
CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Understanding Major Hazard Human Harm Risk Assessment (MHHHRA) for COMAH

Foreword

The Chemical and Downstream Oil Industries Forum (CDOIF), promotes and leads on the management, control and mitigation; of the consequences of major accident hazards in the onshore chemicals and downstream oil sectors.

Working with its members, it has developed this guideline on understanding Major Hazard Human Harm Risk Assessment (MHHHRA), which is focused on establishments subject to the Control of Major Accident Hazards Regulations 2015 (COMAH).

This guideline's primary focus is on the identification, analysis, and assessment of major accident hazard scenario(s) (MAHS); associated with the unit operations performed at an establishment.

The guideline is intended for the practitioners of MHHHRA, including COMAH Operators. This guideline should be used from the date of publication to carry out the assessment of major hazard human harm risks for COMAH. The document will be periodically reviewed to allow both industry and the Competent Authority (CA) to give feedback on any significant issues that arise from its implementation and determine if revision is necessary.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

- I. It is understood that this report represents CDOIF's view of common guidelines applied to the assessment of major hazard human harm risks for COMAH; including determining risk tolerability, and also demonstrating 'As low as reasonably practicable' (ALARP).
- II. CDOIF accepts no responsibility, or liability, for the use or misuse of this document.
- III. The guideline is distributed in a read only format, such that the name and content is not changed, and that it is consistently referred to as 'CDOIF guideline – Understanding major hazard human harm risk assessment for COMAH'.
- IV. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report, except that it is believed to be substantially correct at the time of publication.

While preparing this guideline on MHHHRA, CDOIF noted that the language use in relevant safety legislation (for example, Health and Safety at Work etc. Act 1974, and the Management of Health and Safety at Work Regulations 1999), associated reference documents and guidance was different to that used when considering risk assessments related to major accidents to the environment (MATTE). It was not within the scope of this CDOIF guideline to develop a holistic regime, with a common language, when undertaking the assessment of major hazards associated with human harm and the environment. CDOIF recognises the value of undertaking such work in the future.

Operators may therefore find it useful to read the MHHHRA guideline in conjunction with the CDOIF Environmental Risk Tolerability Guideline¹, noting that the environmental guideline addresses additional MAHS analysis and evaluation of the releases associated with MAHS leading to serious danger to the environment.

The MHHHRA guideline is not intended to be an authoritative interpretation of the law; however, Competent Authority inspectors may refer to it in making judgements about an Operator's compliance with the law. This will be done in accordance with the CAs' published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf).

¹ Chemical and Downstream Industries Forum (CDOIF), (2016) 'Environmental Risk Tolerability for COMAH Establishments – Guideline', V2.0. CDOIF.

It is anticipated that this document will facilitate a consistent national approach and drive the right behaviours. It should be understood that this generic guideline does not explore all possible options for satisfying the good practice principles identified, when carrying out the assessment of major hazard human harm risks for COMAH. The guide is general and does not consider individual establishment requirements. Following this guidance is strongly encouraged by CDOIF, but it is not compulsory, and Operators are free to take other equivalent action.

Some of the 'good practice principles' in this CDOIF guideline, will be relevant to employers in non-COMAH sectors undertaking a 'suitable and sufficient risk assessment' for process safety. However, care should be taken when directing employers in non-COMAH sectors to this CDOIF guideline. All of the 'good practice principles' may not be directly applicable. In addition, the proportionality of a site in a non-COMAH sector, may be quite different to that of a COMAH establishment; this could mean that the required depth, robustness, and resolution, may differ.

The Health and Safety Executive (HSE) 2001 publication 'Reducing risks, protecting people: HSE's decision-making process' (R2P2), set down the general approach used by the HSE for making regulatory decisions. The document made it clear that R2P2 was not intended as guidance for Operators. R2P2 explained that Operators who want to emulate the regulators' approach, have to recognise the different contexts in which HSE applies its framework; taking this into account when applying it to their own sectors of industry (one such context is the COMAH regulatory framework). R2P2 has now been archived by HSE, as many Operators have used it as guidance, or still refer to this document; therefore its previous use is referenced in this guideline. This CDOIF guideline outlines an appropriate approach for COMAH Operators to adopt when applying these principles, including when undertaking a tolerability of risk assessment (**see section 5.5**).

MAHS, MAHS(s): Singular and plural

in the main body of the guidance, for expediency and to avoid unnecessary replication, the acronym MAHS has been used to represent both 'Major Accident Hazard Scenario' singular, and also the plural 'Major Accident Hazard Scenarios'. In the Executive Summary, and the introductory sections, for clarity, the phrase has been used in full, or parentheses have been used.

Contents

1.	Executive Summary.....	9
2.	Scope and introduction	16
2.1	Regulatory context	17
2.2	Competency requirements	17
2.3	Proportionality in risk assessment for COMAH.....	18
2.4	Using this guide	19
2.5	MHHHRA process flow and legend	21
3.	Major accident hazard scenario identification.....	22
3.1	An overview of the key principles of a systematic MAHS identification process ...	22
3.2	Defining MAHS.....	23
3.3	Identification of potential-MAHS.....	26
3.3.1	Technical Folder	28
3.3.2	Existing plant – use of existing studies	29
3.3.3	Chemical behaviours and interaction studies	29
3.3.4	Establishment information	30
3.3.5	Known major accidents and incidents	30
3.3.6	Top-down studies	31
3.3.7	Bottom-up studies	32
3.4	Screening for MAHS.....	33
3.4.1	Screening tables	34
3.5	Periodic review and revision	35
4.	Major accident hazard scenario analysis	36
4.1	An overview of the key principles of analysis.....	36
4.1.1	Purpose of analysis	36
4.2	Scenarios inside and outside the system.....	40
4.2.1	Scenarios outside the system	41
4.2.2	Scenarios inside the system.....	42
4.2.3	Scenarios involving active management.....	43
4.2.4	System scenarios driven by random failures	44
4.2.5	Scenario and sub-scenarios	44
4.2.6	Catastrophic vessel failure due to manufacturing or construction defect.....	46
4.3	Representative scenario set(s)	46
4.3.1	What is not considered to be a representative scenario set?.....	48
4.3.2	What is not considered to be a representative scenario?	48
4.4	Scenario development	50
4.4.1	Scenario description	50
4.5	Scenario basis of safety and safe operating envelope	51

4.5.1	Basis of Safety	51
4.5.2	Safe operating envelope	51
4.6	Scenario consequence extent and severity assessment	52
4.6.1	On-site population determination of death and serious injury	53
4.6.2	Off-site population determination of death and serious injury	54
4.6.3	Source terms.....	55
4.6.4	Modelling and calculations	57
4.6.5	Extent and severity table	57
4.6.6	Consequence map.....	58
4.6.7	Emergency planning	59
4.7	Scenario control measures.....	59
4.7.1	Systems of control	60
4.7.2	Safety systems.....	61
4.7.3	Self-acting devices.....	61
4.7.4	Active management systems	61
4.7.5	Measures for which no credit has been taken	63
4.8	Scenario frequency analysis	63
4.8.1	Qualitative approaches – The use of risk assessment matrices	63
4.8.2	Bow-tie Diagrams	64
4.8.3	Semi quantitative approaches – LOPA	64
4.8.4	Use of LOPA within Process Hazard Analysis/Process Hazard Review studies	66
4.8.5	Common LOPA failings	67
4.8.6	Fully quantitative approaches – Fault Trees	67
4.8.7	Parts count.....	68
4.8.8	Levels of analysis	68
4.8.9	Simplified parts count using the offshore hydrocarbon release database.....	70
4.8.10	Generic failure rates for perforation of piping and vessels	71
4.9	Scenario failure frequency data	72
4.9.1	Supplier data	72
4.9.2	HSE failure rate database	73
4.9.3	SIL certified device data	73
4.9.4	TNO Purple Book data	73
4.9.5	Using multiple sources of failure rates	74
4.9.6	Human factors and failure frequency	74
4.10	Scenario gap analysis (including Relevant Good Practice, RGP).....	74
4.10.1	Hierarchy of control measures and the application of relevant good practice	74
4.11	Scenario additional supporting information	75
4.12	Scenario conclusion.....	76
4.13	Periodic review and revision	76
5.	Major accident hazard assessment.....	77
5.1	An overview of the key principles of assessment.....	77
5.2	Evaluation of serious danger	80

5.2.1	Cumulative risk from the establishment to a person on-site or off-site	80
5.2.2	Collation of basic scenario information	82
5.3	Population profiles on-site and off-site.....	83
5.3.1	Population within the site boundary ['on-site' population]	83
5.3.2	Population outside the site boundary - consideration of the public	84
5.3.3	Review of proportionality	88
5.4	Cumulative individual risk and its relation to risk from the establishment to a person	88
5.4.1	Cumulative individual risk (hypothetical person) - location risk	89
5.4.2	Cumulative individual risk (job function)	90
5.4.3	Cumulative individual risk (named person)	91
5.4.4	Relationship between time on-site and cumulative individual risk.....	91
5.4.5	Use of expectation values for risk tolerability	92
5.4.6	Determining Cumulative Individual Risk.....	92
5.5	HSE's tolerability of risk (TOR) framework.....	94
5.5.1	Consideration of TOR framework against serious injury	95
5.5.2	HSE's societal risk of death.....	95
5.5.3	Assessing societal risk in terms of both death and serious injury	96
5.6	Establishment cumulative risk summary	97
5.6.1	If the cumulative risk tolerability threshold is exceeded	100
5.6.2	If cumulative risk tolerability threshold is not exceeded.....	101
5.7	Periodic review and revision	101
6.	Further risk reduction measures	102
6.1.1	What is a MAHS further measure?.....	102
6.1.2	Are further measures still required if a system meets RGP?.....	104
6.1.3	The relationship of further measures to reasonable practicability and 'all measures necessary'	104
6.2	Producing a list of further measures.....	105
6.2.1	Gap analysis: standards, ACOP and industry guidance (SAIG)	105
6.2.2	Some examples of common improvements considered	105
6.2.3	Extent to which further measures should be explored.....	107
6.2.4	Longlisting and shortlisting	108
6.3	Evaluation of further measures.....	108
6.3.1	Assembling the costs of implementing the further measure.....	109
6.3.2	The benefits of implementing the further measure	110
6.4	Expectation value estimation	112
6.4.1	Expectation value estimation for human harm.....	112
6.4.2	Calculating EVs for scenarios that give rise to multiple consequences	113
6.4.3	Expectation value for MATTE remediation	114
6.4.4	Expectation value for business interruption and rebuilding costs.....	114
6.4.5	Total expectation value for further measures.....	115
6.5	Time horizon.....	115
6.6	Discounting	115

6.6.1	Discounting the capital cost for the further measure	116
6.6.2	Discounting the benefits of preventing harm to the person or the environment.....	117
6.7	Bias.....	117
6.8	Aversion.....	117
6.9	Sensitivity analysis – Identifying ‘switching values’	118
6.10	ALARP Conclusion.....	119
6.11	Periodic review and revision	119
7.	Arrangements for ensuring a suitable and sufficient risk assessment is in place, and adequately maintained	120
7.1	Safety management system	120
7.1.1	Implementation	120
7.1.2	Ensuring performance	121
7.2	Change in on-site and off-site populations	121
7.3	Internal emergency plan	121
Annex 1 -	Regulatory context	123
Annex 2 -	Consideration of MAHS proportionality.....	126
Annex 3 -	Determination of chemical behaviours and interactions.....	131
Annex 4 -	Collated accidents and incidents summary table – for illustrative purposes.	152
Annex 5 -	Open source chemical incident databases	153
Annex 6 -	Typical screening table for illustrative purposes, showing different approaches.....	157
Annex 7 -	Consideration of batch processes	160
Annex 8 -	Suggested criteria to determine harm to the person from thermal radiation .	164
Annex 9 -	Suggested criteria to determine harm to the person from exposure to toxic gases and vapours	167
Annex 10 -	Suggested criteria to determine harm to the person from overpressure (and impulse)	168
Annex 11 -	Example simple scenario frequency summary table	173
Annex 12 -	Example of a layer of protection summary table	175
Annex 13 -	Failure rate data sources	176
Annex 14 -	Deriving failure rates from site data.....	178
Annex 15 -	Standard discount factor table	182
Annex 16 -	Discount factors to value human health.....	183
Annex 17 -	Example population map and population tables	184

Annex 18 - Human error identification/probability references	189
Abbreviations Used	190
Reference List.....	193
Acknowledgements.....	195
Revision History	196

1. Executive Summary

For the purpose of controlling the risk of human harm from the operations performed at an establishment, the Management of Health and Safety at Work Regulations 1999 requires employers to undertake a suitable and sufficient risk assessment. This Chemical and Downstream Oil Industries Forum (CDOIF) guideline has been developed for Operators, practitioners, and regulators. It provides common agreed principles to enable a suitable and sufficient risk assessment to be carried out. Following the principles set out in this document should ensure that the appropriate measures are in place, the remaining residual risk is below the tolerability threshold, Operators comply with the requirements under the relevant statutory provisions, and that risks are ALARP.

These relevant statutory provisions include the Control of Major Accident Hazards Regulations 2015 (COMAH), which requires the identification and assessment of potential major accident hazards. Under HSE guidance (L111)⁴ all measures necessary equates to the principle of reducing risks as low as reasonably practicable (ALARP). The ALARP principle is HSE's operational interpretation of the legal requirement in the Health and Safety at Work etc. Act 1974 to protect people 'so far as is reasonably practicable' (SFAIRP). For lower tier COMAH establishments, a safety report is not required to be submitted, however a risk assessment is still required. This is necessary to both satisfy the need to record key findings, and also to make demonstrations when requested by the COMAH Competent Authority. For upper tier COMAH establishments, the risk assessment underpins the safety report.

The purpose of this guideline is to outline the principles of risk assessment that must be followed, and to suggest methodologies that represent good practice to satisfy them. A methodical structure and approach are described in brief, with references to further reading if required. Applying the guideline by using the methodologies within, or an equivalent that satisfies the principles identified; should result in a risk assessment that is suitable and sufficient. If a COMAH report is required, this will also form the demonstration of 'all measures necessary'.

The guideline consists of four main sections:

- Identification.
- Analysis.
- Assessment.
- Further measures.

An additional section, 'Arrangements for ensuring a suitable and sufficient risk assessment is in place', outlines the expected arrangements to be made for risk assessment by the Operator, including review and revision. Annexes have been provided to give additional support in some areas; these give further information, examples, and additional references; they include:

- Chemical behaviours and interactions.
- Consideration of batch processes.
- Thermal and overpressure criteria.
- Failure rate data sources.
- Deriving failure rates from site data.
- Population map/tables.
- Human error identification.

This guideline has been developed by CDOIF members for the benefit of the UK chemical and pharmaceutical industries, in particular COMAH establishments. The COMAH CA's advice is that this MHHRA guideline outlines good practice MHHRA principles that are

relevant to all COMAH Operators. CDOIF recognises that many of these good practice MHHHRA principles may also be applicable to some non-COMAH sectors, but care is needed as some of the good practice principles (such as those related to tolerability of risk and the depth, robustness and resolution of the MHHHRA) may differ.

When producing this high level MHHHRA guideline, CDOIF recognised that industry may require further guidance in some areas, such as: inherent design, process safety, human factors, competence management, and COMAH safety management systems. CDOIF recommends that industry considers developing guidance in these areas. CDOIF also recognises that some supporting examples of how the MHHHRA good practice principles could be applied in different COMAH sectors would be beneficial.

Summary of guidance principles

A tabulated summary of the good practice principles described under each section of the MHHHRA guideline, is given below. These principles have been presented in the Executive Summary to assist the reader in navigating to the section of the document most relevant to the aspect of MHHHRA they wish to consider. These good practice principles are only in outline and should not be considered in isolation from the supporting text. CDOIF reminds Operators that they are free to choose alternatives to the suggested approaches, so long as the good practice principles can be demonstrated to have been met.

Section 2: Competence and Proportionality	
(1) Competence	It is essential that the MHHHRA is conducted by competent resources throughout the process. If a third party is engaged, it is essential that the Operator both verifies the information used to carry out the study, and reviews its findings; ultimately the Operator is responsible for the adequacy of the assessment.
	See 2.2
(2) Proportionality	The depth, resolution and robustness of the MHHHRA should be proportionate to the severity of the hazard to people.
	See 2.3
Section 3: MAHS Identification	
(1) The study extent should be defined	The extent of the study should be clear, consider each relevant area at the establishment, breaking it down into significant unit operations.
	See 3.1
(a) Collate and consider relevant and current information	<i>Current information needed to identify all the potential-MAHS(s) associated with each unit operation, should be collated.</i> • <i>Technical Folder (collated current technical information relating to the unit operations), this should include both the Basis of Safety and also the Safe Operating Envelope.</i> • <i>Risk Assessments and existing studies (should include both top-down and bottom-up studies).</i> • <i>Chemical behaviours and interactions.</i> • <i>Establishment information.</i> • <i>Pertinent major accidents and incidents.</i> • <i>Basic information on distribution of on-site and off-site populations.</i> <i>Additional studies to be performed as necessary until the data set is current and complete.</i>
	See 3.3

(2) Screen to Identify potential-MAHS/MAHS The Operator should systematically screen all Unit Operations to identify all potential-MAHS(s) using relevant and current information. This should include the 'top-down' and 'bottom-up' studies undertaken. Screening should use the MAHS criteria of: the potential for fatality, and also those MAHS giving rise to three or more serious injuries. See 3.4
(a) Records <i>A suitable record should be provided which identifies all potential-MAHS(s); and then those considered to be MAHS(s); the record noting the reasons why any potential-MAHS has not been taken forward. The record should also include a list of all information considered whilst performing the study.</i> See 4.3
(b) Safety Management System <i>The SMS should define MAHHRA approach, including identifying and evaluating potential-MAHS/MAHS. Noting that some of the potential-MAHS that have been 'screened out' may still require further consideration. For example, they may lead to a major accident to the environment, involve occupational health and safety, or other general duties.</i> See 4.3 & 7.1
Section 4: Analysis
(1) MAHS set for analysis All Unit Operations that have been identified as giving rise to MAHS(s), should have developed scenario(s) with a proportionate level of analysis. A complete list of MAHS should be included. See 4.1 & 4.2
(a) Use of a unit operation representative <i>Where a representative MAHS is used to represent other sufficiently similar unit operations, each instance of the other members of the set it represents should be listed, together with any minor differences.</i> See 4.3
(2) Development of each scenario All initiating and propagating event combinations must be identified; and analysed in a way that shows how the appropriate measures relate to a particular initiating event, or specific groups of events (sub-scenarios). See 4.4
(a) Basis Of Safety/Safe Operating Envelope <i>The BOS/SOE should be determined and reported in each scenario development, together with any necessary preconditions.</i> See 4.5
(b) Extent and severity assessment <i>Extent and severity will be effectively determined and reported for each MAHS consequence; this will include isopleths for both death and also for serious injury. Any source terms used should be given together with the methodology used to derive them, and example calculations provided for that scenario. Harm criteria used should be those indicated in the guidance, or a justified equivalent; and should be appropriate for the populations at risk.</i> See 4.6
(c) Escalation <i>Where the consequences of the MAHS may lead to further loss of containment from surrounding equipment, and consequent escalation; this should be adequately considered in determining the extent & severity, and frequency of possible consequences.</i> See 4.6

(d) Scenario control measures <i>In the development of each MAHS: the specific control systems, safety systems, and self-acting devices should be described in such a way that the layers of protection are readily discernible; their particular role in preventing the event combinations identified is clear, and demonstrates that appropriate measures are in place. General arrangements such as hazardous area classification, lightening protection, and vessel inspection etc should be developed separately.</i> See 4.7
(e) Scenario frequency analysis <i>The frequency of the MAHS top event occurring should be determined using quantitative and/or semi quantitative approaches, then reported. Qualitative approaches should not be used for evaluation of COMAH MAHS (though they may be appropriate for initial screening). Analysis should be conducted for the particular configuration and operating regime, at an appropriate level of analysis.</i> See 4.8
(f) Scenario failure frequency data <i>In most cases, data at the component/equipment level will be combined to represent the system. Any supplier data should be adjusted for site conditions. Where insufficient site data at component level is available, and generic data is used, it should be compared to any available site data. Where plant is approaching the end of its life, normal statistical treatments may significantly underestimate failure rates, and more appropriate models should be used.</i> See 4.9
(g) Consequence frequency analysis <i>An event tree, or similar, should be used to evaluate the frequency of the possible consequence outcomes determined. The use of an opaque software tool on its own is not appropriate; frequency derivation must be clear and reproducible, with an event tree summary table included.</i> See 4.8
(3) Consideration of Relevant Good Practice (RGP) and the treatment of deficiencies A logical demonstration should be made to show that the hierarchy of control has been applied; and also current RGP, or its equivalent, is in place. If no relevant RGP is applicable the appropriate measures should be demonstrated from first principles. A time-limited improvement plan should be given for any necessary improvement identified. See 4.10
(a) Additional supporting information <i>Relevant reported historic major incidents, both on site and world-wide, should be included in the supporting information for the particular MAHS.</i> See 4.11
(4) Scenario conclusion A concluding summary for each scenario should be given stating: compliance with RGP; the adequacy of the appropriate measures present; additional measures considered; scenario frequency; extent and severity; reference to other members of the representative scenario group; and a statement that all measures necessary have been taken for that MAHS. See 4.12
Section 5: Assessment
(1) Basis of assessment The assessment of risk from the establishment to the population, both on-site and also off-site, must consider the cumulative frequency of 'serious danger' (both death and also serious injury) from the MAHS(s) identified. See 5.2

(a) Collation of basic scenario information <i>In order to show the site risk profile across the site and allow the main contributors to be seen; a compact table should be assembled grouped by intuitive area, which summarises the MAHS frequency, also the number of fatalities and number of serious injuries.</i> See 5.2
(2) Population profiles Populations inside and outside the site boundary have different risk tolerability levels, and also very different occupancy profiles; they should therefore be considered separately. Both the on-site, and also off-site, populations should be characterised to an appropriate resolution, to an envelope just beyond that created by the hazard ranges. See 5.3
(a) On-site/off-site population mapping <i>The on-site population profile should clearly be defined on the map and list all on-site occupied buildings and their occupancy level. The location with time for the highest risk job function(s) should be given.</i> <i>The off-site population should be characterised: development types should be identified on the map, and listed together with population densities.</i> See 5.3
(3) Determination of greatest cumulative individual risk and societal risk for both on-site and off-site populations. The highest Cumulative Individual Risk and Societal Risk should be established for both the on-site and off-site populations. This should be the sum of the MAHS consequence frequencies that a person present is exposed to, for both death and also serious injury. To be valid the appropriate form of cumulative individual risk selected must be appropriate for the particular circumstance being considered. See 5.4
(4) Tolerability of risk from the establishment to the person should be established It is necessary to establish whether or not the maximum cumulative individual risk and cumulative societal risk are considered to be above the established tolerable threshold. Noting that for MAHS which result in three or more serious injuries; HSE consider that every three serious injuries are considered to be equivalent to a death. See 5.5
(a) Individual risk tolerability criteria test <i>HSE risk tolerability framework for 'major hazard human harm risk assessment' should be used to test cumulative individual risk.</i> See 5.5
(b) Societal risk tolerability criteria test <i>The cumulative societal risk for both death and serious injuries should be determined and compared to the criteria, this is represented by a line with a slope of minus one, on a log/log plot of frequency vs number of fatalities, passing through a point representing '50 deaths or their equivalent' at a frequency of $2 \times 10^{-4} \text{ yr}^{-1}$.</i> See 5.5
(5) Establishment cumulative risk summary The assessment process should conclude with a set of metrics for both on-site and off-site populations. Risk summary tables should be provided along with a summary of the individual risk job functions sampled. See 5.6
(a) If tolerability threshold is exceeded <i>The assessment may not be of sufficient resolution; further analysis may be required. The Operator should then consider if all appropriate measures are in place.</i> See 5.6

(b) If tolerability threshold is not exceeded

This does not on its own, show that the risk has been reduced so far as is reasonably practicable (ALARP). Credible further risk reduction measures must be determined and evaluated, further reduction in risk achieved by those measures is balanced against the additional costs.

