it has been possible for industry and regulators to agree the tolerability of MATTEs. For a discipline founded on societal constructs of values and expert judgement, the worth of that degree of consensus should not be underestimated!

Embedding the CDOIF approach within "All Measures Necessary" decisions

Following publication, the CDOIF environmental tolerability guideline remained open for comment. It was recognised that whilst the method was a significant step forward to building consensus on MATTE tolerability, there would inevitably be questions arising from initial use. CDOIF reconvened during 2015 to discuss the issues raised by operators and the regulator during initial use and revise the guideline where necessary. Encouragingly the majority of the methodology and the tolerability thresholds themselves were not considered to need revision.

The most fundamental change in guidance concerns handling of groundwater. Here there was considerable attention paid to the guidance on qualifying MATTE to differing types of groundwater and the "harm duration" categorisation. New duration periods were agreed so that the approach for groundwater now aligns better with other receptors. i.e. there is a minimum threshold where, if natural recovery of groundwater occurs more rapidly than stated, the harm should be considered sub-MATTE. Moreover, there is specific differentiation between shorter and longer term harm durations to groundwater.

Version 2 of the CDOIF guideline was published in the spring of 2016 (SEPA, 2016a).

The early use of the guideline, and the fact that, whilst there were modifications between version 1 and 2, the overall approach had been accepted, enabled the COMAH CA to formally endorse it as established good practice for assessing MATTEs. In 2016, new guidance to CA inspectors and officers was published by the COMAH CA (SEPA, 2016b). This built on earlier guidance prepared by the Environment Agency, to discuss the range of issues involved with environmental decision making within the ALARP framework. The guidance also introduced new aspects, such as discussion of typical Probability of Failure on Demand (PFD) data for typical environmental protection layers. This data will be used within the case studies.

Case Studies

The case studies in this paper are case studies 1, 3 and 5 as presented in the Environment Agency special edition of IChemE Loss Prevention Bulletin - LPB (IChemE, 2015). These are used due to availability of detailed incident descriptions for each scenario with the benefit that they were originally chosen to be representative of a range of establishment types, impacts and causes relevant to environmental protection. Thus a variety of issues can be explored. A brief summary of each incident is provided in this paper, but to fully understand each incident readers should refer to the full detail in LPB (IChemE, 2015).

Whilst the case studies are drawn from actual incidents, in order to preserve confidentiality with regards sensitive information, the ERA examples here are completed using industry typical failure/event data and a presumed establishment scale (e.g. assumed number of major accident hazard sources within the establishment). These values are typical of those the Author has observed in use at COMAH establishments, but they do not reflect any site specific factors based on arrangements and measures in place at the establishments, other than the information provided in the case studies themselves.

Methodology

For each case study a Layer of Protection Analysis (LOPA) approach is taken to examine in turn:

- Initiating event frequency (IE). For the purpose of this paper, this is inclusive of preventive measures in place at the time of the incident, which are assumed to be typical so that industry average event data can be used.
- Mitigatory measures in place at the time of the incident, including industry typical Probability of Failure on Demand (PFD). These layers are numbered Mx, such that M1 would be the first mitigatory layer, M2 the second etc. In some cases mitigation was partially successful at reducing, but not fully avoiding environmental harm.
- Further Risk Reduction (FRR – FRR1, FRR2 etc) measures. These are measures not in place at the establishment at the time of the incident, but which could have been implemented to reduce risk. They are generally those measures labelled as “lessons learned” within case studies, and are often measures described in present day good practice (though they may not have been considered established good practice at the time of the incident).

The consequences of each incident are qualified in terms of extent, severity and duration in line with the CDOIF Environmental Tolerability of Risk methodology. Where there were more than one Source – Pathway – Receptor linkage, leading to multiple different receptors being harmed, the receptor with the highest consequence has been selected, since this will be the driver for risk tolerability criteria. In practice, for a predictive (pre-incident) analysis, all receptors need to be reviewed to ensure necessary measures are in place so that risk is tolerable for each receptor. In some cases protection layers result in a trade-off of risk between receptors (e.g. controlled burn decisions require comparison of aerial vs terrestrial pathways which can change the relative risk to differing receptors – smoke plume vs firewater run-off).