See 5.6

Section 6: Further measures

(1) Consideration of further risk reduction measures

A 'further measure' is any additional, reasonably practicable control, safeguard or mitigation; that has not already been implemented; that would lead to an additional reduction in risk, or a reduction in the number of people that would be killed or seriously injured.

See 6.1

(2) Assemble and evaluate a list of further measures

For each MAHS, a list of further measures should be assembled and evaluated. At this stage, inherent safety and appropriate measures should have already been considered. If the requirement for a measure is considered obvious, and the Operator is going to implement it, then a cost-benefit analysis (CBA) for that measure is not needed.

See 6.2

(a) Longlisting and shortlisting of measures

For high proportionality MAHS, the approach should transparently show how the many possible practical measures have been methodically reduced to a small number; then subjected to detailed evaluation.

See 6.2

(3) Undertake Cost benefit Analysis (CBA)

Comparing the 'costs' of implementing the further measure, with the monetary value of the 'benefits' gained (reduction in human harm and damage to the environment). A methodology that reflects the good practice outlined in the Governments Green Book should be adopted.

See 6.3

(a) Consideration of the Costs

The 'costs' should include the capital cost of installing the measure, and if applicable, any associated increased operational costs.

See 6.3 & 6.7

(b) Consideration of Benefits

The 'benefits' must include both the reduction of human harm and also the cost of remediating any damage to the environment should the MAHS occur. It is recommended that the 'benefits' also consider the costs that would be associated with avoiding or reducing: damage to the establishment, business interruption costs, and also any third-party costs.

See 6.3

(c) Use of 'expectation value'

In order to monetise the benefits that accrue over the lifetime of the improvement, it is necessary to determine the expectation value of the risk reduction being considered over a specified period of time.

See 6.4

(d) Time horizon, discounting, and sensitivity analysis

The time period for which 'costs & benefits' from the further measure are accrued must be declared. If it is elected to claim discount for future benefits, this should be clearly explained. Sensitivity analysis should be performed when duty holders have limited information, and the costs and benefits are sensitive to small changes in key inputs.

See 6.5, 6.6, & 6.9

(4) Implementation of reasonably practical further measures Where the expectation value of the further measures is less than the benefits of risk reduction to both people and the environment, it should be implemented. See 6.1
(a) <i>If a further measure is not implemented</i> <i>If the Operator is arguing not to implement a measure, a CBA is required, with an explanation of why a measure has been discounted. It is essential to ensure all the costs and benefits are included and explained, giving a logical justification that is transparent and reflects the proportionality of the MAHS under consideration.</i> See 6.3
(b) <i>Consideration of aversion</i> <i>It is acknowledged that society is much more concerned about a single high consequence event that kills many people, than multiple single incidents that only lead to 1 or 2 fatalities. The greater the number of people killed or seriously injured in a single incident, the greater is society's concern or 'aversion'. This should be accounted for in any cost benefit analysis.</i> See 6.8
(5) ALARP conclusion Once the MHHHRA process is completed, there should be a conclusion at the end of the assessment stating that for all unit operations: appropriate measures are in place; and all reasonably practicable further measures will be implemented in accordance with the time-bound improvement plan (agreed with the COMAH Competent Authority). See 6.10
Section 7, Revision and Review
(1) Review and revise your MHHHRA as appropriate The Operator's SMS should outline the arrangements to ensure a suitable and sufficient MHHHRA is undertaken and remains effective. It should be reviewed and revised as necessary, both periodically and when there are changes to the information used, or the unit operations themselves. It is expected that any time-bound improvement plan is overseen by the executive management team to ensure its implementation; noting that the risks from the establishment cannot be deemed to have been reduced to as low as is reasonably practicable until that phase is completed. See 7

2. Scope and introduction

A logical and appropriate assessment process that leads to a suitable and sufficient risk assessment is the foundation of any safety management system. Risk assessment ensures that major accident hazard scenarios are identified, eliminated, or controlled; and their consequences are mitigated where possible. An appropriate assessment process assures both the Operator and the regulator that 'all measures necessary' have been taken; also that the cumulative risk from the establishment is below the tolerability threshold, and that the risk is 'as low as reasonably practicable' (ALARP). Assessment should be used in making decisions regarding appropriate control measures; and to inform future reviews of the establishment's risk profile; also to help the Operator make informed responses to challenges from the COMAH Competent Authority (CA).

This guideline's primary focus is to assess the risk of human harm from the major accident hazards associated with a COMAH establishment's unit operation(s). A unit operation is a defined physical change, and/or defined chemical transformation, performed within a fixed defined system. A [process] system is a fixed arrangement of process equipment whose boundaries are defined. It may be used to perform a particular process, or a number of defined processes. It is normally designed to be operated either continuously, or just to produce single batches.

A unit operation, either batch or continuous, chemical or physical; normally takes place in a system comprising a main vessel and a small number of ancillaries. Examples would include a continuous distillation column with its reflux condenser and reboiler; a continuous fluidised bed reactor; or a stirred batch reactor, with an overhead condenser, and its charge systems. This does not normally comprise the whole chemical process, which would consist of a number of interconnected unit operations, or discrete process steps undertaken in the same vessel. The guideline suggests that analysis and assessment are undertaken at the unit operation level, or by process step for multi-step reaction processes.

For each unit operation, there will be a number of associated major accident hazard scenarios (MAHS). A MAHS must include the event combinations/sub-scenarios (**see section 3**) that lead to the 'top event', which is normally loss of containment; then describe how the measures prevent the initiating or propagating events (**see section 4**). This would be challenging if attempting to consider a whole multi-vessel process at once.

This guideline outlines a systematic process: MAHS identification, analysis, assessment, and the consideration of further measures. In each section, the text outlines guiding principles, then provides a suggested methodology to satisfy them. This should enable the Operator of a COMAH establishment, or their risk assessment practitioner, to undertake a major hazard human harm risk assessment (MHHHRA) which is suitable and sufficient.

This guideline includes:

- consideration of good practice;
- how to apply the framework of principles in a proportionate way;
- explanations of the common tools and techniques available, and their appropriate application, highlighting common pitfalls; and
- examples of which tools and methodologies that illustrate good practice.

This guideline can be used when developing, reviewing, and updating, an Operator's assessment of major hazard human harm risks for COMAH; considering new processes and unit operations, including emerging energy technologies.

When developing this guideline, CDOIF noted that quantified risk assessment (QRA) means different things to different stakeholders, such as Operators and third-party consultants. This guideline explains that a suitable and sufficient MHHRA requires that all MAHS have been identified, the event combinations that lead to the MAHS are recorded, and that there is a logical argument that the appropriate measures are in place. This is supported by a numerical analysis, including a tolerability of risk assessment, and consideration of further measures. It is for COMAH Operators to decide if they want to go further than the good practice principles outlined in this CDOIF MHHRA guideline.

The Operator's safety management system (SMS) must be based on an assessment of risk. This means that a COMAH Operator's SMS in regard to major accident hazard management, will be based on MHHRA. It is suggested that the SMS should adopt the relevant good practice outlined in HSE's publication 'Managing for health and safety' (HSG 65) or an equivalent, and the SMS principles outlined in COMAH (L111). Further detail is given in **section 7** and also **Annex 1**.

Major accidents to the environment (MATTE)

Where the approaches are also relevant to major accidents to the environment (MATTE), this will be indicated, and link(s) will be provided to the CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments'. For example, cost-benefit analysis undertaken to consider further measures, considers benefits to both human harm and the environment (**see section 6**). Please note that although the Human Harm MAHS identification approach outlined in this guideline will also identify some MATTE, further appropriate approaches such as the methodology in the CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments', may also have to be adopted to identify all MATTEs.

When considering external scenarios such as flooding, wind, rainfall, and snowfall; Operators are encouraged to think about the longer-term issues created by climate change. This includes reviewing relevant design parameters, such as wind loading; also the increased or changing stress, climate change may place on critical systems such as cooling water. For further advice on the appropriate risk assessment required for climate change, see CDOIF's Guideline 'Adapting to Climate Change'².

As it is impossible to cover all aspects of all risk assessments in one place, this guideline focuses on the assessment of major hazard human harm risks for COMAH (for example, major accident hazard identification, analysis and assessment associated with a COMAH establishment's unit operations).

2.1 Regulatory context

This guideline outlines the principles and good practice associated with undertaking a suitable and sufficient MHHRA. The regulatory context for this legal requirement is outlined in **Annex 1**, including how this links with the 'all measures necessary' and safety report requirements given in the COMAH 2015 Regulations.

2.2 Competency requirements

When undertaking the major hazard human harm risk assessment for COMAH, there is a need to ensure that relevant competent resources are used throughout the process. In the context of this guidance, it is likely that for the unit operation(s) with the highest proportionality MAHS (**see section 2.3, and Annex 2**), 'suitably qualified risk assessment professionals' will be required. They will be needed to support the development and implementation of 'suitable and sufficient' approaches to MAHS identification, analysis, and assessment. This may include the adoption of quantitative, and semi-quantitative, approaches to analysis and

² CDOIF, (2024) 'Guideline – Adapting to climate change'. CDOIF.

assessment. Professionals, who may be experienced in applying some risk assessment tools at the control and mitigation measures level (for example, layers of protection analysis, and cost-benefit analysis) may not have the knowledge, competence, or capability, to undertake the analysis and assessment of both individual, and societal risk. They may also not be able to demonstrate that the establishment risk is below the tolerability threshold and meets ALARP.

For MAHS of lower severity (**see section 2.3, and Annex 2**), the depth, resolution and robustness required for a MHHRA may be less. The knowledge, competence and capability required will depend on the suitable and sufficient approaches adopted. Sometimes, the implementation and delivery of the identification, analysis and assessment tools selected; will be well understood by the establishment's health and safety practitioners; on other occasions additional expertise will be required.

2.3 Proportionality in risk assessment for COMAH

Proportionality is used to describe the relationship between the severity of the hazard to people, and the 'depth, resolution and robustness' expected of the MHHRA performed. It is an indicative metric not an absolute measure. In this guide, proportionality is used to inform the appropriate depth, resolution and robustness of risk assessment for each particular major accident hazard scenario.

Quite clearly the degree of depth, resolution and robustness in the assessment for a MAHS which has a hazard potential of three serious injuries, would not be expected to be as great as for a MAHS which could lead to more than a dozen deaths.

An establishment which exceeds the threshold at which COMAH applies, and also presents potential-MAHS leading to serious danger to the person, is already considered of high proportionality. Here, we are considering whether a site is on the cusp of high proportionality, or is of the 'highest' proportionality. The two ends of the spectrum could be represented by: 500 tonnes of methanol, stored in one tonne movable bulk containers, held under ambient conditions, stored close to an occupied building; through to a site storing over 20 tonnes of acrolein, and processing large quantities of acrolein at elevated temperature and pressure, located near a centre of population.

It should also be noted that risk assessment is a dynamic and iterative process; and so depth, resolution, and robustness, may change with the different phases. The initial high-level screening to determine if there is major accident hazard potential could be qualitative, using conservative assumptions (see 'Risk criteria for land use planning in the vicinity of major industrial hazards'¹²). Conversely, a detailed analysis of the MAHS associated with a complex high hazard unit operation, in support of a tolerability demonstration, would involve more detail and less conservatism, so is likely to be quantitative. When considering further measures for a given MHHRA, proportionality will also influence the depth required to underpin its evaluation (**see section 6**).

Determining proportionality

Proportionality is initially established using 'severity', which is the number of both fatalities, and also serious injuries. Factors that would suggest adjusting proportionality are considered collectively, then used to adjust the initial ranking. See **Annex 2** for further details on determining proportionality in regard to MHHRA.

Where the consideration of proportionality is not necessary

There are some external MAHS, such as aircraft impact, which even though they are of very high severity the Operator has no direct control over the initiating and propagating events, or

their possible elimination. This would not discharge the responsibility for the Operator to take necessary measures (see Annex 2).

2.4 Using this guide

As discussed above, this guideline provides a framework of principles, and outlines a systematic process, for carrying out the assessment of the major hazard human harm risks associated with an establishment's unit operations, for COMAH. It does not provide detailed guidance on all aspects of risk assessment (for example, for general arrangements, occupational health and safety, or for MAH to the environment).

The MAHS identification, analysis, and assessment framework; principles and process; outlined in this guideline involves:

- **The identification of MAHS** – This starts with the consideration of appropriate information. This includes current information on the chemical behaviours and interactions; technical information relating to the unit operations as they are currently configured, and final process design; establishment layout information, its surroundings and relevant populations; and information on known major accident hazards. Using this information, and outputs from 'top-down' and 'bottom-up' studies, will identify all potential major accident hazards; and also the circumstances that could lead to each 'potential-MAHS'. The MAHS for each unit operation are then determined by using the COMAH definition of major accident (serious danger to human health, which includes both death and serious injury) and some estimate of extent and severity.
- **Analysis** – Analysis involves developing the MAHS. First fully defining the MAHS, describing the circumstances in which it occurs, and determining the initiating and propagating events. The control measures are then identified, describing how they prevent the identified events propagating. Source terms are developed, examining possible outcomes, determining extent and severity in parallel with frequency of the various consequences. It must be shown that the hierarchy of control and relevant good practice (RGP) have been applied. When there is no RGP or standards, this involves showing the appropriate measures are present from first principles. Representative scenarios may be developed for groups of the same or very similar unit operations.
- **Assessment** – The key aspect of assessment is to assemble a site risk profile, collating the frequency of both death and serious injury for each MAHS by intuitive area. Then identify the on-site and off-site populations affected. For each MAHS determine both the number of fatalities and also serious injuries, for both the on-site and off-site populations. Identify the on-site job function, and the off-site person with the maximum cumulative risk. Finally, assess if the risk of both death and also serious injury are below the tolerability threshold. The tolerability threshold is the boundary between the tolerable and intolerable regions (see section 5, Figure 10).
- **Further measures** – Further measures are only considered when it has been established that the cumulative risk to the person from the establishment is below the tolerability threshold. If the establishment risk is intolerable then further action should be taken using the site risk profile as a guide to determine which scenarios require attention(see section 5.6.1). A 'further measure', is any additional, reasonably practicable: control, safeguard or mitigation; that has not already been implemented for that scenario; and that would lead to an additional reduction in risk, or a reduction in the number of people that would be killed or seriously injured. Operators need to identify further measures, create a shortlist, then evaluate them using cost-benefit analysis (if not immediately implemented).

If the Operator adopts all aspects of this framework and process, it is likely that the required depth, robustness and resolution will have been achieved.

The guideline highlights a range of tools and risk assessment approaches that can be used. It is the responsibility of the Operator of the establishment to ensure the tools and approaches are appropriate for their particular unit operations.

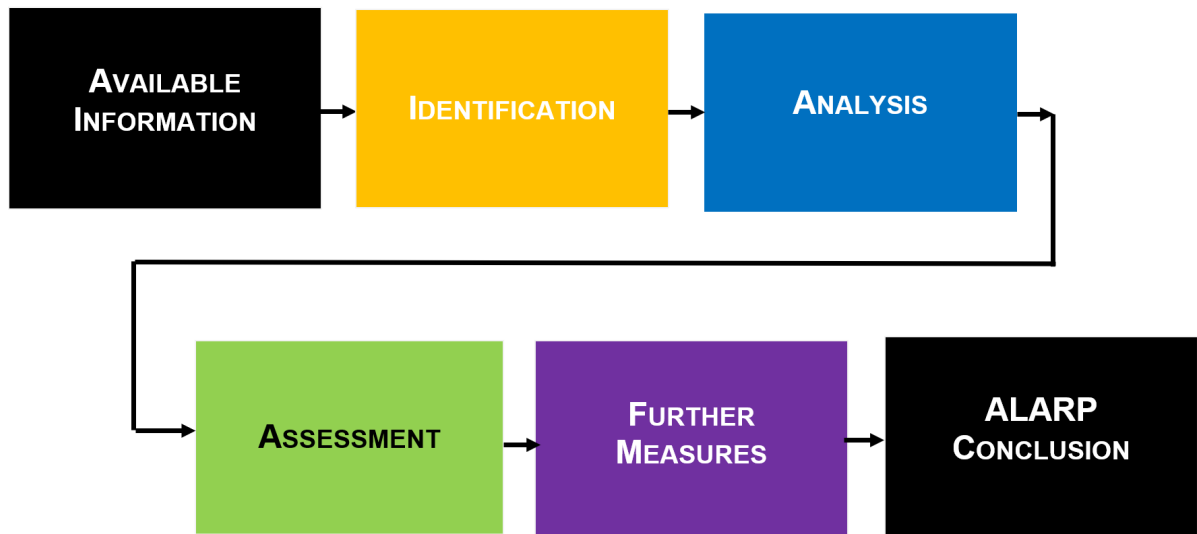
This guidance simply brings together and reconciles the existing essential principles of a suitable and sufficient MHHHRA into a single document, and includes some examples of good practice. The guidance does not contain any new or additional MHHHRA requirements.

To comply with the relevant legal duties and requirements, those undertaking MHHHRA for new COMAH establishments, or new unit operations on existing COMAH establishments; should adopt these MHHHRA principles and follow the good practice identified, or equivalent approaches that meet those principles.

For existing establishments, it is recognised that varying lengths of time will be required to fully comply with this guidance. Operators should discuss their specific case with the COMAH CA.

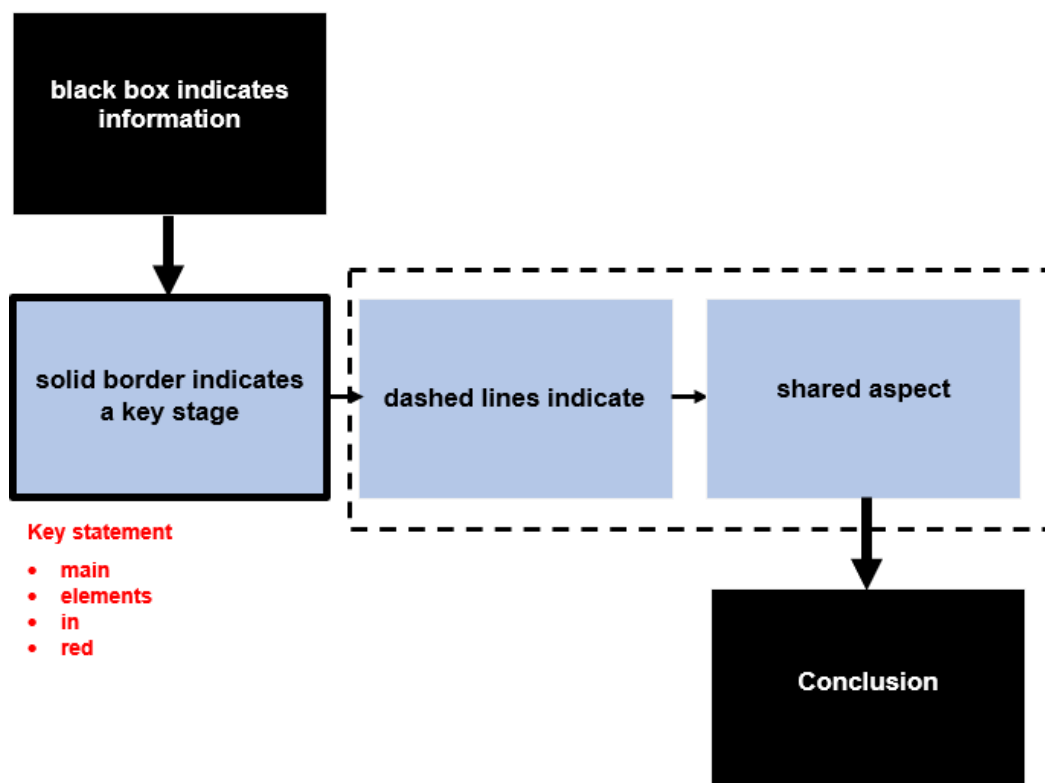
2.5 MHHHRA process flow and legend

The process flow diagram below, Flow Diagram 1, gives an overview of the MHHHRA described previously:



Flow Diagram 1 – Process Flow Overview of Key MHHHRA Stages.

Whilst the operator is free to carry out the assessment as they wish, following the prescribed order is considered the most efficient approach and should result in a suitable and sufficient risk assessment. Near the beginning of each of the main sections (Identification, Analysis, Assessment, and Further Measures) is a flow diagram outlining the key steps to be carried out for that stage. The legend for the section flow diagrams is given below in Flow Diagram 2:



Flow Diagram 2 – Illustrative Key for Section Flow Diagrams.

3. Major accident hazard scenario identification

The identification of the major accident hazard scenario or scenarios (MAHS), associated with an establishment's unit operations is a fundamental part of a 'suitable and sufficient' human harm major hazard risk assessment under COMAH and wider health and safety legislation (for example, Regulation 3 of the MHSWR). MAHS must be identified as the first step in these types of risk assessment, before MAHS analysis, assessment and consideration of further measures (**see sections 4, 5 and 6**).

This section of the guideline outlines the principles to be considered when undertaking a systematic approach to identifying the MAHS related to an establishment's unit operations (**see the process diagram below and Figure 2**). The guideline also gives some explanation of how these principles can be practically applied, with some examples. A proportionate approach should also be adopted, based on the severity of the MAHS for the unit operation and taking account of any adjustment factors. For further information on determining the proportionality of the MAHS, refer to **section 2.3**.

3.1 An overview of the key principles of a systematic MAHS identification process

The purpose of a systematic MAHS identification process is to marshal information on the hazards from each unit operation, and the populations they impact both on-site and off-site. The process aims to first identify all potential-MAHS, then narrow them down to MAHS that require further analysis and assessment (**see section 3.4**).

The starting point is to determine the extent of the study. This can be done by considering each relevant area on the establishment in turn, and then breaking it down into significant unit operations. Next, the information needed to identify all the potential-MAHS associated with those unit operations should be considered. Operators must be prepared to demonstrate that they have used relevant, current information based on their establishment. This is likely to include:

- technical information relating to the unit operations as they are currently configured, and final process design (**refer to section 3.3.1**). This is the fixed set of information related to the design of the process or unit operation used for the study. If the unit operation design, configuration or other details have changed and a new study is to be performed, this technical information will need to be updated. In this guideline, the term 'Technical Folder' is used to reference this set of information;
- information on the chemical behaviours and interactions of the dangerous substances involved (**refer to section 3.3.3**);
- establishment layout, its surroundings and relevant populations (including other COMAH establishments and environment) (**refer to section 3.3.4**);
- major accidents and incidents that have occurred on the site, within the organisation, along with incidents that have occurred around the world at similar plants (**refer to section 3.3.5**).