A fundamental aspect of the CDOIF approach is that risk tolerability criteria are based on unmitigated consequences - i.e. the worst credible consequence associated with the inventory (with no protection layers in place). Herein lies a challenge when analysing historic events. It is not typical in GB that an incident will occur with no mitigation, since even if the operator is not in a position to respond quickly there are well established external emergency procedures whereby designated responders such as the fire and rescue service or the environment agencies will respond to reduce impacts where practicable. Thus the observed consequences of a typical incident are often lower than the worst credible consequence. The Author has thus used professional judgement to estimate credible unmitigated consequence. This is guided by a rule of thumb that unmitigated consequence will be at least one category greater than the observed consequence. This theoretical unmitigated consequence has been considered in line with typical consequences being discussed at current COMAH establishments to validate that assumption. For an assessment under the COMAH regulations the CA would also expect unmitigated consequences to be evaluated through an appropriate model and reference to other comparable historic incidents, with depth of assessment being proportionate to risk.

Environmental tolerability criteria are derived from the theoretical unmitigated consequence, as guided by CDOIF (SEPA, 2016a). Analysis of the risk reduction measures relevant to the establishment are then discussed by comparing the establishment risk criteria (or a modified threshold in cases where the Major Accident Hazard scenario is a fraction of the total risk from the establishment) to the frequency of the mitigated consequence, considered from three perspectives:

1. The Apparent risk (A), derived from initiating event frequency and PFD of existing layers of protection that were claimed to be in place at the time of the incident, for given MATTE consequence levels.
2. The Incident risk (I), derived from the initiating event frequency and considering only mitigatory layers which were successful at reducing consequence. This discounts credit claimed for any protection layers which appeared to be in place, but which actually failed (risk I is greater than risk A).
3. The Possible risk (P), derived from the initiating event frequency and existing layers of protection in place at the time of the incident and then considering FRR measures that could have been implemented.

The reason for taking this approach is to highlight the risk gaps between the Apparent risk, the Incident risk and the Possible risk and thus highlight the criticality of the layers of protection involved in delivering risk reduction or those that could deliver further risk reduction if adopted.

Case Study 1

The incident involved Loss of Containment of approximately 16 tonnes of sodium cyanide from a >750 tonne tank, into a bund and then via drains and an effluent treatment plant to a river estuary. Whilst the incident did cause some environmental harm, the incident did not result in serious harm (a MATTE), due to successful mitigatory emergency response limiting the amount lost from the tank. It is considered though that had this mitigatory action not been successful a MATTE could have occurred. The LOPA data representing the incident is shown in table 1 and discussed below.

Table 1 – Summary of LOPA data (case study 1)

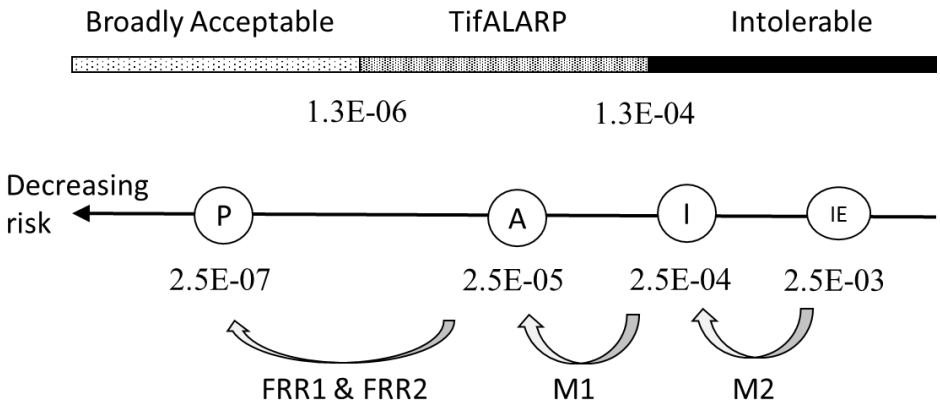
Initiating Event Frequency (IE)		**2.5E-03**	**per tank year (minor leak)**
Ref.	**Descriptor**	**PFD**	**Comment**
M1	Bund	0.1	Gravity drained chemical bund with valve
M2	Emergency response	0.1	Reduction from MATTE A to sub-MATTE
FRR1	Leak detection	0.1	In tank / in bund detection & alarm
FRR2	Enhanced containment systems	0.1	Closed drainage system (tertiary containment)
A	Apparent risk of MATTE	2.5E-05	per year = IE x M1 x M2
I	Incident risk of MATTE	2.5E-04	per year = IE x M2 (i.e. M1 failed to contain)
P	Possible risk of MATTE	2.5E-07	per year = IE x M1 x M2 x FRR1 x FRR2

The release rate is considered to be typical for a minor release (small hole size) and an IE frequency of $2.5x10^{-3}$ is used (HSE, 2012). The PFD of protection layers are derived by consideration of guidance in Table 4-1 and supporting notes of the CA AMN guidance (SEPA, 2016b), with the exception of leak detection PFD which is guided by the CDOIF leak detection guideline (HSE, 2013b). From the incident description it is considered no further preventive measures existed (e.g. benefit of tank inspection regimes is included in the IE frequency) and two mitigatory measures existed (the bund and overall emergency response). During the incident only the emergency response was effective in avoiding a MATTE (the bund failed to contain). Further risk reduction, not in place at the time of the incident, could have been achieved through a leak detection system or improving the containment systems (e.g. ensuring a closed drainage system as tertiary containment).

In order to judge the tolerability of these frequencies it is necessary to compare them with environmental tolerability criteria. In this case the leak was discovered and mitigation implemented such that volume released was limited and a MATTE did not occur (but note, this is not the same as harm being totally avoided). It will be assumed that, had mitigation failed a MATTE A could have resulted in terms of impact to the river estuary. The TifALARP range for MATTE A at the establishment is 10^{-2}>TifALARP>10^{-4}. These thresholds are applicable to all MATTE events throughout the establishment and it is thus necessary to modify them when looking at this specific scenario. It will be assumed that other loss of containment mechanisms from the tank (e.g. overfill) could cause the frequency of tank releases capable of MATTE A to double (in practice a specific fault tree could verify this). The author does not have information concerning overall establishment risk (nature of operations and other loss of containment scenarios at the time of the incident), so for the purposes if this case study it will be assumed that this was a typical bulk storage site such that the tank that leaked was one of 20 similar tanks posing a MATTE A risk and other loss of primary containment events (LoC from pipework, loading facilities etc.) account for a release frequency equivalent to the frequency of release from tanks. From these assumptions it is estimated the total release frequency from the establishment that could cause a MATTE A could have been about $2x10^{-1}$ (i.e. $2.5x10^{-3}$x2x20x2). Considering it another way, the minor leak frequency from a single tank (this scenario) contributes approximately $1/80^{th}$ of the total establishment risk from all scenarios. So for the scenario being considered MATTE A tolerability can be calibrated to 1.3^{-4}>TifALARP>1.3^{-6} per scenario per year (dividing the establishment risk targets by 80).

The LOPA data from Table 1 can now be compared with the scenario MATTE A tolerability criteria and this is depicted in Figure 2. In Figure 2, frequency (per year) and thus MATTE A risk decreases from right to left.

Figure 2 – Case study 1 frequencies vs MATTE A scenario tolerability (1/80th establishment tolerability)



From Figure 2 it can be seen that, with regard to risk of a MATTE A occurring from this scenario:

- The Initiating Event frequency (IE), concerning a minor tank leak, posed an intolerable risk if unmitigated.
- The Incident risk (I) (tank leak and emergency response mitigation) also posed an intolerable risk, in spite of the outcome in this case where a MATTE was avoided. Arguably, (I) represents the operational risk immediately prior to the incident. The bund valve was not correctly seating and leaked, therefore reliance was solely on emergency response. How many operators, if they had a similar arrangement, tested their bund valve and found it passing liquids, would then re-appraise the risk and deem it too high and thus immediately implement other risk reduction measures to compensate or cease operations within the bund until the valve had been fixed? (Especially knowing that the emergency response would reduce consequence to sub-MATTE, but not avoid a pollution incident).
- The Apparent risk (A) is the risk if all protection layers installed (tank, bund and emergency response) were operating as expected. This is the risk most usually demonstrated by operators within risk assessments and in this case it posed a risk in the TifALARP range. Thus even if the bund valve had been working as intended the risk remained such that the operator should have been questioning what further measures could be adopted, so far as is reasonably practicable. It might be time to replace the bund valve with a blind pumped sump? (Human reliability implications increase the PFD for a manually operated gravity drained bund – there are plenty of accident reports which include, "the bund valve was left open"). Or adopt further risk reduction measures?
- The Possible risk (P) is the risk that could be achieved if all available layers of protection, plus FRR measures are adopted. In this case it can be seen that a further two orders of magnitude risk reduction would reduce risk to be broadly acceptable. This degree of risk reduction could be achieved by implementing independent leak detection to increase likelihood of a swift emergency response (i.e. reducing PFD of emergency response) combined with installing tertiary containment. Risks in the broadly acceptable do not require a detailed ALARP demonstration and as long as the protection layers in place are maintained in good operating condition then it is not expected that further risk reduction should be necessary. The specific improvements necessary are subject to ALARP principles, including the test for gross disproportion (costs vs benefits) as outlined in SEPA (2016b).