Using this information and outputs from 'top-down' and 'bottom-up' studies will identify all potential major accident hazards, and the circumstances that could lead to each potential-MAHS (**refer to the process flow diagram below and also to Figure 2**).

The MAHS for each unit operation are then determined by using the COMAH definition of major accident (which includes serious danger to human health and not just death) and some estimate of extent and severity (**refer to section 3.4**).

Where potential-MAHS are found not to be MAHS, for the purposes of COMAH, it is not necessary to analyse and assess the MAHS further to show that individual risk criteria have been met (**refer to section 3.4**). Noting that the more general duties under MHSWR 1999 to carry out a suitable and sufficient risk assessment, and under HSWA 1974 to reduce risks so far as is reasonably practicable remain. If a potential-MAHS is not one that could result in harm to people, it may have the potential to be a major accident to the environment (MATTE), and consequently may require analysis and evaluation under that methodology (see the CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments').

A suitable record of the findings from the MAHS screening process (and the information used to perform it) should be prepared. The MAHS identification process should be reviewed and updated as necessary, in line with the Operator's safety management system (SMS) (**see section 3.5, and section 7**).

Flow Diagram 3 below outlines the suggested MAHS Identification process.

3.2 Defining MAHS

A detailed examination of different types of scenarios, and associated sub-scenarios, is given in **section 4** of this guideline. A MAHS for most cases is a set of interacting event combinations which lead to the top event of 'loss of containment'. A Fault Tree is used in **Figure 1** below to illustrate the relationship between scenarios, sub-scenarios and their consequences. (It is not intended to indicate that a fault tree should be used to evaluate all scenarios, although it may be useful in many cases).

An Initiating Event is an 'action or failure' to danger, in a system of control or other; that starts a sequence of events that would end in the MAHS, or directly leads to it. Propagating Event is an 'action or failure' to danger, in a safety system (or other preventative barrier that is in place to stop a particular initiating event, or group of initiating events); that allows progression through a sequence that leads to the MAHS being realised. An Event Combination, is an identified combination of initiating and propagating events, that leads to the MAHS occurring.

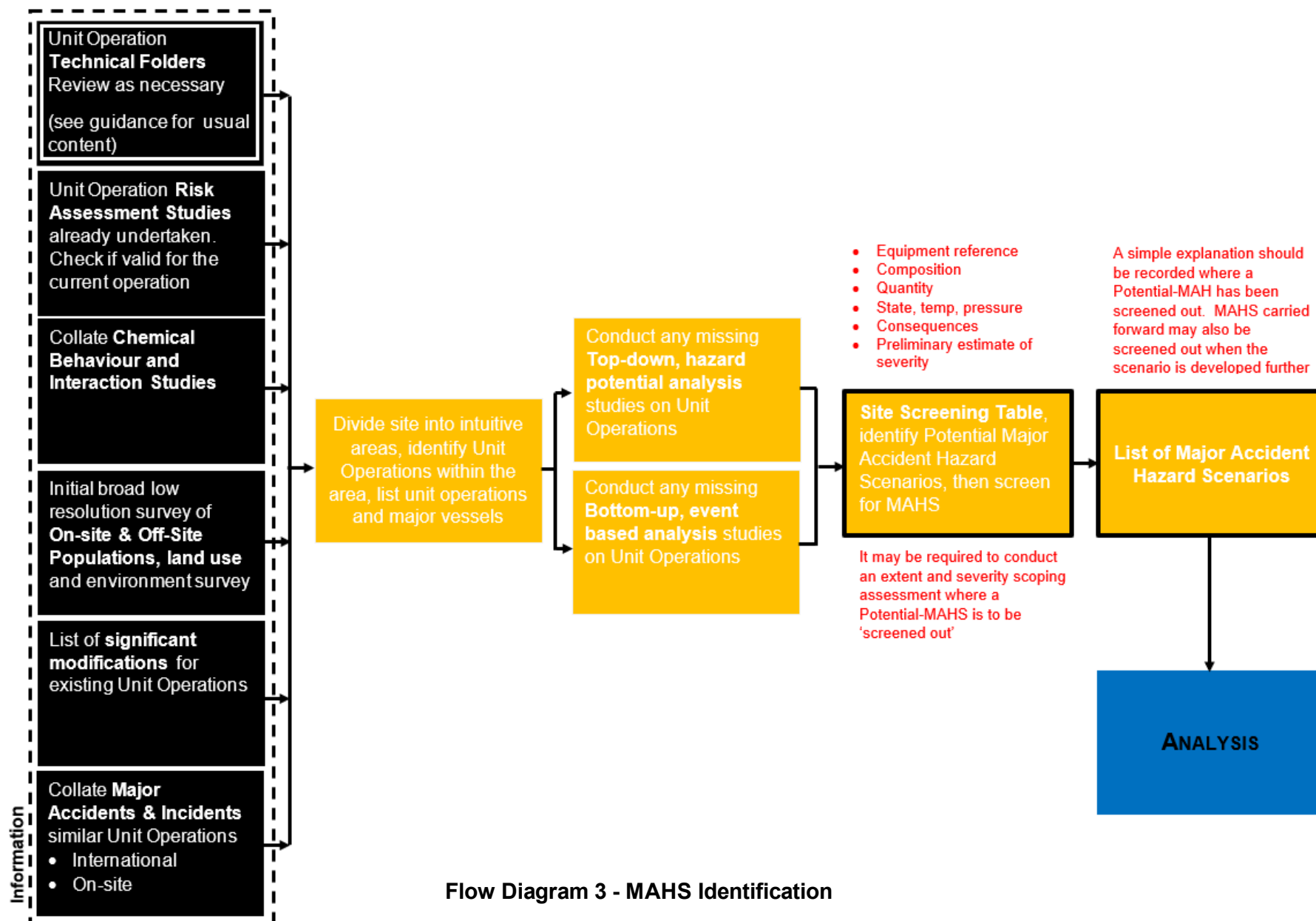
Figure 1 shows how the various sequences of event combinations lead to the top event with:

- initiating events, such as the failure of a control valve, starting the sequence;
- propagating events, such as the failure of a trip or safety system, allowing the sequence of events to continue and develop toward the top event.

Sub-scenarios may help Operators break down a more complex process into discrete parts, to simplify analysis and isolate the frequency contribution from those sub-systems to rank their importance and prioritise. These are discrete groups of initiating events forming part of the main scenario which have specific protective systems. In the example given in **Figure 1** to illustrate a scenario, a sub-scenario could be the collective failures for the distillation column reboiler system. The set of sub-scenarios may share common protective systems, such as shutting off the feed to the column, or a relief valve leading to a disposal system such as a flare stack.

The top event of the MAHS, loss of containment, will be identical for assessing both human harm and harm to the environment. The frequency at which the top event occurs can be broken down by examining the probability of different initiating causes of that release and failures in the protective systems.

IDENTIFICATION → ANALYSIS → ASSESSMENT → FURTHER MEASURES



Flow Diagram 3 - MAHS Identification

The consequence and severity of the top event can be assessed by examining the different consequence outcomes. The outcomes are determined by the hazardous properties of the dangerous substance (for example, whether it is toxic to humans, or flammable) together with its physical state. For example, it could be a liquid or a gas, with subsequent events (such as early/late/none ignition for a flammable substance), together with the quantity of the dangerous substance released, determining the consequence extent and severity. This is discussed further in **section 4, Analysis**. MAHS identification is only undertaken at a simple level. Once MAHS have been identified by screening, they are then developed separately.

The consequence of loss of containment can be developed separately to determine the harm to both people and the environment and should be brought back together when considering further measures beyond relevant good practice. At that stage, cost-benefit analysis can be performed. This is discussed further in **section 6, Further risk reduction measures**.

3.3 Identification of potential-MAHS

To produce a 'suitable and sufficient' major hazard human harm risk assessment, MAHS screening is better organised by unit operation rather than by substance. A substance may be present at hundreds of locations across a site, or within various mixtures of other related substances. Vessels may also contain several different materials or different substances at different stages of the process. Any screening arranged by substance will make it difficult to effectively relate the potential-MAHS to specific areas of plant or equipment.

This guidance is for MHHHRA, for details on screening potential-MAHS for environmental harm, please refer to the CDOIF Guideline on Environmental Risk Tolerability for COMAH Establishments.

The first step before screening for potential-MAHS involves the Operator determining the extent of the study. All the relevant areas on the establishment should be considered and then broken down into significant unit operations (which may include significant plant, storage vessels and major equipment items) for screening. If a unit operation is carried out over several vessels, each significant vessel must be screened. It should be noted that the screening process should also consider potential-MAHS which could arise during preparation of plant for maintenance, start-up and shutdown.

The precursors for screening potential major accident hazards and associated potential-MAHS are detailed and current information on chemical behaviours and interactions (**see section 3.3.3**); a detailed, current, Technical Folder (**see section 3.3.1**); and relevant establishment information (**see section 3.3.4**).

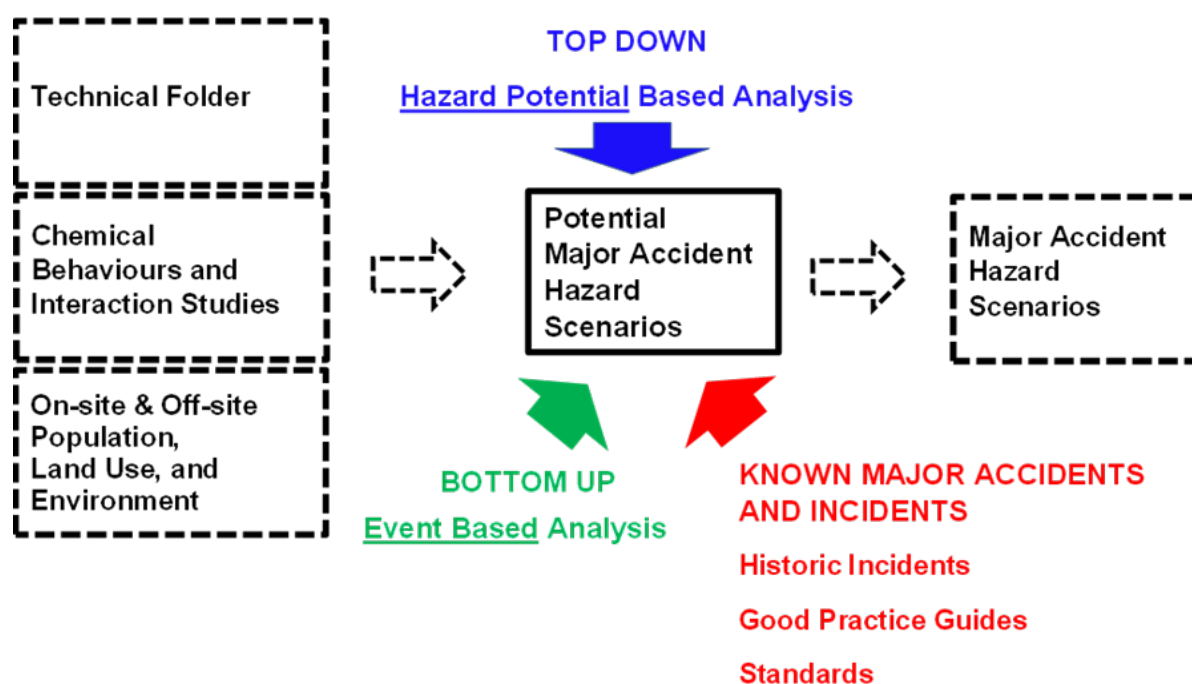


Figure 2 – Screening model for potential-MAHS.

The approach used for screening potential-MAHS should include:

- a **top-down** examination for major accident hazard potential (**see section 3.3.6**);
- a **bottom-up** examination of failures and events that could lead to a major accident hazard scenario (**see section 3.3.7**);
- consideration of **known major accidents** and incidents in similar plants, processes and unit operations (**see section 3.3.5**).

Figure 2 summarises this approach to identifying potential-MAHS. Screening operations in this way, by examining hazard potential, and considering the circumstances that could lead to each potential-MAH, will enable the potential-MAHS for each unit operation to be identified. Please note that just considering event pairs in a process hazard analysis (PHA)/process hazard review (PHR)/hazard and operability study (HAZOP) is not appropriate (**see section 4**).

In all circumstances, even for very simple unit operations, a 'bottom-up' 'guideword/deviation' based approach alone is not appropriate to produce a suitable and sufficient MHHRA. 'Bottom-up' and 'top-down' studies are complementary, and a combination of top-down and bottom-up approaches are necessary to sufficiently screen potential-MAHS. As 'top-down' studies just look at hazard potential generally rather than deviations in operation, they can identify potential-MAHS which may only result from multiple system failures. Frequently, multiple failures, especially those with low frequencies, have not been considered within 'bottom-up' studies. 'Top-down' studies should indicate the extent and severity of any potential-MAHS identified, guiding the degree of scrutiny required, particularly where no causal mechanism was found in complementary 'bottom-up' studies.

'Bottom-up' and 'top-down' studies should also be carried out separately and are most effective when conducted at different times. They are usually planned to take place at different points during the design stage. 'Top-down' studies may also be performed to complement

existing 'bottom-up' studies as part of a review in preparation for undertaking risk analysis and assessment, including when this supports the preparation of a COMAH safety report.

Sections 3.3.6 and 3.3.7 describe 'bottom-up' and 'top-down' approaches in more detail. Also included is what is normally expected to be included in 'top-down' and 'bottom-up' studies. It should be noted that there is some overlap, notably for the unit operation specific 'management failures leading to operations outside the safe operating envelope'; and the more general 'vessel manufacturing defects'. These could be included in either 'top-down' or 'bottom-up' studies to complement what has already been considered in any previous studies.

For each item, the potential-MAHS identified from both the 'top-down' and 'bottom-up' studies, and known major incidents associated with the type of equipment/process must be collated. Using a screening table to collate and summarise the potential-MAHS, and identify MAHS to be taken forward will systematically progress the identification process and provide a record that helps illustrate that all MAHS have been identified (**see section 3.4**).

Each of the key elements of the potential-MAHS screening process are considered in the sections which follow.

When relying on existing information as part of the screening process, Operators must ensure that this information is accurate, relevant and current, as process and equipment changes made subsequently may not be reflected in the original study. Existing information must be supported by a pertinent and current Technical Folder (**see section 3.3.1**) and information on the chemical behaviour and interaction studies of substances processed and/or stored at the establishment (**see section 3.3.3**).

3.3.1 Technical Folder

A Technical Folder is the collective term for the documentation used to define the design and operation, together with any supporting documents, for the particular unit operation.

A Technical Folder should be available for all unit operation(s) on the site, providing: a description of the unit operation; a detailed description of the way it is designed to function, and how it is operated currently (together with the collated changes if it differs from that specified); how the control and safety mechanisms are intended to prevent (and mitigate) the initiating event combinations that lead to the identified MAHS; and collate all the safety studies performed. This technical information should also define the Basis of Safety (BOS) and the Safe Operating Envelope (SOE).

A Technical Folder could be a stand-alone set of documentation or a collated list of hypertext links to form a defined set of documentation, such that it represents the complete, fixed, current design in operation.

Preparing a Technical Folder will evidence the input information used in the screening studies for that particular unit operation. The folder should be easier to maintain when operational changes are made, or when modifications are made. It will also make it easier to demonstrate to the COMAH CA that the appropriate information has been used.

Technical information typically required may include (but is not limited to):

- description of operational intent;
- Piping and Instrumentation Diagram (P&ID) with study boundary and nodes marked;
- Process Flow Diagram (PFD) (may not be required for simple plant displayed on a small number of P&IDs);
- equipment design parameters;

- key operating parameters, and throughputs for each element;
- Basis of Safety and Safe Operating Envelope;
- trips and interlocks - Cause and Effect Diagram and or alarm/trip chart;
- critical safety systems;
- consideration of Relevant Good Practice;
- plant layout drawings;
- information on the populations and domino installations surrounding the establishment (where relevant).

Additionally, for existing facilities, information should include:

- records of modifications;
- safety studies;
- major accident hazards identified/MAHS/analysis/assessment/individual risk;
- incidents and near miss log; and
- individual risk assessments.

3.3.2 Existing plant – use of existing studies

Existing studies may have been undertaken throughout the lifecycle of the plant unit operations (e.g. during design, operation and further development).

Where there are existing ‘top-down’ screening exercises, simply based on hazard potential, unless the size of the vessel or unit operation has increased or its operating parameters have significantly changed, these existing ‘top-down’ studies may be considered still valid.

3.3.3 Chemical behaviours and interaction studies

To inform and support the screening of whether a potential-MAHS could occur, and to assess its consequences, the properties of the materials present and their interactions must have been systematically assessed, established and understood.

Example raw material hazards include:

- **health hazard:** toxicity, mutagenicity, carcinogenicity;
- **physical hazards:** flammability, explosibility, self-reactivity, pyrophoricity, oxidising potential, autocatalytic decomposition.

Chemical interactions are examined:

- Within the intended reaction system.
- Outside the intended reaction system (also applies to plant with no intended reactions).

Example reaction hazards include:

- exothermic behaviour,
- permanent gas evolution,
- thermal instability of reactant mixtures and products,
- polymerisation,
- formation of explosive deposits,
- unintended mixing of incompatible substances.

It should be noted that the storage of substances may also require screening to identify MAHS.

A material may need to be stored in a vessel where active systems are required to keep the material within a safe operating envelope. For example, the headspace may need to be an inert gas, or oxygen; or a floating roof employed so there is no headspace.

It should be noted that sometimes for simple and/or well-established processes and unit operations, some of this information required already exists, for example, in Approved Codes of Practice and sector guidance (such as, UKLPG codes of practice — Liquid Gas UK: The trade association for the LPG and biopropane industry in the UK)³.

Guidance on the information that should be available, and depth of study expected, is summarised in **Annex 3**.

3.3.4 Establishment information

Some establishment level information is required to support the identification of potential Major Accident Hazards MAH, the subsequent screening of potential-MAHS, and then the identification of MAHS. This will include relevant information on the establishment layout, its surroundings, and also other COMAH establishments in the vicinity; together with relevant populations (to determine extent and severity).

3.3.5 Known major accidents and incidents

The process of identifying potential MAH, and potential-MAHS, should consider all ‘relevant’ historic major accidents and incidents both on-site and globally that have occurred to a similar process, process unit, operation and/or mechanisms (for example, control and mitigation measures). In this context, ‘relevant’ means carrying out the same, or similar unit operations; and/or involving the same or similar raw materials, intermediates, and finished products.

A review of incidents should include:

- accidents, incidents, and near misses that have previously occurred on the site;
- accidents and incidents in the sector, both nationally and internationally, that have been reported widely;
- accidents and incidents involving similar substances whether in the same sector or not;

³ LPG Industry Codes of Practice, Liquid Gas UK.

- failure mechanisms that are reported in sector-specific standards, relevant good practice or Approved Codes of Practice (for example, API RP 571²⁴ lists most significant chemical service induced failure mechanisms that may be encountered in refinery type unit operations).

An Operator's safety management system (SMS) should ensure that when major accidents and incidents are investigated, the root causes, as well as the immediate causes, of an incident on an establishment are determined, reported, recorded and, where necessary, acted upon. This will enable them to be considered as part of the potential-MAHS identification process. It will be helpful to collate such accidents and incidents in a summary table for future reference, which should be revised as necessary. **Annex 4** is an example of such a table. Specific mention of the relevant incident, together with any resulting safeguards, should be made when identifying potential-MAHS.

The review of incidents and accidents will need to be reactively updated; for example, after an incident on site, in the organisation or internationally. It will also need to be proactively reviewed as directed by the safety management system (SMS), for example, in line with preparation/revision of an Operator's safety report.

Other sources of information which reference major accidents or incidents are outlined in **Annex 5**.

3.3.6 Top-down studies

'Top-down' studies examine the unmitigated hazard potential of the inventory and its state, present in the unit-operation/major-vessel. This study is not about examining 'operational failures'. Such studies identify general hazard potential rather than deviations in process and plant operation.

'Top-down' studies are not dependent on knowing all modes of failure and event combinations; they are, therefore, an absolute measure of potential. If the Operator has not performed such a study for the unit operations, this should be carried out. If it is concluded from these studies that the Major Accident Hazard potential being considered cannot be realised, the rationale should be recorded. It is not sufficient to claim that these are not MAHS, or to simply apply unsupported risk assessment matrices (sometimes referred to as RAM).

It is not necessary to have carried out the 'top-down' screening study before other studies are held or collated. However, it is more efficient to carry it out first, because if an item does not have the potential for a MAHS, then for the purposes of COMAH, it is not necessary to show it has been studied further, other than to consider possible escalation. As highlighted in **section 3.4**, the further analysis and assessment of such hazards may still be required under other relevant statutory provisions.

The following aspects are often considered during 'top-down' studies:

Substance(s):

Mass/volume.

State (solid, liquid, gas).

Composition.

Physical quantity (temperature, pressure).

Properties (toxicity, flammability).

Unit operation:

Process energy input.

Reaction energy:

Chemical potential energy identified in chemical interaction studies.

3.3.7 Bottom-up studies

To identify potential-MAHS, bottom-up studies examine initiating events at the node or discrete failure level normally using a pre-determined set of guidewords. The types of studies involved include:

- Pre-HAZOP
- What-If
- Hazard and operability study (HAZOP)
- Process hazard review (PHR)
- Process hazard analysis (PHA)

It should be noted that Pre-HAZOP studies are normally only associated with early design work, and not fully developed 'frozen' designs. As a result, such approaches and other studies undertaken on early designs are unlikely to be complete for the purposes of identifying all potential-MAHS.

Other studies may include:

- identifying failures in critical mechanical systems - Failure Mode Effects and Criticality Analysis (FMECA); and
- identifying human error driven potential-MAHS - Human Task Analysis (HTA).

These studies require those involved to have the appropriate competence and also a detailed knowledge of the process, plant and operations being assessed.

It should be noted that some common deficiencies have been observed in bottom-up studies. These include:

- not grouping or summarising and collating failures into scenarios/sub-scenarios;
- inappropriately dismissing failures with multiple barriers as not credible;
- not coping well with dynamic systems; and
- inappropriately attempting to determine ALARP using isolated event pairs.

The studies performed should represent the actual unit operations present on the site, not a generic representation, nor a typical unit operation. This means that the particular unit operation at that establishment, with the specific configuration, together with the actual substance composition present must have been screened.

These studies should consider at least the following operational modes of failure where appropriate:

- service induced deterioration;
- loss of process control;

- mechanical breakdown;
- start-up/shut down induced instability;
- management system failures leading to operations outside the safe operating envelope;
- human error, either as an initiating event or a failure of a safeguard;
- vessel (or component) manufacturing defect.