Case study 3

This incident was very similar to that in case study 1. It involved a minor leak from a kerosene storage tank. However, in this case the leak was from the tank bottom, the tank foundations were permeable and the leak migrated downwards contaminating the underlying aquifer. Because the base was permeable the leak was not visible in the bund and the leak went undetected for many weeks - approximately 650 tonnes of kerosene was released. The incident caused over 1 ha of groundwater to be contaminated (but less than 100ha due to the groundwater being bounded by a stream and the estuary) and recovery with remediation fell between 3 months and 6 years. In terms of CDOIF consequence, the tables in Appendix 4 (SEPA, 2016a) indicate the receptor "Groundwater - Non drinking water source" had been harmed at severity level 2 and duration 2, which is a MATTE A. It will be assumed that without remediation, natural recovery of the groundwater would have been longer and thus unmitigated consequence could have been a MATTE B.

The LOPA data is presented in table 2. The Initiating Event Frequency (IE) is taken as $4x10^{-4}$ per year (Lastfire data cited by SEPA, 2016b). Here a tank bottom leakage rate is specifically chosen, as opposed to a more general minor tank leakage rate, because this failure mode initiated a pathway less readily detectable than leakage from elsewhere in the tank shell, where minor leaks might be noticed in the bund. Whilst it may have been assumed that inventory monitoring could have alerted to a tank leakage (a PFD of 0.1 might have been claimed), this incident has shown that minor leaks from a large tank are difficult to detect without systems specifically set up to monitor stock loss over time. No other mitigation was in place, except post incident remediation. In this case the remediation was successful, but only to the extent that it reduced consequence from potential MATTE B to a MATTE A outcome. It will be presumed that the PFD for remediation is 0.2

(i.e. a one in five chance of being unsuccessful in reducing consequence from MATTE B to MATTE A). FRR measures that could have been implemented include leak detection (tank gauging based wet-stock reconciliation) or retrofitting an impermeable tank base (with tell tales and leak detection). Internal tank lining techniques and improving the risk based inspection regime are also commonly considered options.

Table 2 – Summary of LOPA data (case study 3)

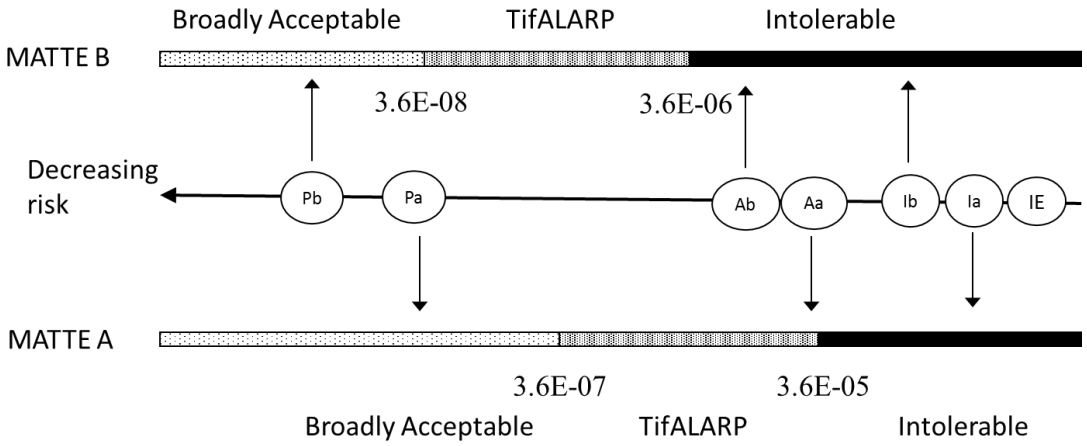
Initiating Event Frequency (IE)		**4.0E-04**	**per tank year (bottom leak)**
Ref.	**Descriptor**	**PFD**	**Comment**
M1	Inventory monitoring	0.1	Detection of minor leak over weeks
M2	Emergency response	0.2	Reduction of MATTE B to A
FRR1	Leak detection	0.1	In tank / in bund
FRR2	Enhanced containment systems	0.1	Under tank lining (secondary containment)
FRR3	Enhanced tank inspections / upgrades	0.1	Tank lining & more frequent / better qualified inspection under risk based inspection regime
Ab	Apparent risk (MATTE B)	8.0E-06	per year = IE x M1 x M2
Aa	Apparent risk (MATTE A)	3.2E-05	per year = IE x M1 x (1-M2)
Ib	Incident risk (MATTE B)	8.0E-05	per year = IE x M2 (i.e. M1 failed)
Ia	Incident risk (MATTE A)	3.2E-04	per year = IE x (1-M2) (i.e. M1 failed)
Pb	Possible risk (MATTE B)	8.0E-09	per year = IE x M1 x M2 x FRR1 x FRR2
Pa	Possible risk (MATTE A)	3.2E-08	per year = IE x M1 x (1-M2) x FRR1 x FRR2