3.4 Screening for MAHS

The MAHS for each unit operation are now determined by using COMAH's definition of major accident, the definition is based on 'serious danger to human health' (not just death), and also some estimate of extent and severity.

Following the identification of potential-MAHS, the MAHS for each unit operation are determined by using COMAH's definition of major accident, which refers to serious danger to human health, not just to death (see L111 A guide to the Control of Major Accident Hazards Regulations (COMAH) 2015)⁴. The use of the risk of death as a selection criterion alone is not appropriate and other criteria are needed. For example, the application of 'dangerous dose' during screening can be used to consider 'serious danger to human health'; which is a range including serious injury, long-term illness and death, and varies for different populations (see sections 4.6.1 and 4.6.2). Serious danger to the environment is considered in the CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments'.

When screening and narrowing potential-MAHS to MAHS, the likelihood and the consequence should have been estimated. This requires the Operator to carry out some work to assess hazard potential, but this should only be at scenario group level, and is only a preliminary estimate used to screen which potential-MAHS are actually MAHS. Frequency is based on any previous studies and expert judgement.

MAHS can be further broken down into sub-scenarios and events when the scenario is developed and evaluated. Remember, it is not necessary at the screening stage to develop all outcomes, only to establish potential-MAHS and MAHS. However, in some cases, if there is only a single initiating event, it may be given. The examination of all the causal events should be carried out, with the scenario analysis equating causes with measures (see section 4).

Where potential-MAHS are determined not to be MAHS for the purposes of the assessment of major hazard human harm risks for COMAH, it is not necessary to analyse and assess them further and to show that individual risk criteria have been met. However, these potential-MAHS may still need to be considered further under COMAH to determine if they are MATTE. The hazards associated with these potential-MAHS may also have to be analysed and assessed under other relevant regulatory regimes (for example, MHSWR 1999) and, when necessary, appropriate measures taken.

The MAHS identified could be further consolidated into a representative set. The process for creating a representative set is covered in **section 4** of this guideline.

⁴ COMAH, (2015) 'The Control of Major Accident Hazards Regulations 2015, Guidance on Regulations L111', 3rd edition. HSE Books.

3.4.1 Screening tables

Section 3.2 highlights that the purpose of screening for potential-MAHS is to marshal information on the hazards from each unit operation and the populations they impact on on-site and off-site, in such a way as to identify all potential-MAHS. These are then narrowed down to the actual MAHS that require further analysis and assessment.

Organising information in this way will also allow the Operator to identify where further information or study is needed, for example, if a top-down study shows potential but there is no corresponding event combination in the bottom-up studies performed. The table will show that not just 'low-frequency/high-consequence' events have been considered. Organising information in this way will also allow the Operator to demonstrate to the COMAH CA that all MAHS have been identified and that an appropriate representative set, if used, has been developed.

A screening table should allow the observer to view all scenarios in the context of their supporting information across the site. **Annex 6** gives an example of how to practically bring this information together, keeping duplication to a minimum. The goal is to lay out the collated information in a logical way that the desired audience can easily follow and understand.

Screening tables, particularly for large complex establishments, should be re-ordered as appropriate to provide as concise a representation of the potential-MAHS across the site as possible. For example, re-ordering the data may be needed when working with large electronic spreadsheets where there are many repeat entries which have been simply cut and paste without any proper structure, and every line has every entry.

Other issues to consider when producing a screening table are:

- in order to allow tracing of the MAHS through analysis and assessment, a unique reference should be provided;
- where an entry applies to a number of row entries, it may be beneficial to combine rows within that column and provide a single column entry for all the rows rather than an identical entry in each row;
- 'plant' and 'process unit' entries may be combined and used as a single entry across the entire table row; to avoid repetition for every single line item;
- some entries can be combined to be more economic for example, 'equipment number', 'equipment type' and 'equipment name'.

The basic aspects of a screening table normally include:

- equipment number,
- equipment name,
- equipment type/function,
- dangerous substance(s),
- quantity/tonnes,
- operating temperature/pressure,
- scenario/sub-scenario number,
- scenario/sub-scenario,
- outcome (worst case for screening purposes, and a range when scenario developed),

-
- consequence level,
 - likelihood,
 - potential-MAHS,
 - MAHS, and
 - representative set if used
(If entry is part of a representative set give the reference number, if the entry is not part of the representative set say which scenario represents it).

3.5 Periodic review and revision

Section 7 of this guideline outlines the general requirement that the Operator's SMS must be based on an assessment of the risk. It must also include an outline of how the Operator will identify and evaluate the potential-MAHS, before moving on to analysis, assessment then considering further measures.

For MAHS identification this may include:

- revisiting the potential-MAHS and MAHS identification process, then reviewing against the current findings, for:
 - 'management of change' (MOC) (operating parameters, operating procedures, change in throughput outside the stated operating range, plant reconfiguration, manning levels, 'creeping change' - periodic review of multiple minor changes individually not considered to warrant MOC);
 - transition of a unit operation within the plant lifecycle for example, mothballing or decommissioning; this also should consider transfer of command and control as well as change in throughput to other units);
- taking appropriate action to keep records and their analyses current (including review of assumptions that inform assessments, reports, and technical information);
- revisiting the potential Major Accident Hazards and Major Accident Hazard Scenarios identification process when new information is received, and reviewing the current findings (this includes updated information on meteorological extremes due to climate change, revised information on physical and chemical behaviour of substances processed, or new lessons from relevant major accidents and incidents).

4. Major accident hazard scenario analysis

4.1 An overview of the key principles of analysis

Analysis involves breaking down each of the defined MAHS into its component parts to examine:

- the types of MAHS and sub-scenarios, representative set if appropriate, and develop understanding of these;
- the control measures required for each scenario event combination.

Then determine:

- frequency of the MAHS top event - normally loss of containment;
- possible consequence outcomes;
- frequency of the possible outcomes;
- extent of the hazard severity for the outcomes (including ranges for the various applicable human harm criteria); and
- how the hierarchy of control and also relevant good practice (RGP), have been applied (see **section 4.10.1.**)

The analysed information can be collated into a form that allows both assessment, and the application of risk criteria, to be applied transparently. The aim is to represent not just the worst case, but to determine the range of risks from the MAHS to people so that these risks across the site are properly understood.

Analysis should be part of a targeted safety management system (SMS) that undertakes appropriate risk assessment of MAHS. This ensures appropriate control measures (and then any relevant mitigation) are in place; also that the establishments risks are below the tolerability threshold. The establishment risk profile that flows from the MHHHRA is essential to inform necessary future prioritisation and investment (for example, further measures and maintenance). This should both enhance resource prioritisation and inform investment.

The elements to be considered during analysis apply to all scenarios. The depth, resolution, and robustness of that analysis, and degree of reporting, will be determined by the proportionality of the MAHS associated with the unit operation being considered (**see section 2.3**).

In the context of this section of this guideline, analysis includes the derivation of risk and severity at the level of the 'unit operation/major equipment' scenarios identified. Assessment of the cumulative risk to the individual from the various scenarios across the site to demonstrate the residual establishment risks are below the tolerability threshold, is examined in **section 5, Major accident hazard assessment**. Residual risk is the risk remaining even after all the appropriate risk reduction measures in place have been considered.

4.1.1 Purpose of analysis

Potential-MAHS deemed to be MAHS during scenario screening (**see section 3**) are taken forward for analysis. Analysis is not simply determining 'extent and severity' together with the frequency of occurrence. It must also be demonstrated that appropriate measures have been taken to prevent or control the event combinations that lead to each MAHS. It is necessary to

relate the measures applied to the particular scenario, demonstrating how those measures prevent foreseeable operational causes

Simple tables from Process Hazard Review (PHR) and Process Hazard Analysis (PHA) [and other similar risk identification tools] supported by simple judgements are not adequate in most cases to demonstrate a suitable and sufficient MHHRA. Many different initiating events may share the same measures, so if collated separately, this could effectively result in double counting.

It is not adequate to show that a scenario frequency is below a particular threshold, such as a risk of death of 10^{-7} per year, and claim the scenario is non-credible. This is for the following reasons:

- It would be a simple matter to break down scenarios into smaller sub-scenarios until inside the risk is below the tolerability threshold; the division of a scenario should only be used as a device to enable meaningful analysis.
- Individual risk 'job function' (or hypothetical presence) requires the summation of the risk from all the scenarios to which the job function is exposed to (**see section 5**). A single scenario could appear to be below the tolerability threshold in isolation, but when added to the risk from the other scenarios the job function is exposed to, it could become intolerable.
- Most importantly, the primary focus is to reduce risks to 'as low as reasonably practicable' (ALARP); it is not the summation of risk in order to demonstrate the risk tolerability threshold has not been exceeded (**see section 5**). Relevant good practice has to be evaluated, and also further risk reduction measures need to be considered if they are deliverable and not disproportionate in terms of cost and the degree of risk reduction they provide. **Refer to section 6, Further risk reduction measures.**

COMAH Operators should note that the HSE Safety Report Assessment Manual, 2015 (SRAM)⁵ is not intended to be a guide for COMAH Operators on how to demonstrate they have undertaken a suitable and sufficient risk assessment. Sorting scenario information by SRAM assessment criteria, then collectively presenting scenario elements against the manual; is unlikely to lead to an effective analysis, assessment, and supporting argument.

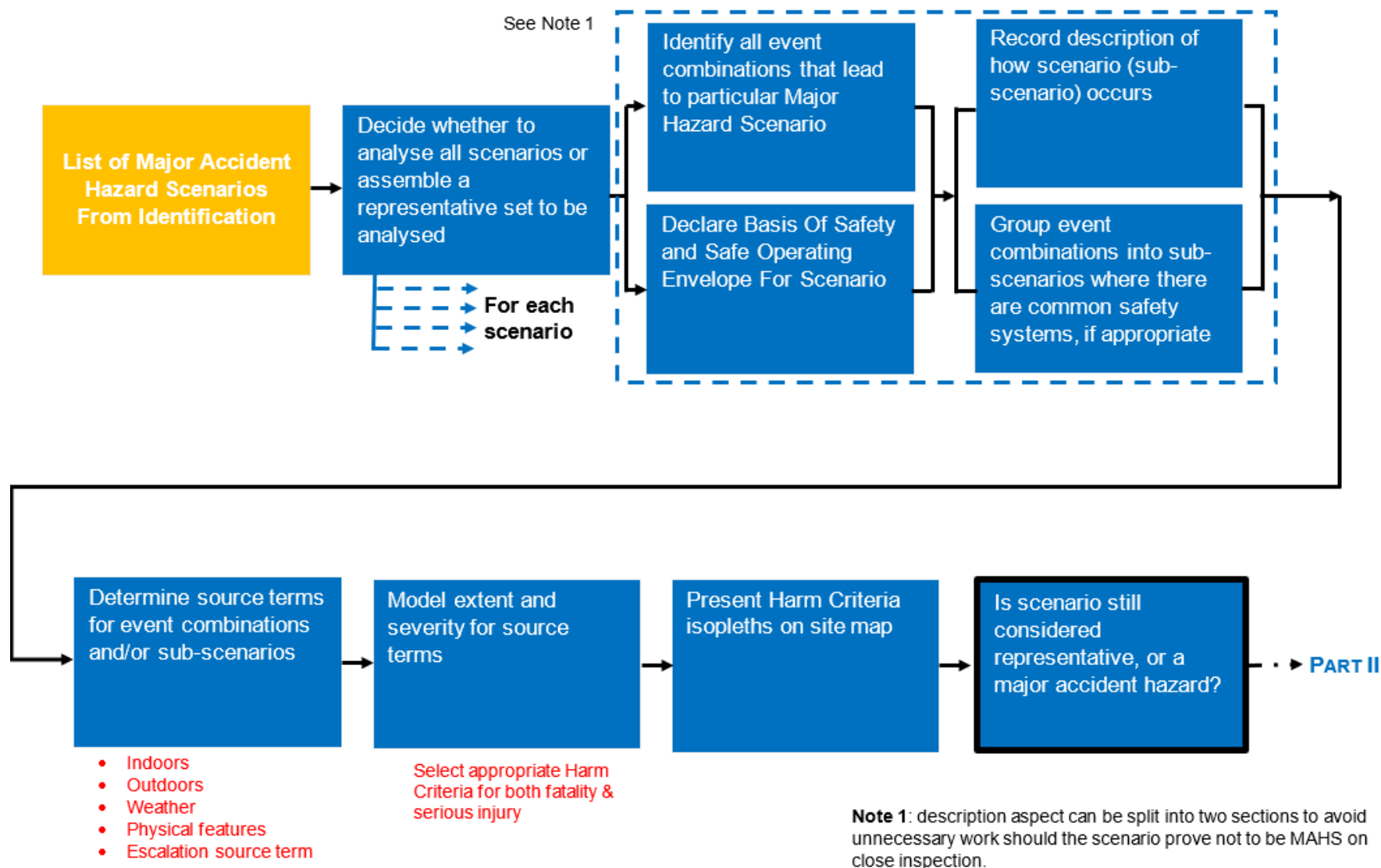
Analysis of a scenario is not always a linear process; when results or new information suggest the frequency/severity is much greater than expected, there may be an element of 'iteration and review' with increasing resolution.

The analysis needed is not just for the assessment of cumulative risk, but also to support the logical argument that is being made, such as the suitability of the representative set. One of the most important aspects is showing the link between the event combinations that lead to the MAHS, and the appropriate control measures that have been taken to prevent the scenario. Further measures, including mitigation measures to limit consequences, and how their practicability is assessed is discussed in **section 6, Further risk reduction measures.**

For information on environmental analysis, Operators should refer to the CDOIF publication: Environmental Risk Tolerability for COMAH Establishments.

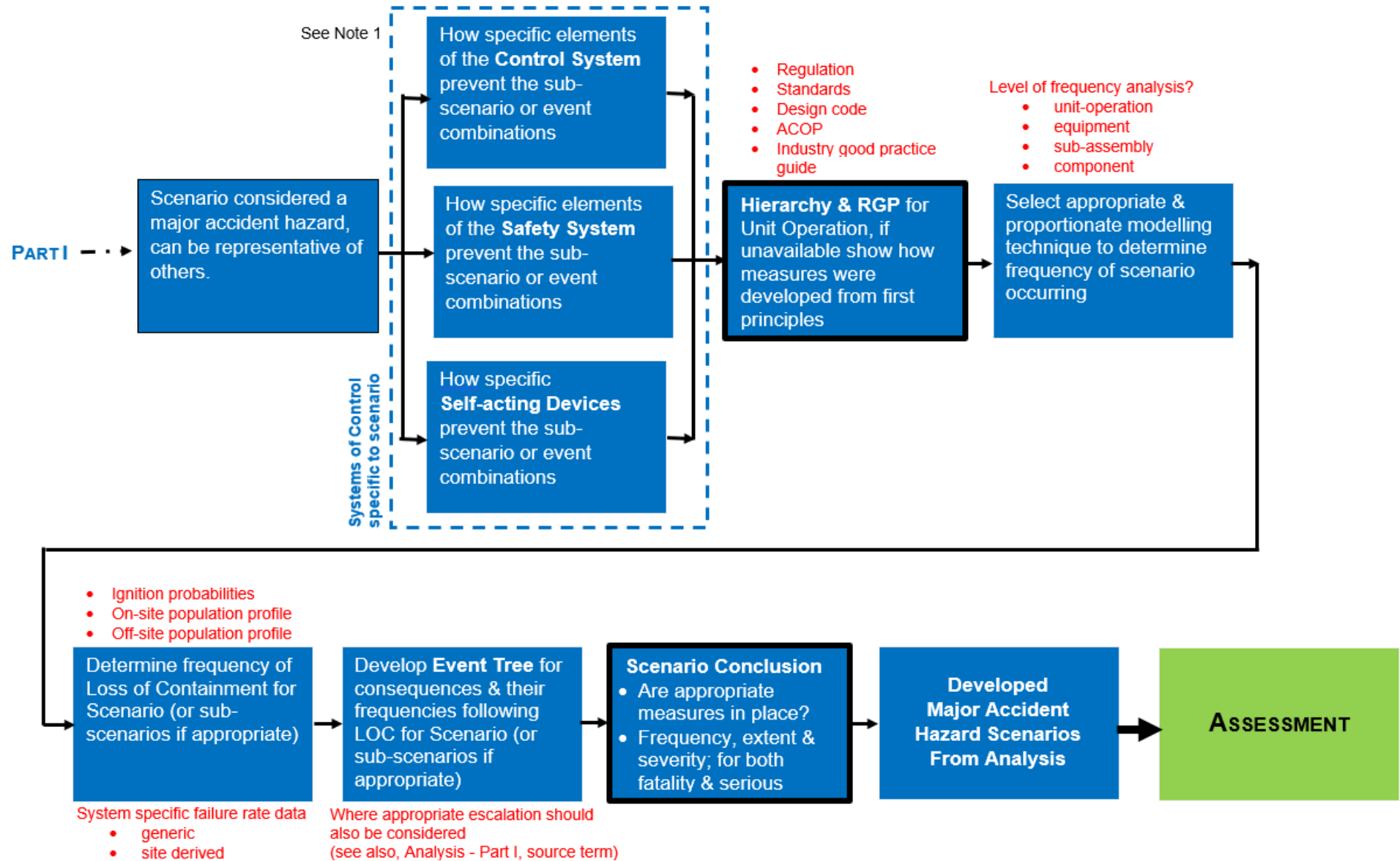
⁵ HSE, (2015) 'Safety Report Assessment Manual (SRAM)'. HSE.

IDENTIFICATION → **ANALYSIS** → ASSESSMENT → FURTHER MEASURES
PART I



Flow Diagram 4 – Analysis Part I

IDENTIFICATION → ANALYSIS → ASSESSMENT → FURTHER MEASURES
PART II



Flow Diagram 5 – Analysis Part II

4.2 Scenarios inside and outside the system

In the majority of cases, a MAHS comprises of a set of initiating and propagating event combinations which lead to a loss of containment. These initiating events can be categorised as either 'outside' the system, such as lightning or flooding, or 'inside' the system, such as loss of process control or human error (the process operator is considered part of the control system).

Scenarios are categorised in this guidance to show how best to consider the different types. Some categories are managed by general arrangements and are more easily handled by a common description of the arrangement. This description can be referred to when expanding that scenario, and just an example given to illustrate its application to the scenario. Other types of scenario, such as control failure, have particular measures for that particular unit operation and need to be described in that context.

By using the suggested convention above, descriptions of scenarios (and safety reports, when relevant) become more succinct. However, there may be some instances when particular scenarios outside the system are best considered as a specific scenario, rather than a reference to general measures, as the particular measures are specific and not widely applied.

In this context:

Inside: means everything **internal**, or contained by, or **directly connected to**, the particular system (unit operation/major vessel) being examined. A control valve failure would be a scenario inside the system.

Outside: means everything **external** to the system, including the environment in which the system sits, or is **indirectly attached** to the system. A vehicle impacting a vessel is a scenario outside the system, even though it is internal to the site, because it is external to the unit operation/major vessel being examined.

It should be noted that 'inside' does not mean everything inside the site, and 'outside' does not mean everything external to the site. Analysis of scenarios is at the unit operation/major vessel level, not at the site level. This may differ from aspects of environmental assessment. The CDOIF publication 'Environmental Risk Tolerability for COMAH Establishments' gives further information on environmental analysis.

Scenarios may not always fit into the inside or outside classification. For example, a cyber-attack could be inside or outside the system. It could result from the control system containing malicious code, or it could be input by some external agent if the appropriate precautions are not in place.

In summary:

Scenarios initiated by events 'outside' the system

Can be from:

- on-site events,
- off-site events,
- environmental events.

System scenarios initiated by events ‘inside’ the system

Can be:

- driven by random failures such as:
 - loss of process control,
 - operator error,
 - mechanical breakdown.
- driven by long-term failure to manage the system within a defined regime:
 - service-induced deterioration,
 - managed operation outside the safe operating envelope,
 - start-up/shutdown-induced instability.

(Further information on scenarios inside and outside of the system can be found in **sections 4.2.1 and 4.2.2**).

4.2.1 Scenarios outside the system

Scenarios outside the system are normally controlled and managed by ‘general arrangements’.

For example:

- structural wind loading leading to collapse is addressed by basic design specifications for buildings and installed equipment;
- lightning protection and conductors are normally addressed by relevant design codes and general site measures;
- fire systems are addressed by recognised design codes such as those from the National Fire Protection Association (NFPA).

When screening the site, scenarios outside the system may be better described and analysed collectively in their own sections (for example, flooding and lightning), which are often dealt with under general arrangements, and referred to as necessary. When screening the site, it is suggested that most scenarios outside the system can be listed in a separate site-wide general table, as the majority of significant equipment could be affected by most or all of them.

Examples of outside scenarios include:

- flooding (due to high river/sea levels or excessive local rainfall),
- earthquake,
- aircraft impact,
- vehicle impact,
- site electrical power loss from the electricity supplier, or site switching,
- external fire,

- domino (impact of scenario from another installation),
- cyber-attack (can be inside or outside the system – (see section 4.2),
- dropped load when lifting over 'active' equipment,
- vandalism by an employee or member of the public,
- vessel manufacturing defects,
- high ambient temperature and high ambient humidity,
- lightning,
- subsidence/landslip,
- high snow/rainfall,
- high wind speeds.

It should be noted that there are instances where environmental stress can become critical. This can be where insufficiently robust systems, which have limited or no-fault tolerance, have been deployed. For example, cooling water tower performance dramatically reduces in high ambient temperatures and high humidity. If cooling water supplies are critically balanced for circumstances such as exothermic batch reaction, the situation may arise where the system only remains stable provided it is not subjected to any disturbances. An increase in reaction rate, or decrease in cooling performance, may cause the reaction to 'run away'. In this case, it is not an equipment failure, but a failure in the management and design of the system. This situation is often encountered when reactors are successively added to a cooling circuit whose design is not then re-evaluated, with any factor of safety (deliberately included additional capacity to provide a margin of safety) allowed to erode.

Major accident events which are caused by natural hazards (for example, flooding, or strong winds) are classed as NaTech (natural hazards triggering technological) events. These should be considered and managed through general arrangements and separate risk assessments, which consider both impacts of such events today and under predicted climate change. Existing hazard studies may identify some of the causes/consequences of such events, which should be incorporated into the general arrangements and wider assessments, as appropriate. The CDOIF guideline, 'Adapting to climate change', outlines the requirements of sites to manage their NaTech risks.

4.2.2 Scenarios inside the system

Scenarios inside the system have initiators which are created by, or result from, failures in the unit operation/major vessel. These failures may be immediately expressed, such as failures in pressure and temperature control; or they may be created in one piece of equipment and manifest sometime later in another unit operation. For example, failure in a reaction system may lead to unreacted material inducing a hazardous chemical interaction in another unit. Scenarios inside the system are dominated by predictable combinations of random failures, and those which involve progressive degradation and require active management to keep them within their stable operating envelope.

An example of a random failure could be an actuator failed to danger. An example of progressive degradation is where a material of construction is subject to a predictable rate of corrosion, so a vessel has a thickness plus a specified corrosion allowance. The vessel is monitored to check the rate of corrosion and to establish that it has not exceeded its corrosion allowance.