The tank bottom leak frequency is approximately 1/7th of all tank failure modes (from analysis of Lastfire data). To enable ease of comparison with case study 1 it will be assumed that the scale of operations at both case study 1 and 3 establishments were similar (20 tanks and similar scale of pipework, loading/unloading facilities etc.). Thus the tank bottom scenario is (1/(7x20x2)) 1/280th of total establishment risk. Scenario tolerability criteria are thus:

MATTE A - $3.6x10^{-05}$>TifALARP>$3.6x10^{-05}$ and MATTE B - $3.6x10^{-06}$>TifALARP>$3.6x10^{-08}$.

Figure 2 then allows comparison of this data with the scenario tolerability criteria. Because in this case the remediation does not avoid a MATTE (it reduces consequence from MATTE B to MATTE A) it is necessary to use a modified LOPA approach (a LOPA - event tree hybrid). In figure 3 the upper tolerability criteria are for a MATTE B outcome (remediation fails) and the lower for a MATTE A outcome (remediation succeeds).

Figure 3 – Case study 3 frequencies vs MATTE A&B scenario tolerability (1/280th establishment tolerability)



From this analysis, the tolerability (or rather intolerability) of the situation can clearly be seen. The absence of under tank secondary containment led to delayed alert to tank leakage and this, combined with a more sensitive receptor, results in a greater environmental risk than for case study 1. The IE Frequency, Incident MATTE A and B risk (ie MATTE A&B frequencies discounting credit for the failed inventory management) and Apparent MATTE B frequency (i.e. the frequency claiming credit for all protection layers that should have been effective) are all intolerable. Only the Apparent MATTE A

frequency is borderline TifALARP. Thus, if the CDOIF method had been available and carried out prior to the incident, the conclusion should have been that further risk reduction was needed. The FRR measures examined here, selected from published good practice, could have reduced risk by several orders of magnitude so that risk could have been broadly acceptable had they been in place. The decision on measures necessary are subject to ALARP principles (SEPA, 2016b).

Case Study 5

Whilst the previous two case studies involved stock tanks, this case study involves another common MATTE scenario - factory & warehouse fire. Operations at the establishment involved packaging and storing swimming pool and water treatment chemicals. A fire started in an unattended screw conveyer and though the alarm was raised the fire escalated whilst the fire and rescue service were planning how to tackle the fire. The containment systems of the factory were inadequate and speed of escalation meant insufficient time for mobile containment to be implemented. Chemicals were released to the nearby drains (previously unknown pathways) and into a river causing serious harm over a 6km stretch with recovery estimated at 4-7 years. In terms of CDOIF consequence Appendix 4 (SEPA, 2016a) indicates the receptor "Fresh and Estuarine Water Habitats" had been harmed at severity level 2 and duration 2, which is a MATTE A. In this case the emergency responders were able to contain some liquids and it will be assumed that without this mitigation the consequence could have been worse - a MATTE B.

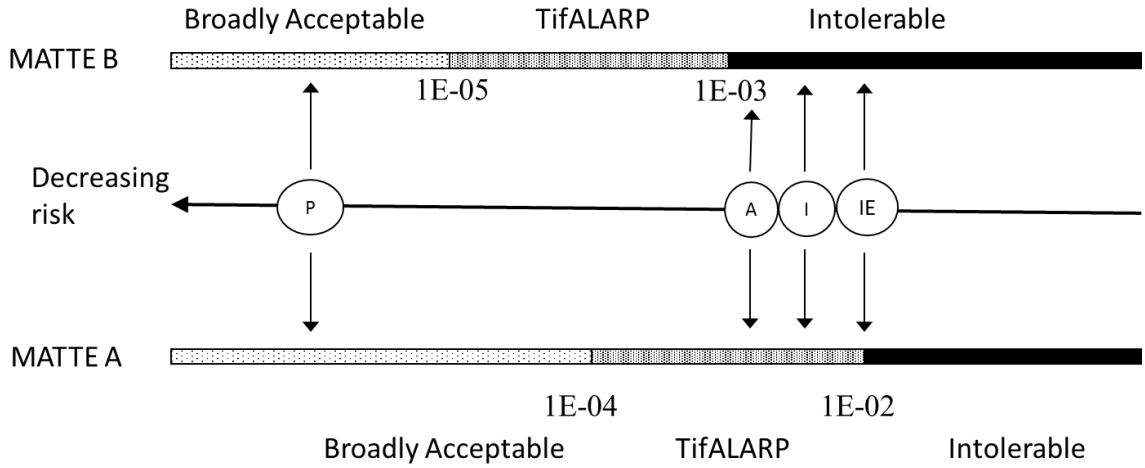
The fire initiation rate is taken as $1x10^{-2}$ per year. Some credit can be claimed for initial emergency response, and it is not uncommon for an order of magnitude risk reduction (0.1 PFD) to be claimed. However, since in this case there was a reliance on detection of fires by staff (who left equipment unattended) and then fire and rescue service intervention it is felt that the PFD for these arrangements is relatively thigh (0.5 say). The remaining mitigation involving emergency containment reducing impact from potential MATTE B to actual MATTE A. It will be assumed these emergency arrangements have PFD of 0.5. The LOPA data for this scenario is presented in table 3. This table also includes Further Risk Reduction measures possible at this site including better segregation (e.g. a fire wall between the packaging and storage areas), automatic sprinklers, secondary containment and better knowledge of off-site drains enabling focused off-site mitigation (drain blocking).