Examples of inside scenarios driven by random failures include:

- loss of process control,
- operator error, and
- mechanical breakdown.

Examples of scenarios inside the system driven by long-term failure to manage the system within a defined regime include:

- service-induced deterioration,
- managed operation outside the safe operating envelope,
- start-up/shutdown-induced instability.

Similar to long-term failure scenarios outside the system described in **section 4.2.1**, there are general management controls which are better described separately when making a demonstration of a suitable and sufficient risk assessment. These are then referred to when discussing any general measures for particular scenarios. For example:

- hazardous area equipment/zoning,
- bund integrity,
- vessel inspection, and
- proof testing.

Examples of the implementation of the particular 'general control measure' should be appended and referred to as part of the demonstration; for example, a sample vessel inspection.

Software

The writing and control of software is an important aspect of control and safety systems in order to avoid systemic failures; cyber-attacks on control and safety systems are also a potential risk. It is considered that these are general measures and would be discussed in a separate part of the report and referred to where necessary.

4.2.3 Scenarios involving active management

Systems requiring active management are typified by those scenarios where materials of construction suffer from a known severe type of corrosion or cracking. This is prevented by keeping equipment within a strictly defined operating regime. Two examples of this are high temperature/pressure hydrogen heat exchangers and mild steel hydrogen fluoride alkylation units.

Example - High temperature hydrogen heat exchanger cracking

High temperature hydrogen attack (HTHA) occurs in carbon steel vessels when gaseous hydrogen is present in high concentrations and high temperatures, typically in the range of 210° to 480°C. Molecular hydrogen attacks the carbon/carbide atoms in the steel, causing erosion and deep cracking. This was exemplified by the catastrophic rupture of a heat exchanger at the Tesoro Anacortes Refinery in Washington, USA in 2010, which killed seven people. The combination of temperature and partial pressures of hydrogen

at which this occurs, are given by the 'Nelson curves' in API 941²⁵. The process must be managed to ensure operation takes place outside of the vulnerable area described by the curves.

For scenarios involving active management, a failure in the controlling management systems does not normally lead to spontaneous loss of containment, as serious corrosion/cracking does not normally occur immediately, but over time. A suitable and sufficient MHHRA should focus on describing the management measures for the system, and the long-term control and measurement of corrosion/cracking/deterioration. It should be noted that the SMS which reviews these measures, and particularly changes to inspection intervals, should also be referenced and specific examples given.

4.2.4 System scenarios driven by random failures

Random 'failures to danger' in system components are the largest group of scenarios. This includes mechanical components, such as pumps and valves; as well as electronic component failures in the logic solver and instruments of the control and safety systems. Random failures which follow a normal distribution, allow the use of reliability data to determine failure rates and to predict the likelihood of occurrence. If the failures are not random, such as may occur if equipment is purposely operated outside its design parameter, or there is an underlying wear mechanism, then other predictive approaches must be used, and so are analysed in a different way.

Example - Gas supply pressure is greater than the design pressure of a vessel

An 'initiating' event of a pressure control valve failing open allows the uncontrolled flow of gas into the vessel. If the control system pressure trip also fails, and then the subsequent separate safety system also fails. This allows the scenario to 'propagate' until the vessel relief valve set pressure is reached. If the relief valve then fails to open, this allows the pressure to rise until the vessel catastrophically fails due to overpressure. The chain of these initiating and propagating events is known as the 'event combination'.

Control systems have mechanical and electrical components, which if correctly specified and implemented have low predictable rates of failure. The combinations of known modes of failure can be determined to predict overall failure rates. Human error, while less predictable, can still be assessed, and likely rates of failure determined. If high reliance is placed on operator intervention this needs particular study, and an explanation given as to why the operation is not automated.

As stated in **section 3, Major accident hazard scenario (MAHS) identification**, a 'scenario' in this context is the top event, 'loss of containment'. A scenario is not a particular consequence, such as a vapour cloud explosion (VCE) as given in the example below; or a particular initiating event type, such as temperature sensor failure or, level control loop failure.

For a suitable and sufficient MHHRA the evaluation and demonstration of 'all measures necessary' is based on the evaluation of all event combinations and outcomes for that particular scenario.

4.2.5 Scenario and sub-scenarios

The scenario is the overall set(s) of event combinations that lead to the top event. Sub-scenarios are event combinations that share a particular set of protective measures. This subdivision enables scenario development and analysis to be simplified, indicates the importance of certain event combinations, and places emphasis on critical systems.

Figure 1, shown in **section 3**, uses a Fault Tree to illustrate the relationship between scenarios, sub-scenarios and their consequences using example 1 below. The Fault Tree is just an illustration, and not intended to imply that a Fault Tree should always be used.

Example 1: Loss of containment from a distillation column due to overpressure

Possible sub-scenarios:

- S1.1 Re-boiler system failure.
- S1.2 Re-boiler tube failure (water reactive).
- S1.3 Reflux condenser system failure.
- S1.4 Vent failure.
- S1.5 Column feed control failure.

Example 2: Loss of containment runaway exothermic reaction in a batch reactor

Possible sub-scenarios:

- S2.1 Temperature control failure.
- S2.2 Cooling water supply failure:
 - Tower (or other system) failure;
 - Fan failure,
 - Packing collapse,
 - Low cooling water level (LOC),
 - Valve closed in error,
 - Strainer blocked,
 - Demand exceeds tower capacity.
- S2.3 Quench system failure;
 - Tank level low,
 - Operator error,
 - Exotherm exceeds quench addition rate/charge,
 - Trip failure.
- S2.4 Relief failure;
 - High level in reactor,
 - Relief valve fails,
 - Dump tank unavailable.
- S2.5 Insufficient catalyst charged;
 - Concentration too low,
 - Insufficient quantity charged,

Charged too late/early,
wrong catalyst charged.

- S2.6 High reactant addition rate.
- S2.7 Under addition.
- S2.8 External heating.

4.2.6 Catastrophic vessel failure due to manufacturing or construction defect

This scenario is addressed by general measures such as management system controls utilising written inspection schemes. It is recommended that this scenario type is, therefore, treated as a site-wide topic, not repeated for each unit operation; and grouped together with scenarios that are outside the system and are also subject to a site-wide treatment (**see section 4.8.8**). With appropriate design standards and manufacturing assurance, generic failure rates can be used. It is suggested that this is not evaluated together with operational causes of catastrophic failure. The emphasis should be on having appropriate management systems in place and ensuring inspection intervals are not overridden without due consideration. For specialised bespoke vessels that are not designed to a specific detailed code but more general standards, for example, when considering a 50 000 tonne cryogenic liquid ethane tank, it would be expected that catastrophic failure is explored in detail.

4.3 Representative scenario set(s)

Following screening there may be a large number of MAHS identified across the site. These should all be separately developed to account for differences in each, noting that different unit operations may have very different initiating and propagating events. However, for establishments which have multiple identical streams/systems, or many near identical unit operations, provided there is parity, it can be reasonable to group these similar major pieces of equipment or unit operations. One piece of equipment or unit operation can be developed to represent the other members. 'Representative' means that it represents the whole of that unit operation or major piece of equipment, its initiating and propagating events, and evaluates all consequences.

Adopting a representative set can significantly reduce the analysis required, and the amount of information needed to demonstrate a suitable and sufficient risk assessment. Operators need to recognise that risk assessment is an iterative process; it may be that some unit operation MAHS are found to be no longer representative after further analysis, and that these scenarios will need to be developed further. Some of the issues to take into account when considering a representative set are outlined below.

Multiple identical unit operations

Where there are multiple identical unit operations, the associated scenarios for loss of containment in one can be used to represent all identical units. However, where identical units are dispersed across a site, thought may need to be given to their location as the extent and severity could differ. This could be addressed by developing different outcomes for the representative unit.

Identical unit operations with different operating conditions

The Operator may have many distillation columns operating at different pressures. In decreasing order of risk, these would be operating:

- at high pressure;
- around atmospheric pressure;
- under vacuum.

The Operator could take the example with the greatest risk of serious danger and use it to represent all the other columns. However, using the example with the greatest risk of serious danger could lead to a falsely high individual risk, as they may be exposed to the risk from multiple columns that have all been given the highest extent and severity. In this case, the resolution could be increased by having a representative scenario for particular ranges of distillation column operating pressure.

Similar unit operations

Many operations may use very similar variants at similar temperatures and pressures. If their control regime, scale and mode of operation, are sufficiently similar such as hydrocracking and hydrotreating, the same exemplar could be used for both. For example, catalytic hydrocracker/ hydrotreater.

Batch reaction systems

A reactor module for toll manufacture may be used for a number of different reactions. In this case, it is acceptable if representative scenarios are assembled for specific ranges of types of reactions within a defined boundary; (for example, acetylation, transesterification, Grignard reaction, oligomerisation). It would be expected that any supporting work (for example, a chemicals behaviours and interactions study) would have been undertaken during the development stage.

Large complex establishments

A representative set for each of the main process units will be required for a complex establishment with a large number of MAHS (for example, refineries or large establishments carrying out multiple refinery operations). For other bulk commodity refinery scale processing, it would also be expected that a representative set is provided for each of the main process units and major vessels.

Many complex process units have a variety of sub-units which carry out multiple unit operations. It should be noted that there should be a representative set or specific complete set for each of the main process units where a MAHS has been identified in the site screening.

It must be clear which unit operations, discrete vessels, and systems, the scenario is actually representative of. This linkage should be readily discernible and capable of audit, by being listed, cross-referenced or tabulated.

If processing conditions and the dangerous substances involved are significantly different, then using a common representative must be explicitly justified.

Evaluation of a single initiating event or single consequence from a scenario, where there are multiple initiating events and consequences, would not be considered a complete scenario development.

Examples of main process units that should have their own representative sets are:

- Fluidised Bed Catalytic Cracker Unit - reactor, catalyst regenerator, separator/stripper, electrostatic precipitator, primary fractionator
- Continuous Catalytic Reformer Unit - catalytic reactor, heat exchangers, stabiliser columns, regenerator tower, transfer train, compressor train

4.3.1 What is not considered to be a representative scenario set?

Selecting exemplar events, consequences and scenario types from a list of categories (non-unit operation related) is not sufficient to produce a representative set. An example of such a list is:

- substance category - toxic, flammable, oxidising;
- consequence type – vapour cloud explosion (VCE), flash fire, pool fire;
- environmental receptor – aquifer, river, air;
- initiating event type – cold catastrophic failure, overflow;
- a human factors initiated scenario;
- equipment type – continuous, batch;
- release size – large, medium, small.

The use of 'selection criteria' such as those above can lead to a variety or collection of scenarios, not a set of scenarios that represent all the unit operations present.

4.3.2 What is not considered to be a representative scenario?

The following would not be considered a representative scenario:

- consideration of only a consequence or part of the scenario;
- formation of scenarios by combining parts of non-related unit operations;
- common unit operation carried out by dissimilar systems;
- where complexity is the only representative feature;
- use of a generic or theoretical example that does not exist at the site.

Consideration of only a consequence or part of a scenario

As an example, the boiling liquid expanding vapour explosion (BLEVE) of a butane sphere is a single consequence and not a full scenario for the unit operation. On its own, it does not consider the specific initiating and propagating event(s) such as a local leak or dewatering. This may result in a pool or jet fire, which subsequently escalates to a BLEVE. If only BLEVE is evaluated, this would ignore the other sub-scenarios that could lead to loss of containment; and therefore underestimate the frequency of fatality, or serious injury.

Other possible sub-scenarios or initiating events leading to overpressure and loss of containment from a butane sphere could include:

- overfill - level control failure, vessel overfilled in error;
- mischarge - vessel filled with propane in error;
- nitrogen breakthrough from hydrogen fluoride alkylation plant;
- rundown containing high level of propane;
- leakage - from flange, or local pipework.

The scenarios should include development of all sub-scenarios and event combinations that lead to loss of containment.

Formation of scenarios by combining parts of non-related unit operations

Sub-scenarios are groups of initiating and propagating events related by sharing the same protective measures and the same top event. Sub-scenarios from different unit operations, parts of different scenarios or discrete failures; cannot be used as available 'representative parts' from which to assemble other scenarios, for different: unit operations, substances, temperatures and pressures. For example, a level control system in one unit operation may operate in a different way, using different equipment, and suffer from different initiating and propagating events.

Common unit operation carried out by dissimilar systems

There may be many different types of storage tank, such as pressurised spheres, pressurised cylindrical tanks, floating roof tanks, and fixed roof tanks. These may be filled from a variety of sources, including ship, pipeline or road tanker. These storage tanks may also contain a wide variety of dangerous substances from pressurised gases, liquified gases and flammable gases.

It would be expected that a representative would be chosen for each type of tank as they have different failure modes. It may also be necessary to further differentiate by either having separate scenarios for particular duties or where there are known special cases. For example, a floating roof tank filled with petroleum at high flow rates from a ship, where overfill is likely to lead to the formation of a large flammable vapour cloud. If the same tank is used to store a wide variety of dangerous substances, the scenario can be developed, and the top event frequency calculated. The extent and severity can then be determined for the different categories of materials stored within it – flammable, toxic, hazardous to the environment.

Similar complexity alone

A similar operation would process similar dangerous substances, at similar temperatures and pressures, with similar control loops and safety systems. A unit which possesses similar complexity only, but not the similar substance or process conditions, would not allow it to be represented by the same scenario.

Use of a generic example

The representative member for the group must be a complete installation that exists at that site (or will exist if for a modification, or new installation). It must not be assembled from parts of the other process units in the same representative set to create a typical process unit that represents them all. If the operation of the other members of the set differ to the point where the frequency of the top event is greater, further modified scenarios will be required.

4.4 Scenario development

In order to make a structured demonstration, that 'all measures necessary' have been taken to prevent and mitigate the MAHS, the Operator must make the link between the following:

- the context in which the MAHS occurs,
- the event combinations that lead to the MAHS,
- the particular measures taken to prevent and stop the propagation of the event combinations identified for the MAHS.

The outline below provides a suggested format for the development of each scenario; this is effective for the majority of cases. It is suggested that they are developed in this order, as the consequence and severity determine the proportionality of the assessment:

1. **Scenario description**
2. **Basis of safety and safe operating envelope**
3. **Consequence extent and severity assessment**
4. **Consequence map**
5. **Scenario control measures**
6. **Scenario frequency quantification**
7. **Gap analysis**
8. **Additional information**
9. **Conclusion**

The content and depth, resolution and robustness of analysis required will be determined by the proportionality of the MAHS associated with the unit operation being considered (**see section 2.3**).

It should be noted that it is not sufficient to simply describe the control measures out of context, or collectively with other unconnected scenarios.

4.4.1 Scenario description

The scenario description should contain the following:

- the outline description for the MAHS or scenario group,
- any included sub-scenarios (refer to **section 4.2.5**),
- critical process parameters.

This should be an outline description of the scenario to allow the elements of the analysis to be put into context. Links to the process description and any specific management systems should be provided. It may be a few lines of description for a simple failure or a few paragraphs for a large unit operation.

Including a process drawing(s) is an effective tool to show exactly what is included. It is suggested that this is added as a scenario specific appendix at the end of the section. This

will be important for large complex processes with diffuse battery limits. For a simple system with a single fill and discharge, this is not essential. But where the vessel/equipment is linked to other equipment such that loss of containment will allow the system to disburden through the failed vessel/equipment, this should also be shown.

A diagram should be included which shows principal control systems, safety systems and self-acting devices. The relative position of sensors and actuators should be clear. The layer of protection the element belongs to (control system or safety system or self-acting device) should be differentiated by symbol, tag, and ideally colour. For simple systems, this could be a scrap view taken from an Engineering Flow Diagram (EFD), Process Flow Diagram (PFD) or Piping and Instrumentation Diagram (P&ID), or similar. For larger systems, reference to an appended drawing may also be required. The actual unit which is represented by the scenario must be illustrated and developed, not a 'typical' system which combines aspects of differing members of the group the scenario represents.

4.5 Scenario basis of safety and safe operating envelope

The Basis of Safety (BOS) is a simple statement that captures the principal design intent. The Safe Operating Envelope (SOE) defines the operational envelope within which the process must be maintained in order for it to operate in a safe, stable state.

4.5.1 Basis of Safety

The BOS informs the degree of inherent safety and fault tolerance in the safe operating envelope. Without a stated BOS and defined SOE, it is difficult to show that the systems of control and safety are adequate, such that it can be demonstrated that all measures necessary have been taken, and therefore the risks from the process are ALARP. It should be noted that the Operator would be expected to have already considered the hierarchy of control measures during design.

Examples of BOS include:

- total containment;
- control and relief;
- control, relief and disposal (flare, dump tank, neutralisation, or other);
- control and high integrity protection systems (HIPS); and
- control, quench, and relief.

'Total containment' is a phrase used to describe a system that is constructed in such a way that it can withstand all MAHS without losing containment. In its simplest form it could be a pressure vessel that is constructed with a wall thickness, piping, and valves; specified to withstand the maximum temperature and pressure that would result from any MAHS identified. There are usually also some simple safety systems in place to avoid placing unnecessary stress on the vessel.

4.5.2 Safe operating envelope

The SOE should be defined, for one degree of freedom, for all critical operating parameters for that scenario. For example, level range, pressure range, temperature range. It is possible to define an operating envelope using multiple degrees of freedom, but this requires very complex numerical analysis, as the number of permutations under which the process can operate safely increases. This can be complex for batch processes where there may be a large number of variables, refer to **Annex 7** for further information.

Preconditions

The SOE must include any required preconditions for safe operation. For example, a relief system may require a certain vessel headspace to allow for level swell and/or dis-entrainment. This would mean that the vessel must be kept below a certain level in order for the relief system to be effective. Therefore, if its BOS is control and relief, then it must have measures to ensure its level is maintained below the point at which the relief system will not be effective; so this must be part of the SOE.

4.6 Scenario consequence extent and severity assessment

For each MAHS, the possible outcomes following loss of containment are identified, and the consequences determined:

Outcomes may include:

- toxic release,
- pool fire,
- flash fire,
- BLEVE,
- Fireball,
- jet fire,
- vapour cloud explosion (confined/congested),
- warehouse fire involving toxics solids, or
- missiles (equipment fragments).

The distance from the loss of containment to the appropriate specified harm criteria is calculated (**see Annexes 8, 9 and 10**). Harm could be in the form of:

- thermal dose;
- overpressure/blast/impulse (primary, secondary and tertiary);
- toxic dose by inhalation (by ingestion is not normally considered);
- missile impact; or
- single dose carcinogen, where appropriate.

This may be dealt with by taking the largest source term, or breaking down the consequences by sub-scenario. This may be necessary if there are frequent sub-scenarios with much lower extent and severity.

An effective way to assess and present the consequence assessment is as a part of each particular scenario development, rather than examining all the consequences from all the MAH scenarios in another section in the report. This is beneficial when there are many scenarios and substances to consider.

Confirmation that Potential-MAHS are MAHS

Following the determination of extent and severity, the Operator is advised to confirm that the potential-MAHS still meets the criteria for a MAHS. This is to avoid unnecessary work in developing scenarios that are not MAHS. If it is found that the MAHS no longer meets the criteria, this may require the representative set to be reconsidered.

Harm criteria

When determining the effects on people, examining the intensity of exposure (flux, concentration) alone is not sufficient. The time people are exposed is also required in order to determine 'dose', a function of exposure and time.

$$\text{Toxic dose} = c^n \cdot t \quad \text{ppm}^n \cdot \text{min} \quad c \text{ concentration ppm}$$

$$\text{Thermal dose} = I^{4/3} \cdot t \quad \text{kW}^{4/3} \cdot \text{m}^{-2/3} \cdot \text{s} \quad I \text{ thermal flux kWm}^{-2}$$

When calculating thermal dose, the time exposed should consider the time to escape to an appropriate place of refuge, or where there is no further significant accumulation of radiation.

Where people are subject to overpressure, the effect on any occupied structures may lead to additional harm and must therefore, also be taken into consideration. Guidance is available in the publication by the Chemical Industries Association (CIA) 'Guidance for the location and design of occupied buildings on chemical manufacturing and similar major hazard sites'⁶.

Toxic exposure to people in buildings is accounted for in the modelling software not by separate criteria **see also section 4.6.4 and Annex 10**.

Harm criteria used should be sufficiently sensitive to calculate both fatality and serious injury, for both on-site and off-site populations. To evaluate serious injuries, Operators will need to make judgements on the range of harm that constitutes serious danger to human health (COMAH guidance L111 defines this as: "a substantial number requiring medical attention or some people seriously injured, requiring prolonged treatment").

The HSE's suggested criteria for toxic exposure, thermal exposure and overpressure are available in **Annexes 8 to 10**. The criteria must relate to both fatality and serious danger. The use of 'dangerous dose' is able to give sufficient sensitivity so the number of serious injuries (and deaths for the off-site population) can be determined for different groups of the population.

4.6.1 On-site population determination of death and serious injury

Fatality

A pragmatic estimate for the dose that will lead to a fatality for a working population of normal distribution can be taken by assuming that receiving a dose above the LD₅₀ (also known as the value for the significant likelihood of death, SLOD) results in fatality.

Serious injury

A dangerous dose is a level of harm, that can be differentiated for different parts of the population. For the working population of normal distribution (assumed to be aged between 18 to 65, male or female), the least susceptible group, a dangerous dose is considered to give rise to serious injury.

⁶ CIA, (2020) 'Guidance for the location and design of occupied buildings on chemical manufacturing and similar major hazard sites', 4th edition. Chemical Industries Association (CIA).

4.6.2 Off-site population determination of death and serious injury

Unlike the on-site population, those present off-site are not just of working age, but may comprise young, old, vulnerable and sensitive.

A dangerous dose would lead to 33% of the normal population being fatally injured, with the remainder being seriously injured; 100% of any vulnerable or sensitive population would be fatally injured.

Noting that dangerous dose is not sensitive enough to determine risk of death (ROD) for populations solely comprising those of working age.

For further details of fatality, serious injury and dangerous dose, in relation to on and off-site populations, **see sections 5.3 and 5.4.**

For suggested harm criteria values, see the following annexes at the end of this document:

Annex 8 Suggested criteria to determine harm to the person from thermal radiation.

Annex 9 Suggested criteria to determine harm to the person from exposure to toxic gases and vapours.

Annex 10 Suggested criteria to determine harm to the person from overpressure (and impulse).

Criteria should be appropriate to the population at risk

It should be noted that offshore indicative criteria for human health given in the document 'SPC/Tech/OSD/30 – Indicative human vulnerability to the hazardous agents present offshore for application in risk assessment of major accidents'⁷ and 'Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment'⁸ are not suitable for onshore assessment. This is because they are based solely on the population of working age found offshore, and do not include the full breadth of the general population (old, young, sensitive and vulnerable). The criteria given in these documents are also based on fatality, not serious danger (as defined for a MAHS). Many criteria such as thermal harm do not consider 'dose' but only incident flux, so do not account for cumulative exposure during escape. The criteria also do not have sufficient resolution as they are intended for a different regulatory regime.

The harm criteria used should consider the characteristics of particular population(s) present, and be adjusted as appropriate. For example, females have statistically thinner skin and are, therefore, more sensitive to thermal radiation. The general off-site population should be considered to be commensurate with a normal population distribution. However, particularly sensitive or vulnerable populations identified (schools, hospitals, care homes, and the like) should be differentiated.

⁷ HSE, (2013) 'SPC/Tech/OSD/30 - Indicative human vulnerability to the hazardous agents present offshore for application in risk assessment of major accidents'. HSE.

⁸ HSE, (2013) 'Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment'. HSE.

4.6.3 Source terms

The source terms used must represent the condition at the moment of release/catastrophic failure. This may be significantly different to that during normal operation; for example, if a vessel has been subject to overfill or overpressure.

Source term parameters normally include:

- release rate (or instantaneous loss),
- total mass/volume released,
- release duration,
- temperature,
- pressure, and
- composition.

So that the risks are properly represented, source terms used should be as representative as possible, not just a crude worst case. There may be two cases, one with effective isolation, and one without.

Catastrophic failure

The definition of catastrophic failure used to establish the source term should be given in the analysis. For a single discrete vessel, this will normally be instantaneous loss of the entire inventory.

Where multiple vessels are interconnected, this will normally be represented as immediate loss of the entire joint inventory over a few seconds.

Where inventory loss is deemed to be limited by isolation arrangements, these must be shown to be sufficiently robust; considering both how the failure is revealed, how actuation is reliably achieved, and the time to act.

The ability of any bund to retain the material should be examined, this includes bund integrity and overtopping.

Isolation

If isolation is used to limit the source term, then its reliability must be used to modify the failure frequency such that there will be a case with, and without, isolation. The unmitigated case cannot be dismissed because the frequency is low. In addition, the time to isolate must also be considered, comparing the time to act with the time for the failure to develop.

Isolation could be carried out by the control or safety system(s), be automatic, automated or rely on direct manual intervention. Isolation must be timely and achievable without the operator being further exposed to harm. The system used to make the isolation should be described and failure to isolate included. If isolation is initiated manually by the operator remotely, the point from which the isolation is made must be outside the hazard range for significant injury, and the failure to make the isolation included in any frequency calculation. If credit is taken for isolation using a hand valve, a detailed description of how this system of isolation can be effectively and safely undertaken should be included.

If broad assumptions are made, they are required to be fully justified. For example, if it is claimed that catastrophic failure is limited to loss of material from the largest nozzle, rather than complete vessel failure, this needs a detailed explanation.

Overpressure and loss of containment

The source term, amount of material released, and physical state at loss of containment is often dependent on the pressure at which the system fails. It is sometimes claimed that a relief path (such as gasket failure) will be found before the design pressure is reached or that a vessel will not fail until it has reached many times its design pressure.

Noting that design pressure, is the set pressure plus allowable accumulation under the code. For all cases where any credit, numerical or descriptive, has been taken for a pressure systems ability to exceed more than 1.1 x design pressure: the common arguments below are not normally appropriate unless a detailed case is presented to demonstrate its validity.

Some common arguments/assertions are:

- The smallest pipework or gaskets fail first, allowing sufficient pressure relief.
- Maximum pressure that the system can withstand for short periods is equal to the hydraulic test pressure. *Inappropriate unless the hydraulic/pressure test was performed and held at the operating temperature.*
- 1.5 times or 2.5 times the MAWP is allowable (Centre for Chemical Process Safety, 'CCPS'). *To be valid this would require a detailed analysis to justify the system does not fail.*
- Overpressure is less than the material yield point. *To be valid this would require a detailed analysis and consideration of stress raisers and operating conditions to have been made.*
- A relief valve or bursting disc is present. *To be valid it would need to be shown, or stated to be, that it is sized for the scenario it is being claimed to prevent (including the vent line and any attached disposal system).*
- The operator will open a hand valve. *To be valid the failure would need to be directly revealed, and shown that there is sufficient time for recovery. It would also require a detailed human task analysis (HTA).*

Noting that the exception is where the maximum overpressure conditions are commensurate with hydraulic test conditions under the appropriate standard (often 1.5 x maximum allowable working pressure (MAWP) at ambient temperature.

Design codes have built-in factors of safety which allow a range of vessels and pipework to be constructed, within a range of configurations, and still operate safely. There are often factors that considerably raise stress, such as vessel supports, manways, branches, ladders, and body flanges; these are accommodated by those factors of safety. If the MAWP is to be exceeded by more than that allowed by the design code at the specified temperature of operation, then a detailed stress calculation carried out by a competent person is required.

4.6.4 Modelling and calculations

Extent and severity are normally determined using proprietary software (for example, Phast™). Modelling approaches should be based on established, peer reviewed methodologies, and use validated models, together with associated physical property libraries. The Operator should provide the input data sets and outputs from the model used, presenting them in a summary table, where appropriate. Details of the software package used should be provided in the report in a general section. Where bespoke modelling approaches have been used, full details should be included or appended. Closed approaches should not be used; the regulator must have sufficient information to be able to recreate and test the analysis.

Weather/external conditions

Modelling will require consideration of the meteorological conditions both during the day and at night, together with the general topography. The parameters selected must be representative of the site. Operators should ensure that the weather station data selected represents the weather conditions for the site.

People in buildings or refuges

Exposure to substances toxic by inhalation is changed by being in a building. This is normally accounted for in the modelling software by adjusting the rate of ingress in proportion to the estimated number of air changes per hour. If credit is taken for the building being classed as a refuge, and the building is purged or sealed on detection, then this must be described in the scenario; and a probability for failure to detect the toxic release, and failure to prevent ingress included. If credit is taken for escape to the refuge, this should also be accounted for. It is not appropriate to assume a person can escape from an open area to the refuge with zero exposure.

Where a building may be subject to explosion blast, this may increase the likelihood of fatality or serious injury due to collapse. See **Annex 10** for Harm criteria, and further guidance.

Ignition probability

For flammable releases, ignition probability may have a profound effect on the extent of the risk isopleth. For a volatile evaporating liquid, early ignition may result in a pool fire, whereas delayed ignition could lead to a vapour cloud explosion (VCE). If delayed further until the cloud is dispersed below the lower flammable limit (LFL), this results in a very limited hazardous consequence. For materials that are both flammable and toxic, the toxicity may be such that the hazard range goes beyond $\frac{1}{2}$ LFL, so that delayed or no ignition gives rise to a much greater hazard range.

The probability of ignition should be justified, particularly when subdivided into 'early', 'late' and 'very late'/'no ignition'. The presence of high energy ignition sources within LFL should also be considered as this has a high probability of immediate ignition. However, if the materials are flammable and very toxic, some sensitivity analysis may be required.

4.6.5 Extent and severity table

The results of the extent and severity calculations should be summarised in an appropriate table.

Jet Fire hazard ranges							
F2 weather conditions							
Angle from horizontal (deg)	Release rate (kg/s)	Flame length (m)	Distance (m) to jet fire radiation (TDU)			Distance to LFL (m)	Flash fire envelope at LFL/2 (m)
			1800	1000	500		
0	297	228	325	290	255	321	631
30	297	201	240	190	-	-	-
60	297	175	170	81	-	-	-
90	297	148	115	40	-	-	-
D5 weather conditions							
Angle from horizontal (deg)	Release rate (kg/s)	Flame length (m)	Distance (m) to jet fire radiation (TDU)			Distance to LFL (m)	Flash fire envelope at LFL/2 (m)
			1800	1000	500		
0	297	188	282	253	218	358	720
30		30	297	175	8	-	-
60	297	144	171	111	-	-	-
90	297	122	114	53	-	-	-

Figure 3 – Example extent and severity table.

4.6.6 Consequence map

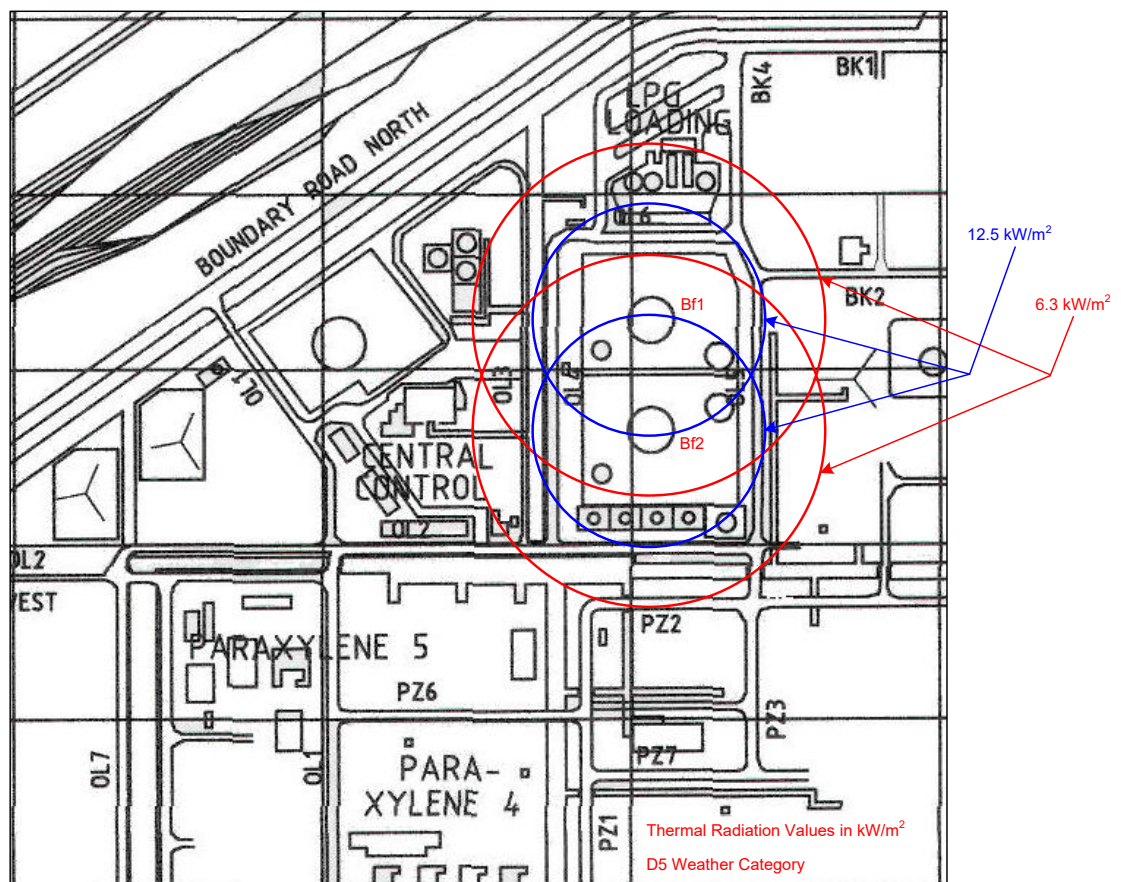


Figure 4 – Example scenario consequence map.

The location of the scenario should be shown on a site layout drawing, or a map(s) of a suitable scale, together with the hazard isopleths (a line connecting equal values) showing the extent for each consequence criteria. Normally, this will be the dose values for fatality and serious injury (SLOD and dangerous dose respectively). This is in order to allow cross referencing of the hazard range with the area in which a job function occurs. Where a threshold is relied on such as LFL and $\frac{1}{2}$ LFL for a flash fire, or the flux level at which a person will no longer accumulate further significant amounts of thermal radiation, 6.3 kW/m², this should also be shown.

Escalation

Equipment which is within the hazard range and therefore may lead to further loss of containment and escalation should be considered. For example, when examining the consequence of a loss of containment beneath a Butane Storage Sphere in a tank farm:

- would the thermal radiation from a BLEVE or pool fire be sufficient to cause the other spheres to lose containment, or even escalate to surrounding plant?
- how far are the other spheres away?
- what is done in mitigation, will the deluge system on the other spheres be triggered as soon as a fire under one of the vessel group occurs?

4.6.7 Emergency planning

When considering emergency planning, including the siting of incident control rooms and the populations affected, the greatest extent and severity will need to be considered. These may not be represented by the scenario as developed, as the worst possible case may not be considered credible or representative. This may require further analysis for dominant scenarios. Incident control rooms should be located considering the worst possible cases.

4.7 Scenario control measures

The measures that prevent and control a particular scenario should be described. This may be on the basis of the scenario, or for each sub-scenario.

A control measure in this context does not just apply to the control system, but any system, such as a procedure using human intervention, or management system, that is used to control the risk.

This is an important section of the risk assessment as it explains the relationship between the initiating and propagating events and the appropriate measures taken. It is strongly recommended that the measures are broken down into their respective layers:

- **systems of control;**
- **safety systems;**
- **self-acting devices.**

This approach enables the appropriate measures to be easily reconciled against any subsequent Layer of Protection Analysis (LOPA) or Fault Tree study. For control failure scenarios, it is recommended that a simple Cause and Effect Chart is included in this section. This should show the function, instrument tag numbers, valve numbers and set points. If the chart is organised such that the functions are ordered by control/safety/self-acting devices and given a different colour, for example, green/blue/red, and the set points are clear, the progressive response can be seen. This also gives some idea if the control and safety system

response is likely to cascade. Using a Cause and Effect Chart can significantly reduce the amount of description required; an example table is given below in **Figure 5**.

The independence of each layer of protection should be carefully considered, as common items or arrangements may cause similar or linked failures. Common cause failures (CCF) and common mode failures (CMF) should be considered as part of the analysis.

4.7.1 Systems of control

For automated systems, control system measures are predominantly any system at the basic process control system (BPCS) level, where the function is primarily to control the process. Control level trips and interlocks could be mechanical, electrical, pneumatic, or include an operator as part of the function (loop). A brief description of the control system measures should be given, including set points, also trip action, as well as describing the measures in the context of the scenario. A link should be given to the architecture of the control system, including the logic solver, CMF and CCF, communications and diagnostics.

The integrity of the BPCS should be such that it does not place a demand on the safety system greater than once per year. Its integrity needs to be demonstrated through the way in which the BPCS is designed, operated, and maintained; this is best described in a specific section separate to the scenario.

Control Systems Safety Systems Self Acting Devices			Please note that this diagram is included for illustrative purposes only and does not represent any system or particular functionality			EFFECT											
CAUSE						Close MCVE100 EDA Feed to PR1	Close MCVE101 Acetic Acid Feed to PR1	Stop P01 Acetic Acid Priming Pump	Stop P02 EDA Metering Pump	Close HCV2 102 Transfer Valve RD1 to RD2	Close HVCE103 Hot Oil Supply to RD1	Close MCV101 RD2 Control Valve	Close HCV2 103 Transfer Valve RD1 to RD3	Close HVCE104 Hot Oil Supply to RD3	Close HVCE106 Acetic Acid to RD3	Close MCV102 RD3 control Valve	Close HCV2 108 Transfer Valve RD3 to RD10
Function	Device	Setting	DCS/PLC/SA														
RD1 High Level	LEH100	0.26 m3	***			x	x	x	x								
RD1 High Pressure	PSH100	0.26 barg	***			x	x	x	x								
RD1 Temperature	TT100	190 deg C	DCS 800			x	x	x	x								
RD1 High Condensate Temperature	TT102	80 degC				x	x	x	x								
RD1 Bursting Disc Line Fault	XS111F		PLC 400			x	x	x	x	x	x	x	x	x	x	x	x
EDA IFS Valve Position Fault	XCVE100					x	x	x	x								
Acetic Acid IFS Valve Position Fault	XCVE101																
RD1 Bursting Disc Rupture	XCVE101		Self Acting			x	x	x	x	x	x	x	x	x	x	x	x
RD2 High Level	LSH101	8 m3				x	x	x	x								
RD2 High Pressure	PSH110	0.29 barg				x	x	x	x		x		x				
RD2 High Temperature	TT108	80 deg C				x	x	x	x		x						
RD2 High condensate Pressure	TT114	250 deg C	Local Hd wire			x	x	x	x		x						
RD2 Bursting Disc Line Fault	XS112F					x	x	x	x		x	x	x		x	x	x
RD2 Bursting Disc Rupture	XS112					x	x	x	x		x	x	x		x	x	x
RD3 High Level	LSH102	5 m3										x	x			x	
RD3 High Pressure	PSH111	0.25 barg										x	x		x	x	x
RD3 High temperature	TT111	90 deg C										x	x		x	x	

Figure 5 – Example Cause and Effect Chart.

Where a BPCS is used to provide a trip function, the risk reduction is limited to a probability of failure on demand of 0.1. No further risk reduction for control through the BPCS, or trip system which uses the same BPCS, should be claimed unless independence can be demonstrated.

For actively managed scenarios such as service-induced failure (corrosion, fatigue, high temperature hydrogen attack (HTHA) etc.), the control system will be a monitored management system designed to keep the system under control consistently within its safe operating envelope.

Scenarios outside of the system which rely on general arrangements are best handled collectively with examples given for specific unit operations to demonstrate compliance (**see section 4.2.1**).

4.7.2 Safety systems

For automated systems, safety system measures are a separate protective layer independent of the control system. They could be hard wired, use a programmable logic controller (PLC) or other relevant certified systems and equipment. Where high integrity protective systems (HIPS) are deployed, a separate description should be given for that protective system. For example, quench systems on reactors, hydraulic block valves on a Fluid Catalytic Cracking Unit (FCCU), or where fast acting shut down systems are to replace relief valves.

In all cases, the safety instrumented function needs to be adequately described.

Trips and interlocks could be mechanical, electrical, or pneumatic. A brief description of the safety system measures should be given, including set points and trip action, as well as describing the measures in the context of the scenario. A link should be given to the architecture of the system, including the logic solver, CMF and CCF, communications and diagnostics.

Where the system is reliant on ancillary systems to ensure effective prevention, such as the availability of the flare system or dump tank, this also needs to be included, although it could be fully described elsewhere and referred to.

For actively managed systems, safety measures independent of the control measures include active testing to ensure that the service induced failure mechanism is under adequate control. This could be an analysis of the process materials; testing of coupons; thickness testing and other non-destructive techniques or analysis of process information to determine remaining life.

4.7.3 Self-acting devices

A self-acting device is a device which operates autonomously, independent of other systems, without a signal from the control or safety systems. The most common example would be a bursting disc, or a spring actuated relief valve. Combinations of systems may introduce their own failure modes; for example, when a bursting disc is directly below a relief valve on dirty service, fragments may jam the relief valve preventing it from opening or closing. Self-acting devices normally provide a further independent layer of protection, and where this is the case, they should be represented as such.

4.7.4 Active management systems

Systems requiring active management are typified by those scenarios where materials of construction suffer from a known severe type of corrosion or cracking, which is prevented by keeping equipment within a strictly defined operating regime. These scenarios should be developed separately as the control measures are largely management-based systems.

Example - HF alkylation corrosion

Hydrogen fluoride (HF) is used as an alkylating agent to increase the octane content by alkylating a stream of isobutane with HF to produce a stream rich in isooctane. HF is so corrosive that only exotic alloys and metals can withstand attack. The scale of these systems is such that they were designed using carbon steel in order to be economic to construct. The carbon steel is able to resist acid attack as long as it has a passivation layer of iron fluoride, which is formed and maintained by keeping the system in its defined operating envelope.

- Managing:
 - feed composition quality (not exceeding limits set on: water, oxygenate contaminants, sulphur, nitrogen compounds, dienes; and ethane);
 - concentration of acid soluble oils (ASO) in the system;
 - concentration of water/alkyl acid/ HF acid; and
 - chosen operating temperature profile and recycle rate.
- Monitoring:
 - integrity of passivation;
 - build-up of corrosion scale in the system;
 - identification of vulnerable areas; and
 - inspection.

The likelihood of catastrophic failure can be predicted but needs to be assessed differently as failures are not random and therefore standardised failure rates cannot be used. Noting that a particular rate of corrosion will occur at a particular temperature, and substance concentration. Operation at higher rates of corrosion is a conscious management decision; the BOS being that the rate of corrosion is managed, and the inspection regime is appropriate.

The analysis, assessment and supporting description should include:

- causal mechanisms, the rates and nature of corrosion expected;
- control of water into the system – drying of feed, control of acid concentration;
- presence and control of butadiene;
- accumulation of corrosion products/scale within the system;
- predictability of corrosion – presence of localised high corrosion points and vulnerable areas general corrosion, historical evidence;
- operating envelope/ranges – maximum water/alkyl acid concentration/HF concentration/butadiene concentration;
- integrity of passivation where it is used as a specific measure; and
- example records.

For scenarios involving 'active management', a simple failure in the control regime does not lead directly to loss of containment, as corrosion/cracking is not immediate. The analysis, assessment and supporting description should focus on highlighting the management measures for the system, and the long-term control and measurement of corrosion/cracking/deterioration. It should be noted that the management system which reviews these measures and particularly changes to inspection intervals should also be referenced.

4.7.5 Measures for which no credit has been taken

In many cases there are systems present that reduce risk or provide additional mitigation for which no credit has been taken. It is advisable to add a brief description of these systems, as this assists illustrating defence in depth.

4.8 Scenario frequency analysis

Overview

Once the Operator has shown that appropriate measures are in place through logical argument; it is necessary to show that the cumulative residual risk from the establishment to a person on-site or off-site is below the tolerability threshold (**see section 5**). The cumulative risk is the sum of all MAHS consequence frequencies that a person is exposed to, that leads to fatality, also the sum that leads to three or more serious injuries.

To undertake this part of the assessment, the Operator first needs to generate the MAHS frequency (the frequency of the top event, which is normally loss of containment), then the frequency of each of the possible consequence outcomes. This is achieved by determining the probability of each particular consequence associated with that loss of containment. For example: pool fire, flash fire, VCE, or toxic exposure.

In parallel for each MAHS, the source term (the amount and physical state of the material released) is used to determine the extent of different levels of harm for the consequences identified. When these frequencies and probabilities are combined with the extent and severity, the frequency of death and/or serious injuries can be determined. This is carried out for each MAHS (or representative MAHS).

It is most likely that an Operator will need to select from a range of techniques to determine a unit operation's MAHS frequencies. These consider the failure frequencies of components, equipment items and, in some cases, sub-assemblies. It may involve using a range of information sources to generate the MAHS frequencies required. It would be unusual to find the MAHS frequencies for a whole unit operation that uses the same process parameters, has an identical configuration, is controlled the same way, and also encompasses all scenario failure mechanisms leading to loss of containment. Any sources of equipment/component frequency should be reconciled against the establishment's experience when available.

This section also highlights when some approaches are not considered appropriate for MHHRA, but which may be used for other purposes such as insurance.

4.8.1 Qualitative approaches – The use of risk assessment matrices

Qualitative approaches involving risk assessment matrices (RAM) use broad ranges of frequency versus broad consequence categories, overlaid to indicate which squares are intolerable, tolerable, and broadly acceptable. These are used to make judgements by determining which event pair combinations are 'tolerable'. The frequency assessment of the actual failure frequencies may often be based on a series of guidewords using judgement rather than analysis. Risk matrices are an effective means of ranking and screening risks from event outcomes. However, they cannot effectively demonstrate that all necessary measures have been taken. They also often use part scenarios or separate consequences. It is

considered that a simple guideword driven frequency analysis is insensitive, and not normally adequate where it is shown that the scenario leads to an MAHS. If there are a few simple scenarios, it is straightforward to use a simple LOPA table instead. If there are multiple scenarios, then a RAM or other qualitative approach is an unsuitable method for determining frequency. Even if used for screening for very large sites, multiple matrices would be required, as the extent of scenarios is normally limited, therefore not everybody is affected by all the scenarios occurring across the site.