Table 3 – Summary of LOPA data (case study 5)

Initiating Event Frequency (IE)		**1.0E-02**	**per year (Fire initiation)**
Ref.	**Descriptor**	**PFD**	**Comment**
M1	Initial emergency response	0.5	Detection of minor fires & extinguishment
M2	On/Off-site mitigation & remediation	0.5	Reduction of MATTE B to A
FRR1	Sprinkler system	0.03	Early extinguishment prior to escalation
FRR2	Enhanced containment systems	0.1	Warehouse containment system (secondary)
FRR3	Improved supervision of equipment and segregation (fire wall)	0.2	Increased likelihood of early fire detection and early extinguishment prior to escalation
Ab	Apparent risk (MATTE B)	2.5E-03	per year = IE x M1 x M2
Aa	Apparent risk (MATTE A)	2.5E-03	per year = IE x M1 x (1-M2)
Ib	Incident risk (MATTE B)	5.0E-03	per year = IE x M2
Ia	Incident risk (MATTE A)	5.0E-03	per year = IE x (1-M2)
Pb	Possible risk (MATTE B)	1.5E-06	per year = IE x M1 x M2 x FRR1 x FRR2
Pa	Possible risk (MATTE A)	1.5E-06	per year = IE x M1 x (1-M2) x FRR1 x FRR2

It will be assumed that, in this example, MATTEs are only credible for the scenario of full factory fire (smaller spills / leaks are sub-MATTE). Since the whole establishment was involved in the fire then the establishment risk thresholds as presented in CDOIF can be compared directly with the data in table 3, without calibration. This is presented in figure 4.

Figure 4 – Case study 5 frequencies vs MATTE A&B tolerability (whole establishment)



This case study illustrates the importance of considering the tolerability of all possible outcomes. Whilst the actual outcome of the incident was a MATTE A (and this can be assessed to pose a TifALARP risk) it should not be overlooked that the consequence was reduced by the actions of emergency responders. There is a possibility that these actions could have failed to avoid a MATTE B (50/50 chance in this example) and when MATTE B frequency is considered the risk is intolerable.

As with previous examples, the gap between the Apparent Frequency of MATTE (existing control measures) and Possible MATTE frequency (with FRR measures) is several orders of magnitude. Thus risk reduction should have been implemented, subject to ALARP principles, and if good practice and commonly available measures were implemented then risks could have been controlled to be Broadly Acceptable.

Discussion

It has been discussed that safety legislation and standards have developed such that environmental protection is now integral to all safety considerations. This is certainly the case for establishments under the COMAH regulations, but with changes in definition of harm to explicitly incorporate the environment as a receptor, all sites that follow international safety standards will need to address safety to the environment. This poses particular challenges for standards such as those dealing with functional safety (61508/61511) where a degree of qualification / quantification of risk is necessary, combined with judgement on tolerability of risk, in order to determine the amount of required risk reduction.

For COMAH establishments this issue was recognised after Buncefield and work has been carried out to establish agreed tolerability criteria for differing scales of consequence caused by potential MATTEs (SEPA, 2016a). Early feedback from use has indicated that the methodology and the risk criteria are workable, useful and most importantly give a level of risk based environmental protection which is proportionate to the scale of harm and by consensus is “about right”. This guideline, whilst good practice for COMAH establishments, could also provide a useful start point for any non-COMAH sites where environmental protection is a significant issue and where qualification / quantification of that risk is required (see for example Manton et al (2016) where the CDOIF approach has been applied to an incident at a U.S. non-COMAH site).