4.8.2 Bow-tie Diagrams

Bow-tie diagrams are usually usefully employed as a training aid to visualise the initiating events together with the propagating events, which are often termed barriers. However, they do not represent either the logical or mathematical relationship. This is for a number of reasons, the most common is use of threat lines where all the barriers for a particular cause are listed in series. In reality, a single barrier may prevent a number of causes but on the Bow-tie diagram the barrier is repeated in each threat line. Often management arrangements are also included together with design standards. Bow-tie diagrams are considered inappropriate for the methodical development of a MHHRA.

4.8.3 Semi quantitative approaches – LOPA

Layer of protection analysis (LOPA) may be used to calculate the frequency of the top event for low to medium complexity scenarios. This can be used in conjunction with an event tree to evaluate the frequency of all the consequences. By its nature, it is a simplified process risk assessment technique and not suitable for complex relationships. It can be used for multiple outcomes, but this requires additional analysis (for example, materials which are both flammable and toxic, and released as a flashing liquid).

Figure 6, below, shows the use of an event tree to develop scenario consequence frequencies. The example scenario 'S12 Overfill of finished Gasoline Storage Tank (Buncefield scenario)' has been taken from **Table 1**. (see also **Table 2**: Illustration of consequence frequency expansion for scenario S12.)

RELEASE	WIND SPEED	IGNITION	CONSEQUENCE	
CASCADING RELEASE 1.00	>2ms ⁻¹	None	Evaporating Pool	
		0.8	0.02	0.016
			Early	Pool Fire
			0.07	0.056
			Late	Flashfire & Pool Fire
	<2ms ⁻¹	0.91	0.728	
		0.2	None	Evaporating Pool
			0.02	0.004
			Early	Pool Fire
			0.07	0.014
	Late	VCE & Pool Fire		
	0.91	0.182		

Cascading Gasoline Release 1 x10⁻⁴.yr⁻¹

Consequence Following Cascading Gasoline Release	Probability of Consequence Given release	Frequency of Consequence
Evaporating Pool	0.020 [0.016+0.004]	2.0 x10 ⁻⁶ .yr ⁻¹
Pool Fire	0.070 [0.056+0.014]	7.0 x10 ⁻⁶ .yr ⁻¹
Flash Fire and Pool Fire	0.728	7.3 x10 ⁻⁵ .yr ⁻¹
Vapour Cloud Explosion (VCE) & Pool Fire	0.182	1.8 x10 ⁻⁵ .yr ⁻¹

Figure 6: Extension of LOPA to determine consequence frequency.

LOPA is often treated as a single established technique, but there are many variants. In its simplest form, it is the tabulated representation of demand versus credit taken for measures in successive independent protection layers (IPL), to give the frequency of the top event. For a layer to be independent it must not share any elements, prevent an unsafe scenario progressing, and be capable of a functional test. An example of simple LOPA scenario frequency table is given in **Annex 11**.

The method was principally developed as an order of magnitude screening/design tool with powers of 10 (related to safety integrity levels [SIL]) used to populate the fields in the LOPA

table. The technique was developed to give an indication that the system should meet its tolerability criteria early in the design process. It is sometimes extended by adding probability of a person being exposed to a hazard, and also conditional modifiers (CM) to modify the probability that a person would be within the hazard range, giving the frequency of fatality from the scenario for that single outcome. This 'score' is then judged against a fixed risk tolerance criteria (RTC), often a risk of fatality $10^{-7} \cdot \text{yr}^{-1}$. This assumption is sometimes modified still further by assuming that there will be approximately 10 scenarios, so therefore the RTC becomes $10^{-6} \cdot \text{yr}^{-1}$. Whilst an effective tool for screening, it is not suitable for demonstrating all measures necessary in isolation; as scenario groups could be broken down into sub-scenarios, or even down to event pairs until the threshold is met. A simple threshold cannot be used to determine ALARP and the adequacy of measures.

For low to moderate complexity systems, LOPA can also be used to determine the frequency of the top event by using a higher resolution than a crude 'order of magnitude' screening study. The scenario risk of fatality and serious injury calculated can also then be calculated in the table or separately as required. This is achieved using the failure/demand frequency/rate (λ), and the appropriate reliability data to derive the probability failed to danger (PFTD) for each layer of protection. If there is only a single direct consequence, then the risk of serious danger can be easily calculated directly within the table.

If there are many consequences, then either a supplementary event tree would be required to support the table (see an example given in **Figure 6**); or multiple LOPA entries are required, with results collated within the table. Supplementary studies may be required to support the study where human factors are used to determine frequency of demand, or reliance is made on operator lead recovery. For some systems, a more complex table including the sub scenarios will be needed if all of the sub-scenarios do not share all the same safety systems (see **Annex 12**, though for brevity this only shows how the frequency of loss of containment could be calculated). When using LOPA to determine scenario frequency as a part of the risk assessment of the final frozen design or an operational plant, it is inappropriate to use LOPA to infer that a scenario is ALARP. This can only be determined when cumulative individual risk (job function) is calculated (see **section 5**).

4.8.4 Use of LOPA within Process Hazard Analysis/Process Hazard Review studies

The use of a form of LOPA within PHA/PHR studies, that just assesses single event/consequence pairs judged against a fixed risk tolerance criterion, can be used for screening. However, for all but the simplest cases, single event pairs are not suitable for judging tolerability or calculating scenario frequency. This form of embedded LOPA cannot normally sum the demand from all the different initiating events that lead to the same top event. This type of LOPA often takes credit for the same safety system elements for each entry, but treats them as separate entities. Initiating events that rely on the same safety systems and lead to the same top event, need to be assessed together.

Even when scenario frequencies have been correctly analysed, individual risk must be derived by summing the frequencies for fatality, and also the frequencies of serious injury, for all the scenarios they are exposed to. The hierarchy of control measures and relevant good practice (RGP) also need to be shown to have been considered before the risks can be deemed to have been reduced to 'as low as reasonably practicable' (ALARP).

With increasing complexity:

- Simple table - case with a few initiating events and simple preventative measures, i.e. tank overfill, refer to **Annex 11**.
- Complex table - scenario with many sub-scenarios, and having many safety systems which are common to some but not all of the sub-scenarios. For LOPA refer to **Annex 12**.
- Fault tree - complex relationships with many sub-scenarios some with different preventative measures; may require a supporting report.

4.8.5 Common LOPA failings

The following failings should be avoided in LOPA studies when evaluating serious danger to people:

- does not include all the possible hazardous consequences from the scenario;
- use of 0.1 for BPCS functions involving operator in the loop without giving adequate justification;
- partial credits for relief systems that do not have sufficient capacity;
- failure to consider the secondary risk when flammable or toxic materials are relieved directly to atmosphere;
- bunds included as an IPL (unless it has been specifically designed to prevent particular consequence events, such as a running pool fire or offers full containment such as a high collar bund);
- failure to adequately consider common mode failure, and common cause failure;
- including PPE as a protective layer;
- 'time at risk' calculated for a named person, rather than job function (for example, one operator only spends four hours per shift in the area at risk, but that person is replaced by another operator, so that overall, somebody is always present);
- generic study not based on a defined system; and
- credit given for written procedures.

4.8.6 Fully quantitative approaches – Fault Trees

For complex high hazard unit operations, such as Continuous Catalytic Reforming, it is recommended that fault trees are used. They are able to largely eliminate common mode failure from the calculation, because common systems can be placed further up the tree. They are able to properly assess contributions from sub-scenarios that share some safety systems. They are also better able to show fault propagation/progression through respective layers. Most fault tree packages also offer a variety of models to develop failure frequencies, and allow proof tests with fractional diagnosis. Fault trees are also recommended for complex mechanical protective systems such as Fluidised Bed Catalytic Cracking Unit slide valve systems.

4.8.7 Parts count

The phrases 'parts count' and 'generic failure rates' have become confused and ambiguous. A 'parts count' is used to describe a variety of very different methodologies that derive the failure to danger for the unit operation, from the frequency of failure of its 'parts'. This may range from a fault tree representing progressive failure of control, to simple addition of the numbers of 'parts' in a system multiplied by an 'all modes' failure rate. Any analysis needs to be carried out at a level which represents the particular unit operation being analysed and consider its particular failure modes.

For example, a car and a bicycle are both mechanical transport systems for people. They share many failure mechanisms including: bearing failure, corrosion, punctures, brake failure, lighting system failures. However, one is a very simple low energy system under low stress; the other is a very complex system under high stress, with many sub-systems and many more modes of failure. The failure rate values could be similar but that does not mean they represent each other, and in particular would not include all of the significant modes of failure.

The determination of frequency must be carried out in a way that reflects:

- the particular unit operation being performed,
- the particular operating conditions,
- substances present.

The frequency derivation of the top event must take into account the particular operational causes for that MAHS.

Operational causes due to random failure include:

- loss of process control,
- operator error, and
- mechanical breakdown.

Operational causes due to failure to manage the system within the defined regime (non-random failures) include:

- service induced deterioration,
- managed operation outside the safe operating envelope, and
- start-up/shut-down induced instability.

4.8.8 Levels of analysis

Successive levels of decomposition of a plant into its elements could be:

Unit operation > equipment > sub-assemblies > components

Unit operation level

The principle of a parts count, if carried out at unit operation level, is that the actual or synthesised failure rates are obtained from a similar unit. A unit operation may share the same operating principle or process; but other than repeated unit operations and parallel streams at the same establishment, the majority of unit operations of the same type have markedly different configurations, and/or specifications. Even if an exception were found, operating

parameters, modifications, manning levels and active management schemes would mean it would again significantly differ.

The unit operation comprises of: equipment items, control and safety systems, chemical inventory and services. Examples of some common unit operations are: phenol/formaldehyde batch reactor, distillation column, continuous catalytic reformer, blending system, thermal recovery unit, fluid bed drier, and also storage tank systems.

For risk assessment purposes, it is not appropriate to use generic failure frequencies 'all modes' for a whole unit operation, or MAHS frequencies for a whole unit operation developed for another site, or collated historical failure frequencies for whole unit operations from several sites.

Equipment level

Equipment items can be seen as the basic building blocks that are assembled together to form the unit operation. Examples of equipment level items are: valve with actuator, logic solver, sensor, column, agitator, pump, heat exchanger, flare header, flare, compressor, pipeline, filter, sieve, catalytic bed.

Analysis of the scenarios, sub-scenarios and event combinations that are driven by random failures, will require consideration of at least failure rates at the equipment level. LOPA or fault tree analysis are the principal methods used to calculate the frequency of MAHS, by using generic failure rates of valves, sensors, and logic solvers together with the initiating event frequency. It should be noted that different types of valves such as ball, globe, disk, and butterfly; have different failure rates, these can be found in the references given in **Annex 13**.

Analysis of scenarios caused by failure to actively manage the system within a defined regime, such as corrosion or erosion, are so dependent on the quality of the active management regime: that these scenarios can reasonably be represented by generic failure rates, using frequencies for different hole sizes, in different sized pipes and vessels. (**See also section 4.7.4 Active management systems, and 4.8.8 Generic failure rates for perforation of piping and vessels**).

For example, storage vessels may have MAHS which could include: control failure and human factors leading to: overfill; mechanical shell and roof failure; corrosion, cracking and mechanical defect. Frequently used guide IOGP 434-03 'Storage incident frequencies'⁹ gives generic frequencies for all the above scenarios, but is blind to the particular configuration and location. Failure frequency guides are intended to give frequency data for many different purposes, not just risk assessment. 'IOGP 434-03, section 4.1.3' gives the frequency of overfill as 2.1×10^{-6} per filling operation, but a caveat states: 'There are a large number of variables involved in the mechanism for overfill. It is therefore recommended that to model overfill effectively would require detailed analysis using fault tree techniques.'

It is considered appropriate to use this general data for actively managed scenarios such as perforation (loss of containment resulting from corrosion) and mechanical shell and roof failure. However, for control failure (human or control system element) a configuration specific assessment must be used.

A parts count at equipment level; comprises of breaking down a unit operation into a simple set of building blocks – line, vessel, column. Then using a generic failure rate for each element derived from data from across the sector, that does not consider the causes of failure, but represents cumulative failure 'all modes'. This simple methodology cannot consider the particular process, the way in which the process is controlled, or the particular event combinations for particular scenarios. The method evaluates the frequency of loss of

⁹ IOGP, (2022) 'Risk Assessment Data Directory - Storage incident frequencies Report 434-03'. International Association of Oil & Gas Producers (IOGP).

containment unilaterally without considering the frequency of each scenario (such as causes of loss of control), sub-scenario or event combination. This may be of sufficient resolution for assessing insurance or estimating financial risk, but this method does not have sufficient resolution for MHHRA, including ensuring all necessary measures are in place.

Component level (and sub-assemblies)

Each piece of equipment, such as a centrifuge, reactor, heat exchanger or logic solvers; will have different component parts, or sub-assemblies made up of component parts. For critical safety systems including high reliability systems such as logic solvers, and emergency shut down valves, failure rate analysis is undertaken at component level. This is because different control system architectures can have very different reliabilities. Often systems are designed and built to a required reliability or SIL. These calculations are normally performed by the system vendor, and use speciality risk assessment techniques such as reliability block diagrams. Examples of component level items are: logic solver- I/O card, power supply, barriers, field cabling, processor card, multiplexor; valve - stem, ball, body; heat exchanger - tube pack, tube sheet, expansion bellows, shell, head, and inlet manifold.

The validity of any parts count related study depends on the level at which the analysis is undertaken. The greater the resolution, the greater the difference between configurations is reflected in the failure frequency.

4.8.9 Simplified parts count using the offshore hydrocarbon release database

In this simplified form of the parts count approach, it is assumed that the Offshore Hydrocarbon Release Database (HCRD) failure rate encompasses all scenario failure mechanisms leading to loss of containment, for that unit operation/vessel/plant item being represented. Different frequencies are generated for different hole sizes and catastrophic failure by a parameterised model for each type of equipment/unit operation. The extent and severity of the different consequences is calculated for each release size. A risk contour plot can then be made by summing the risk for each grid square. Using the position of the person with time, the cumulative risk for the person or job function is derived. This method is sometimes incorrectly justified for use on refineries on the basis that both process crude oil.

However, work by HSE has shown Off-shore Production Platform (OPP) operations are characterised by:

- relatively simple processing of un-stabilised crude with few unit operations; low to medium pressures, 0 - 30barg; and low temperatures <100°C. Approximately 20% of current North Sea wells would be classified as high temperature high pressure (HTHP) with an operating pressure of approximately 30barg and crude temperatures of up to 150°C;
- dominance of gravity driven separator units which separate out gas, oil, and water. The bulk of the equipment is carbon steel, with some stainless steels, and exotic materials such as titanium and monel where required; and
- no significant potential for exothermic reaction, no large-scale chemical reactions or catalytic conversions; only relatively small quantities of other chemical processing reagents involved.

In contrast, refinery and downstream operations are dominated by:

- distillation processes;
- extremely large amounts of atmospheric flammable storage;

- complex multistage processing routes with recycle loops;
- complex control;
- process pressures in a similar range to OPP, 0 - 30barg, however some very high-pressure unit operations operating at up to 110barg;
- process temperatures very much greater than OPP. Many processes above 210°C, the point where high temperature corrosion processes occur; and
- presence of large quantities of toxic non-petroleum reactants.

This difference in operations suggests that service-induced failures on an OPP are not sufficiently representative of those found on a refinery and downstream operations.

Comparing the main processes carried out on a refinery, and those in downstream processing, to an offshore production platform; it can be seen that a high proportion of the unit operations are more complex than those on an OPP. Examples of these more complex operations are distillation, HF alkylation, isomerisation, fluidised bed catalytic cracking, hydrotreatment, oligomerisation and continuous catalytic reforming. These processes require multivariable control carried out through multiple nested control loops.

In distillation, one of the most common refinery unit operations, the product composition and column pressure are controlled by balancing the: boil up rate, reboiler level and steam flow; reflux distillate temperature, reflux drum level, and reflux ratio; feed rate, feed preheating temperature; bottoms product flowrate control. Control systems respond to maintain the material and energy balance across the column.

Many of the exothermic catalytic processes require close control to limit accumulation of chemical energy below the threshold that can lead to overpressure and loss of containment. This requires critical control of heating/cooling, catalytic bed monitoring and temperature trips, and may also require a minimum raw material flow.

For the majority of unit operations, the plant is under active, rather than passive control; failures to danger in the control loop cause the operation to move out of the safe operating envelope. Demand is then placed on safety systems such as trips and interlocks, together with self-acting systems such as relief valves and vent disposal systems. The number of failure modes in these complex interacting systems is very much greater than would be expected on a relatively simple OPP.

The simplified Parts Count methodology should only be used where the failure modes reflect the operations carried out offshore, such as simple fixed wall low pressure storage, gravity separators, and turbo compressors.

4.8.10 Generic failure rates for perforation of piping and vessels

Where mechanical failures that may lead to MAHS are driven by predictable service-induced degradation, for example wear, corrosion, and erosion; safe operation relies on established service thickness tolerances, together with predictable rates of degradation. The systems are actively managed to keep within a declared safe operating envelope, such that the rate of degradation is predictable, and the testing/detection regime can reliably detect/predict when service tolerances will be reached or are exceeded.

In these circumstances, the failure rate is largely determined by the quality and rigour of the management system. As long as the inspection interval and testing regime is such that degradation can be detected before failure occurs, the rates of failure are very low. Given that there are no established correlations between management systems and failure rates, the

use of generic failure rates in the assessment for holes of various sizes, and cold catastrophic failure, is considered appropriate. In these circumstances a Parts Count considering the length, diameter, and location, of a line/vessel; together with a component count: can give a meaningful estimate of background failure frequency for mechanical failure leading to various hole sizes, and catastrophic failure.

The source term used should be based on the total volume that can be discharged. Where the vessel is interconnected with other systems, the total interconnected volume should be taken (**see section 4.6.3, Source terms**). Using this approach, source terms are limited by examining a compartment volume. This is often taken as a simple boundary or 'node limit', however this is inadequate in most cases. As a minimum, the assessment should study the isolatable inventory (**see section 4.6.3, Source terms, Isolation**).

Where the use of generic non-specific pipeline failure rates for holes of various sizes are used in the assessment, it would be expected that these generic rates are compared to actual pipeline failure rates on that site. This is particularly important for pipelines which rely on passivation to resist chemical attack; lines which have been in service for longer than their intended design life (often 25 years); lines which are subject to erosion; and lines which are subject to high levels of stress or vibration, where there have been recent cases of loss of containment due to corrosion.

4.9 Scenario failure frequency data

The failure rates used to estimate the frequency of the top event should be tabulated, and the source of the information recorded.

The use of the standard relationship relies on random component failures occurring at a constant failure rate:

$$P_{FTD_{Av}} = 1 - e^{-\frac{\lambda t}{2}}$$

P_{FTD}	= probability failure to danger	unitless
t	= time between proof tests	yr
λ	= failure rate	yr ⁻¹

If failures are due to a known degradation mechanism such as managed rates of corrosion, and are not random, this relationship cannot be used in isolation.

If the system is not brought back to as installed condition, or only a partial proof test can be conducted, then the following more conservative relationship should be used:

$$P_{FTD} = 1 - e^{-\lambda t}$$

If the fraction of unrevealed failure to danger has been synthesised rather than derived from failure rate data, the derivation must be given, or it should be assumed that all failures lead to danger. It is not sufficient to use a rule of thumb that 50% of the failures are unrevealed to danger without proper justification.

References to failure rate data sources are provided in **Annex 13**.

4.9.1 Supplier data

For safety system logic solvers, the supplier failure rate data should be used whenever possible as logic solvers have significant differences in design, architecture, and

configuration. Safety system logic solvers should be provided with a comprehensive data package by the manufacturer for the configuration supplied. This is particularly important for logic solvers where the degree of diagnostic coverage and architecture, are important in order for them to achieve the desired reliability/SIL level.

For equipment in direct contact with the process, such as valves, pumps, and instruments: manufacturers' data should be used with caution, as the data is derived from 'clean' conditions and may not reflect operation in the field. In addition, manufacturers' data can be based on maintenance returns, which may under report failure. It is important that an appropriate adjustment to failure rate data is made for duties performed in a harsh environment, and/or on an aggressive or dirty duty. Possible approaches for adjusting failure rates are given in the literature, see **Annex 13**.

The Operator should collect site failure rate data from breakdowns, and proof testing, as part of the SMS. This is required in order to determine if:

- there are significant unpredicted failure modes; and
- equipment is as reliable as predicted and, therefore, proof test intervals are appropriate/adequate.

An established site would be expected to have compared site failure rate data with that used in any assessment and to revise any predicted failure rates as appropriate, noting any significant change to individual risk. It is often helpful to compare manufacturers' data with generic equipment data when there is limited site history.

4.9.2 HSE failure rate database

The HSE Failure Rate and Event Data for use within Risk Assessments (FRED)¹⁰, was derived and intended for general low resolution Land Use Planning assessment. It was not intended for use in specific assessments and does not necessarily take into account all of the factors that could be relevant. However, in the absence of site-specific data or high-resolution generic data, the values given may serve as a starting point. If Operators use this data, it should be stated why the use of FRED is appropriate, or if it has been used simply as a comparator.

4.9.3 SIL certified device data

The concept of using Safety Integrity Level (SIL) certified devices may suggest a simple solution to calculating failure rates and Probability of Failure on Demand (PFD). However, unless there is access to the full analysis (for example, Failure Modes and Effect Analysis 'FMEA' report), and the device has been tested with similar materials to those being processed, it can be difficult to be confident in its suitability for the duty. SIL certified equipment does not remove the Operator's responsibility to check it is fit for purpose. Operators are recommended to carry out their own Failure Modes, Effects and Criticality analysis (FMECA) or other appropriate study, on new or replacement equipment, to ascertain that the device is suitable and its failure rate will not be significantly different.

4.9.4 TNO Purple Book data

Caution should be applied when using TNO Purple Book values as the Dutch system for implementing Seveso III (implemented as COMAH in Great Britain) is somewhat different to that of Great Britain. In the Netherlands, the scenarios the duty holders must assess are already prescribed, and so the Purple Book failure rates are tailored to these scenarios and may not be sufficiently conservative.

¹⁰ HSE, 'Failure Rate and Event Data for use within Risk Assessments'. HSE.

4.9.5 Using multiple sources of failure rates

One source of failure rate data may not cover all the different components in the system, so some degree of mixing of sources could be required. The Operator should avoid selecting low values, and seek to identify mid-range values biased toward the degree of environmental stress and any aggressive duty encountered. Consistently selecting low values may reduce the validity of the assessment.

Site data

Site derived failure rate data can be used where there are large numbers of a certain type of components/equipment on specific services for long periods of time. Correct statistical treatments are required to process the data, see **Annex 14**.

4.9.6 Human factors and failure frequency

When Quantitative Human Reliability Assessment (QHRA), is used to determine Human error probabilities (HEP), for principal initiating and propagating events, the process should be carried out by a competent human factors assessor. All assumptions should be justified and the assessment systematic. In the absence of a QHRA, generic HEP data should not be used unless it has been qualified to reflect local circumstances, or is more than or equal to a HEP of 0.1.