It has also been discussed that recent changes in law have made more explicit the requirement for operators of COMAH establishments to review historic incidents (both at their own establishments and nationally/internationally) to identify any historic incidents with the same substances or processes and thus identify lessons and ensure all necessary measures have been adopted to control risk.

Three case studies from historic incidents have been chosen to illustrate how the CDOIF environmental risk tolerability guideline can be used to analyse the risk gaps between the Apparent risk at an establishment, the Possible risk if FRR measures were to be adopted and also, the risk at any given point in time if existing protection layers fail or are compromised. In this paper, this is the Incident risk, but an analysis can equally inform management decisions around failed protection layers before an incident actually occurs (e.g. if inspection reveals defects in safety critical protection layers).

Often, lessons from incidents include the fact that deficiency in analysis of major accident hazards is a root cause. The three incidents chosen all occurred prior to the CDOIF environmental risk tolerability methodology. Thus whilst there should have been some form of environmental risk assessment carried out (and the lessons indicate this) at the time of the incidents there was not the degree of consensus that now exists. In the future, operators should be in a much better place with regard to understanding of methodology and environmental tolerability end points, to judge establishment risk and thus the measures necessary within the existing ALARP framework. The COMAH Competent Authority will seek to ensure SMSs have environmental risk assessment integral to their Hazard identification and analysis procedures.

The case studies have illustrated how use of environmental risk tolerability criteria can support decision making on All Measures Necessary. By placing environmental risk within the ALARP framework, judgements can be made about tolerability of establishment risk given existing and possible FRR measures. The established ALARP approach, including cost benefit analysis where appropriate, can be used to reach conclusions on required measures. This can in turn ensure

resources available for reducing risk are targeted where they will be most cost effective. The case studies have demonstrated how this approach can be used at establishment level (case study 5) and at a scenario level, through suitable modifications (calibration) of the risk tolerability criteria (case studies 1 and 3).

The case studies have also demonstrated how graphical representation of risk shows comparative scale of risk reduction from measures in place, the increase in risk if measures fail or the possible risk with FRR. In this paper a LOPA / modified LOPA approach has been taken, but the method is equally suited to a risk matrix, developed through a bow tie (fault & event tree) approach (SEPA, 2016a&b).

The case studies have also highlighted specific issues:

- In all three cases the Initiating Event frequencies represent an intolerable risk when compared to unmitigated consequences. Thus preventive measures alone were insufficient to deliver adequate risk reduction in these cases. This might seem counter to the safety hierarchy where preference should fall with inherent safety and avoidance of Hazard, and this would ultimately be the preferable way of achieving a tolerable risk. But by definition, COMAH establishments are those where a large inventory of dangerous substances already exist (the source), so any establishment where there is also a pathway to a sensitive receptor will find itself at greater risk and further down the hierarchy in terms of need for multiple protection layers.
- In all three case studies there were insufficient protection measures in place to ensure risk was ALARP or Broadly Acceptable. Moreover, some protection layers such as basic inventory management to detect loss of containment from a stock tank or a bund drain valve (leaking) were shown to be insufficiently reliable and failed to avoid environmental harm. Thus Incident risk (I) was greater than the Apparent level of risk (A) when all protection layers should have been functioning correctly. The risk gap A-I is indicative of the scale of reliance placed on measures that were proven to be vulnerable in a Major Accident scenario and with hindsight an unjustified degree of reliance was placed on these measures.
- During normal operations, if a protection layer is found to be compromised (e.g. a bund valve found leaking or an audit reveals deviation from the need to supervise operating equipment) then the risk assessment should be revisited to inform decisions on whether operations can continue, depending on the amount of risk reduction offered by the failed protection layer and the risk without it. In these case studies the risk gap A-I could have been recognised and decisions about how to continue safe operations subsequently made.
- In all three cases FRR measures that could have been implemented have been analysed to show that Potential MATTE risk (with available FRR measures) could have been much lower, and considered Broadly Acceptable. Though it should also be noted when considered FRR under ALARP principles, a Cost Benefit Analysis might show that cost of upgrade is grossly disproportionate to benefits.
- PFD data has been based on guidance provided by the COMAH CA (SEPA, 2016b), which is largely derived from experience of behaviour of protection layers under Major Accident scenarios (e.g. a bund might have a very low PFD for small spills, but a significantly greater PFD for a large pool fire or catastrophic tank failure). Further discussion on these issues is provided by SEPA (2016b) and data analysis presented in IChemE (2015).
- The case studies all involved liquid release to the aquatic environment (the most common of MATTE scenarios). Secondary and tertiary containment systems are good practice for mitigation of these events. Moreover, since secondary and tertiary containment systems are often based on civil / structural engineering disciplines they can more reliably bring independent risk reduction, compared to say enhancing an already existing tank inspection regime. But secondary and tertiary containment can fail and PFD will depend on various factors specific to the site and accident scenarios (SEPA, 2016b).

Conclusion

In many ways the findings in this paper are not surprising. Good Practice includes use of mitigation such as secondary and tertiary containment alongside preventive measures, so it could be expected that absence or degradation of secondary containment in these cases increased risk and proved intolerable. Unfortunately the incidents resulted in environmental harm. It is widely recognised that successful control of major accident hazards requires defence in depth – the use of multiple, independent protection layers. This is as true for protection of the environment as it is for protection of people. Thus even if one or a few layers fail, then operational risk (Incident risk – I - in this paper) should not become intolerable. If it does, measures should be in place to recognise the increased risk due to deterioration of protection layers and if intolerable, cease operation until the protection layers have been reinstated (or compensatory risk reduction implemented). This principle has clearly been illustrated here using a risk gap approach.

Fundamentally, this paper has illustrated the benefits that the CDOIF risk tolerability guideline can bring, in being able to make environmental risk decisions on All Measures Necessary, within the existing ALARP framework. This can be risk for the whole establishment, or by calibration of risk criteria, risk of a specific scenario. Moreover, experience in use of the risk tolerability criteria has, through continuing discussions between the regulator and industry, confirmed that the agreed thresholds of tolerability for differing scales of MATTE are “about right”. The case studies further demonstrate the validity of the thresholds by showing an absence of good practice is intolerable whilst adoption of good practice would deliver broadly acceptable risk. A degree of consensus on environmental risk tolerability, previously unseen, has now been reached (for GB COMAH establishment at least). The environmental risk tolerability debate now needs to be extended to all areas of industry where environmental protection needs to be managed within a safety “ALARP” framework.

References

EC (2017), eMARS Major Accident Reporting System, accessed 3/1/17 at https://emars.jrc.ec.europa.eu/

EC (2013), Lessons Learned Bulletin No.3 "Major accidents having significant impact to the environment", European Commission Major Accident Hazards Bureau, June 2013, accessed 23/12/2016 from https://minerva.jrc.ec.europa.eu/en/content/minerva/f30d9006-41d0-46d1-bf43-e033d2f5a9cd/publications%20

EI (2016) "Guide to predicting environmental recovery durations from major accidents: Supporting Guide to the Environmental Risk Tolerability for COMAH Establishments Guideline", DRAFT received through steering group correspondence, Energy Institute publication expected in 2017.

HSE (2012), Failure Rate and Event Data for use within Risk Assessments (28/06/2012), accessed 3/1/17 at http://www.hse.gov.uk/landuseplanning/failure-rates.pdf

HSE (2013a) CDOIF "guideline Environmental Risk Tolerability for COMAH Establishments" [v1 of the guideline, now unavailable since superseded by v2 - see SEPA, 2016a]

HSE (2013b) CDOIF guideline "Leak Detection", accessed 3/1/17 at http://www.hse.gov.uk/aboutus/meetings/committees/cif/leak-detection-guide.pdf

HSE (2015) "A guide to the Control of Major Accident Hazards Regulations (COMAH) 2015", L111, accessed 3/1/17 at http://www.hse.gov.uk/pUbns/books/l111.htm

IChemE (2015) Loss Prevention Bulletin – Environment Agency Special Issue, accessed 3/1/17 from http://www.icheme.org/lpb/free%20downloads.aspx

ISO/IEC (2014) Guide 51 "Safety aspects – guidelines for their inclusion in standards", accessed 3/1/17 from http://www.iso.org/iso/catalogue_detail.htm?csnumber=53940

Manton, Farquharson, Nicholas (2016) "An "Intolerable" Risk: Applying the UK Environmental Risk Assessment Methodology to Freedom Industries, WV", AIChE Spring Meeting and 12th Global Congress on Process Safety

Nicholas, Brocklebank, Coates, Davidson and Bray (2014), "Environmental risk tolerability for major accident hazard sites: A method for quantifying and assessing environmental risk", IChemE Hazards 24

SEPA (2016a) CDOIF guideline "Environmental Risk Tolerability for COMAH Establishments" v2, accessed 3/1/17 from http://www.sepa.org.uk/media/219154/cdoif_guideline__environmental_risk_assessment_v2.pdf

SEPA (2016b) "All Measures Necessary - Environmental Aspects", COMAH CA, accessed 3/1/17 at https://www.sepa.org.uk/media/219152/d130416_all-measures-necessary-guidance.pdf