For discrete human-in-the-loop activities, generic values of 0.1 to 0.9 are considered appropriate, but these need to be properly derived. When there is more than a single human interaction (this could be more than one person, or one person being responsible for several layers of protection), this should not be considered to collectively have a modifier of less than 0.1. When 2 people are in the loop they cannot be considered totally independent of each other, or to the overall 'system', and caution should be applied when claiming any factors of independence.

4.10 Scenario gap analysis (including Relevant Good Practice, RGP)

The justification that the risks to people, both on-site and off-site, have been reduced to ALARP should focus on making a logical demonstration that all reasonably practicable measures have been taken, not simply that a numerical value for a scenario or individual risk has been met. The scenario conclusion should show how the Operator has applied the hierarchy of control measures, and used relevant good practice.

Consideration of appropriate measures is iterative and undertaken both on a scenario level, and again considering the cumulative individual risk (job function) tolerability threshold. The tolerability threshold is the boundary between the tolerable and intolerable regions (**see section 5, Figure 10**) The Operator must show that they have considered the hierarchy of control measures and relevant good practice.

Appropriate measures should be in place before considering, 'further measures' (**see section 6**).

4.10.1 Hierarchy of control measures and the application of relevant good practice

For many chemical process unit operations there is no prescriptive standard for the basic design. The assessment should have considered the hierarchy of control measures:

- eliminate the hazard;
- reduce the hazard (by substitution or control); and
- minimise its consequences.

For example, where safety systems with an operator in the loop are described, the reason why an automated safety system has not been employed should be given.

Where the scenario involves equipment designed against a current relevant prescriptive code (for example, fired thermal heaters), a statement should be made as part of the assessment that the equipment fully complies with all aspects of that code, or compliance against the main points of the code should be summarised. If the equipment is designed to a previous revision of a standard or code, then a gap analysis should be performed highlighting the differences between versions, and also why any additional measures given in the standard/code are not necessary, or the reasons for any alternative being taken. An audit of relevant good practice can be undertaken in tabular form taking each main point in turn. It is not sufficient to only state what the relevant code of practice is.

Relevant good practice

In this context, relevant good practice is considered to include (in order of legal standing)::

- Specified standards:
 - minimum standards defined by Acts and Regulations; and
 - HSE Approved Code of Practice (ACOP).
- Recognised Standards:
 - British Standard (BS)/European Standard (EN) and appropriate international standards, such as American Petroleum Institute (API).
- Elective Standards:
 - recognised guidance produced and adopted by trade bodies and institutions.

It should be noted that Operators can adopt alternatives to RGP standards/codes if it can be demonstrated that they are equivalent. For equipment built before the current code; or to an older code, an RGP audit should be performed. This is normally a simple table indicating compliance against the main safeguards expected to be present. Exception and non-compliance to the code within any of the representative set should be highlighted and reasons for non-compliance given.

Where a relevant ACOP has been followed by the Operator, the system is sometimes deemed to be compliant, and that no further measures are necessary. However, the risks may not necessarily have been reduced to be 'as low as reasonably practicable' (ALARP). **Section 6** discusses the test of 'reasonable practicability', and how further measures are identified, then evaluated.

4.11 Scenario additional supporting information

Additional supporting information specific to that scenario that doesn't warrant a separate appendix should preferably be grouped together and collated. For example, this could be a relief valve data sheet detailing specification and sizing; or an example vessel inspection sheet.

Known major accidents and incidents

Part of the process of identifying potential-MAHS and actual MAHS, should be to consider relevant reported historic major accidents and incidents, both on-site and worldwide (refer to

section 3.3,5 and Annex 4). Those incidents should be included in the supporting information for the particular scenario.

4.12 Scenario conclusion

A concluding summary should be provided for each scenario capturing the key findings of a suitable and sufficient MHHHRA, which includes:

- compliance with relevant good practice;
- the adequacy of the appropriate measures present in the context of the scenario;
- additional measures considered for this scenario at this stage to support consideration of further measures (**see section 6**);
- scenario frequency;
- extent and severity summary;
- reference to other members of the representative scenario group (where appropriate); and
- a statement that all measures necessary have been taken for the MAHS, cross referencing the consideration of ALARP in the assessment (**section 5**), or a time bound improvement plan (as necessary) cross referencing any further consideration of further measures (**section 6**).

4.13 Periodic review and revision

Section 7 of this guideline outlines the general requirement that the Operator's SMS must be based on an assessment of the risk, and should include an outline of the Operator's approach to achieving a suitable and sufficient MHHHRA for all unit operations at the establishment.

For analysis, review and revision is expected as new information becomes available. New information would include RGP, standards, other control measures, failure rates and harm criteria.

5. Major accident hazard assessment

5.1 An overview of the key principles of assessment

A risk profile is produced for person(s) most at risk, both on-site and off-site, by collating the MAHS they are exposed to; then summing the risk for both death and also serious injury. This determines the maximum cumulative risk from the scenarios to which a person is exposed, as well as producing a profile for the relative contribution of the MAHS to both death and serious injury.

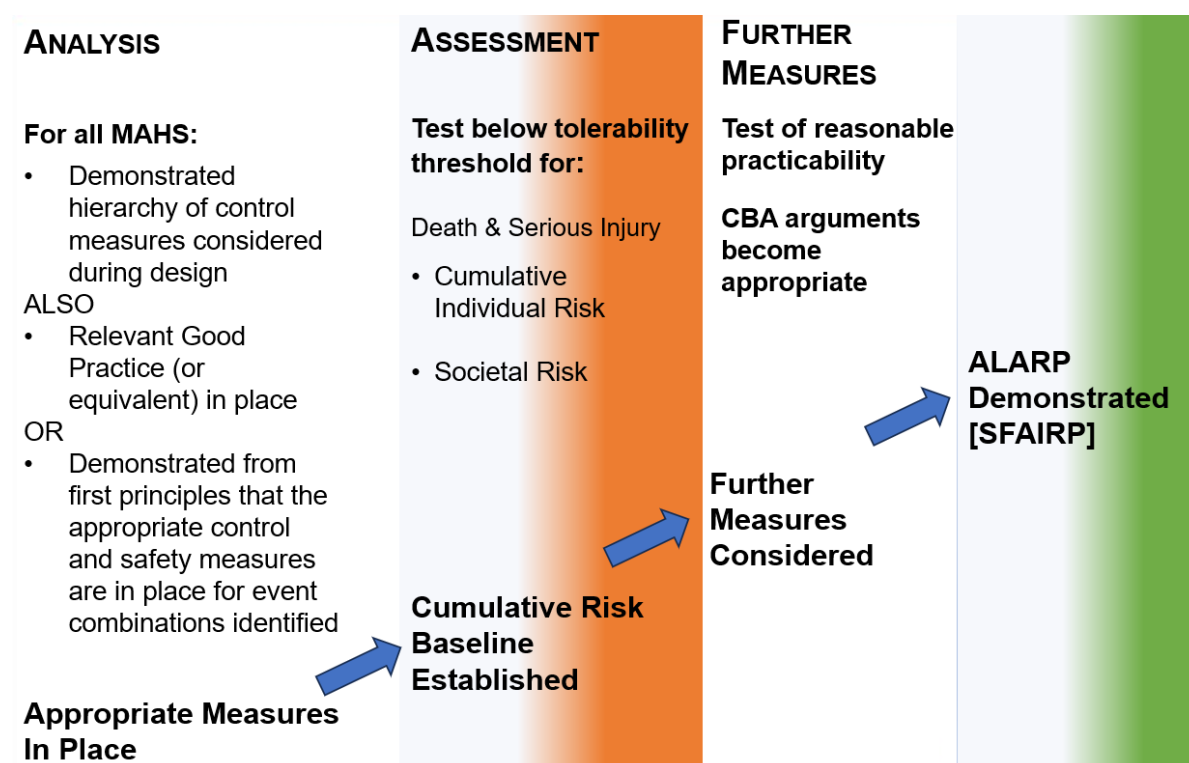


Figure 7: The pivotal role of risk tolerability.

The primary objective of a suitable and sufficient MHHRA is to support the logical case that all reasonably practicable measures have been implemented, it is not simply to show that a risk is below a tolerability threshold or is 'Broadly Acceptable'. That is why the narrative showing a suitable and sufficient risk assessment approach to MAHS identification, analysis and consideration of further measures is key. This narrative is supported by the numerical assessment case.

The key steps of the assessment are to:

- identify the on-site and off-site person(s) affected;
- overlay the hazard ranges determined for the MAHS;
- initially identify those persons who are most likely to have the maximum cumulative risk of death and also serious injury;
- collate the risk profile for the person on-site, and off-site, for the person(s) who have the maximum cumulative individual risk;
- determine if the risk of death and also serious injury are below the tolerability threshold;

- review the relative contribution of the MAHS to the people selected; and
- if the risks are not tolerable, consider the resolution of the assessments performed, and/or whether all the appropriate measures are in place.

A valid assessment of MAHS cannot be undertaken unless all MAHS have been identified **and** a meaningful analysis has been conducted.

In this context, analysis is the examination of the defined MAHS (further breaking down a MAHS into sub-scenarios where applicable). This analysis process has three elements; the first is a logical case that shows that the hierarchy of preventative control measures has been considered; the second how the appropriate measures prevent the scenario; and thirdly how the requirement to meet or exceed relevant good practice (RGP) has been applied.

The conclusion from the logical case for the scenario should show that analysis has considered these elements, and the appropriate measures for each MAHS meet, or exceeds, RGP (**see Analysis section 4.12, Scenario conclusion**). If it is not shown and concluded that: the system design, or later analysis, has considered the hierarchy of control measures; also that the system at least meets RGP (or has a reasonable logical case if RGP cannot be derived); then it has not been demonstrated that appropriate measures have been taken.

The second element of analysis is the determination of frequency, extent, and severity, for the scenario (and/or for its sub-scenarios if required to increase resolution). In some cases, the same safety systems prevent a number of different initiating events propagating in different scenarios. For complex systems where there are many scenarios/sub-scenarios that share different elements of many safety systems, a detailed numerical case is required, as without it the logical case is too complex to be resolved with simple relationships.

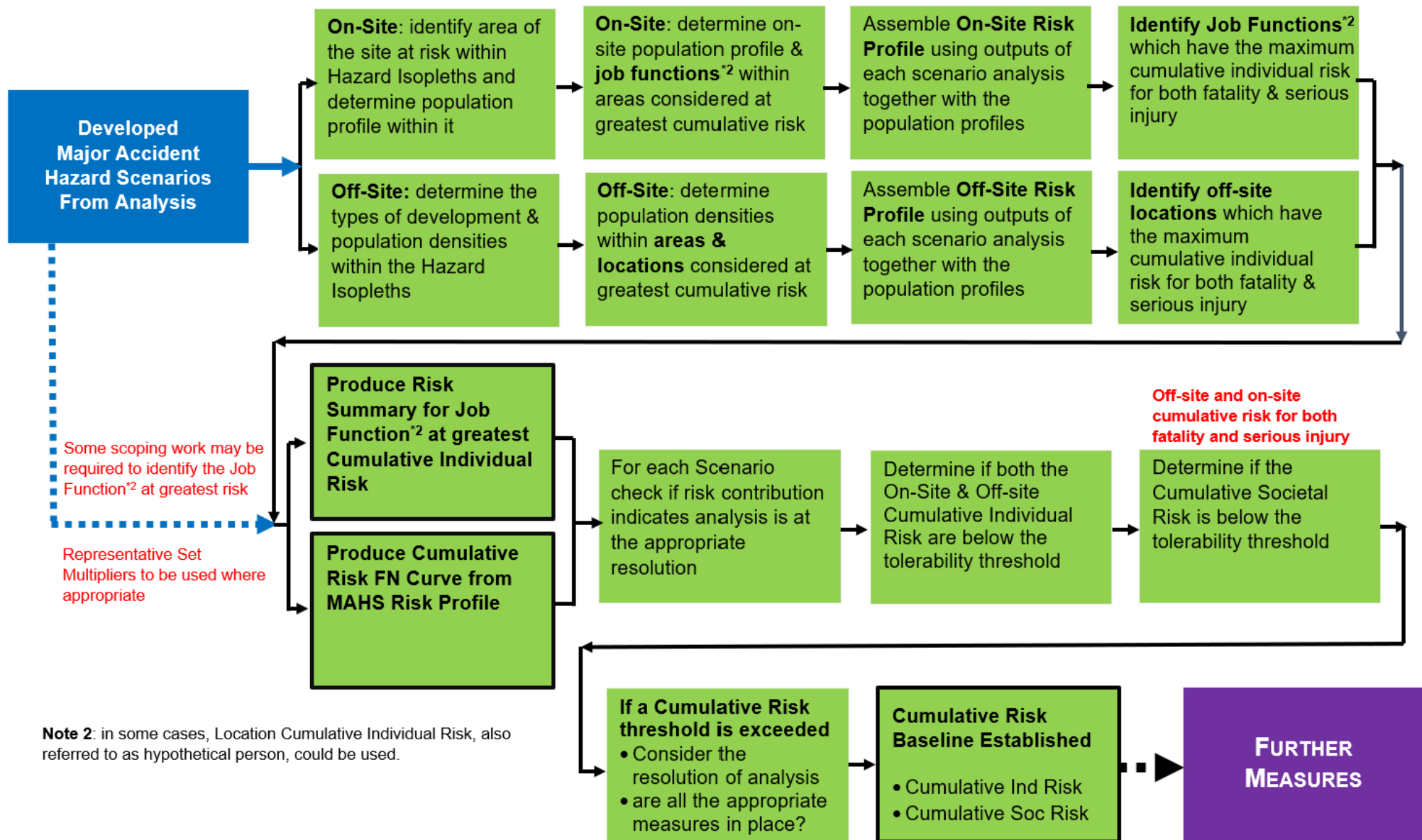
The quantitative aspect is to:

- support the case that all measures necessary have been taken, and that the risks have been reduced so far as is reasonably practicable;
- allow cumulative risk to be determined for specified individuals, and different populations both on and off-site;
- indicate if the cumulative risk from the establishment to the person is not intolerable; and
- show the relative contribution and importance of scenarios to the risk profile of the site.

If the risk from the establishment is found to be intolerable, the Operator may first need to reflect on the resolution of one or more MAHS. The Operator is advised to examine the contribution of the MAHS(s) to both the site risk profile and the maximum cumulative individual risk. This should identify the MAHS(s) that give rise to the greatest contribution to the establishment's risk. The largest contributors can then be re-examined in greater detail, in order of their contribution. If the risk from the establishment is still intolerable the Operator should then consider if all appropriate measures are in place. In extreme cases, it may require modifying or changing a unit operation, or even the process.

This guidance is for MHHHRA, for details on the assessment of MATTE, please refer to the CDOIF Guideline on Environmental Risk Tolerability for COMAH Establishments.

IDENTIFICATION → ANALYSIS → ASSESSMENT → FURTHER MEASURES



Flow Diagram 6 – Assessment

5.2 Evaluation of serious danger

As discussed in the MAHS identification section (**see section 3**), the definition of a MAHS is: “involving one or more ‘dangerous substances’, subject to ‘uncontrolled developments’ in the course of the operation, leading to ‘serious danger to human health’ (or the environment) inside or outside the establishment.”

It is the frequency of ‘serious danger’ that must therefore be evaluated; this is defined in the COMAH guidance (L111) as a risk of both:

- **death,**
- **physical injury or harm.**

Physical injury or harm means: a substantial number of people requiring medical attention; a number of people being seriously injured, or a number of people requiring prolonged treatment. A small number of carcinogens are listed in the regulations, and the effects of exposure from a MAHS could manifest themselves much later. The important point is that the harm arose from a single acute exposure, release, or event.

A common failing in MHHHRA is to only address fatality. There are many instances where serious danger has occurred and there are no direct fatalities, but many serious injuries and long-term effects. This is illustrated by the Seveso Disaster where dioxins were released. There were no immediate deaths at Seveso, but 15 children had to be rapidly hospitalised due to severe skin inflammation. Of the 1,600 local people of all ages who had been medically examined, 447 people were found to suffer from long-term skin lesions. An advice centre was set up for pregnant women, of whom 26 opted for a termination. The male children of mothers who were exposed during pregnancy to high levels of toxic dioxins due to the Seveso disaster, have been found to have lower than average sperm counts. For those exposed to dioxin, increased mortality was found for a number of diseases.

It is not appropriate to consider individual risk of death (IROD) alone, or to integrate from ‘Probit’ equations which calculate risk of death to determine the number who are seriously injured. Neither can the numbers of serious injuries be directly used to calculate the number of fatalities. The relationship between criteria thresholds for death and serious injuries differs for the various types of harm and the respective populations subject to them.

Advice on what constitutes serious injury is given in **section 4.6.1 Harm criteria**. See also **Annexes 8 to 10**.

5.2.1 Cumulative risk from the establishment to a person on-site or off-site

People both inside and outside the establishment are exposed to a wide variety of risks. It is only the cumulative risks from the MAHS to which people are exposed which are considered in this case; not the risk from everyday life, or occupational risks such as slips, trips, falls, and failed crane lifts. The COMAH Regulations and 1974 HSWA do not focus on the individual but harm to ‘people’, ‘employees’, and ‘persons other than employees’. The cumulative risk is determined for serious danger to these people, both singularly, and collectively, both on-site and off-site.

Cumulative risk is the sum of all the MAHS frequencies that a person is exposed to that cause death; and also the sum of all the MAHS frequencies that cause serious injury. However, everybody is not normally exposed to all of the MAHS, as MAHS take place in different areas of the site, and may have different hazard ranges. Also, people are usually located in several different locations, or may move around as they perform different tasks.

Scenario Reference	Description	Meets RGP or Better (improvement ref if required)	Scenario Frequency. yr ⁻¹	Consequence Category	On- Site		Off- Site	
					Number Fatalities	Number Of Serious Injuries	Number Fatalities	Number Of Serious Injuries
STORAGE AREA 1								
S1	Overfill of Pentane Tank T158	Y	3.30 x 10 ⁻⁴	2	1	10	0	0
S2	Liquid Overfill Flare System Area 1	N (A1)	2.50 x 10 ⁻⁶	3	2	20	0	0
S3	Catastrophic Failure Propane Pump P159	Y	1.90 x 10 ⁻⁵	1	0	6	0	0
ALKYLATION								
S4	Loss of Containment HF Alkylation reactor R006	Y	5.00 x 10 ⁻⁴	6	40	90	3	10
S5	Distillation Column C005 Loss of Containment Due to Overpressure	Y	1.50 x 10 ⁻⁴	2	10	40	0	0
NORTH QUAY DOCKSIDE OPERATIONS								
S6	Rupture of Jetty Hard Arm G011 on Propane Duty	N (A2)	2.50 x 10 ⁻⁵	4	3	30	1	5
S12	Overfill Of Finished Gasoline Storage Tank T003 (Buncefield Scenario)	N (A3)	1.00 x 10 ⁻⁴	3	3	3	8	30
GENERAL CHEMICALS 2								
S7.1	Epoxidation Reactor R456 Runaway Exothermic Reaction	Y	3.51 x 10 ⁻⁵	3	2	20	1	6
S7.2	Epoxidation Reactor R456 Internal Explosion	Y	5.00 x 10 ⁻⁵	3	3	30	0	1
S8	Internal Explosion Methanator R896	Y	2.50 x 10 ⁻⁴	3	2	20	0	0

Table 1: Suggested summary table structure for representative MAHS risk profile.

When performing the initial MAHS analysis, detailed information on the population may not have been available as the initial objective is to determine the frequency of fatality, as well as extent and severity. At the beginning of the assessment stage, the hazard ranges are known; detailed information is obtained regarding both the on-site and offsite populations just outside those ranges. It is also at this stage, when the scenario frequencies and severities are being collated, that the areas of greatest risk and severity emerge.

Table 1 above, summarises the MAHS frequency, number of fatalities and serious injuries, in order to allow an easily read compact table to be constructed. It should be noted that following loss of containment, not all of the possible consequences may lead to either death or serious injury, therefore MAHS frequency may often be greater than the risk of either death or of serious injury. The profile table shows the highest number of fatalities, and also the highest number of serious injuries selected in turn from all of the consequence permutations which can occur for that particular MAHS. For smaller sites, the Operator could include the full consequence frequency expansion within the table if they wish. It is important to ensure that there is no double counting when considering both death and serious injury, this is explained in **section 6.4.1**. For example, if a scenario with a single consequence gives rise to 2 fatalities and 7 serious injuries, but not a MATTE; then a value of 2 would be used for the number of fatalities, and a value of 5 for serious injuries. This is because a dose that leads to death would also cause serious injury.

To illustrate this the consequence expansion for scenario 'S12 Overfill of Finished Gasoline Storage Tank (Buncefield Scenario)' is given in **Table 2** below. The development of the top event is represented by the event tree for scenario S12 given in **section 4.8.3, Figure 6**. The consequence frequencies are derived by multiplying the scenario frequency by the consequence probability derived for each of the consequences considered. Some of the consequences are given as a pair in this case, for example VCE and pool fire. This is because the cascade of overflowing gasoline creates an expanding vapour cloud and forms a pool at the base of the tank. If the vapour formed by the cascade of overflowing gasoline does not ignite, the pool simply evaporates, and the vapour cloud disperses. If the wind speed is very low and the vapour cloud formed is subject to delayed ignition, a VCE will result; this will then flash back to ignite the pool formed around the storage vessel. VCE, pool fire, flash fire and unignited evaporating pool, could all be represented separately, but this does not indicate the full outcome as a pool fire could be part of a number of outcomes. In addition, the consequence development carried out as shown can inform emergency plans.

The on-site frequency of death is given by summing all of the S12 consequences which give rise to a fatality, the risk of serious injury being summed in the same way.

5.2.2 Collation of basic scenario information

It is important that a full list of MAHS (or the representative set with appropriate multipliers), and the derived values, are given in a summary table (**see the example given in Table 1**). These should be grouped by intuitive area, so that the site risk profile can be readily determined. This also assists in beginning the process of determining the job functions which are at greatest risk; or deriving risk for a hypothetical person, as this allows the main contributors to be clearly seen.

MHHHRA is dynamic, as there may be significant changes to the on-site processes, or off-site populations, over time. In addition to setting time periods for normal planned review, the safety management system (SMS) should consider other circumstances when a review is required (**see section 7**).

Scenario	Scenario Frequency . yr ⁻¹	Scenario Consequence	Consequence Frequency . yr ⁻¹	On- Site		Off- Site	
				Number Fatalities	Number Of Serious Injuries	Number Fatalities	Number Of Serious Injuries
S12. Overfill Of Finished Gasoline Storage Tank T003 (Buncefield Scenario)	1.0 x 10 ⁻⁴	Evaporating Pool (no ign)	2.0 x10 ⁻⁶	0	1	0	1
		Pool Fire	7.0 x10 ⁻⁶	2	3	0	5
		Flash Fire and Pool Fire	7.3 x10 ⁻⁵	3	3	1	5
		VCE and Pool Fire	1.8 x10 ⁻⁵	3	3	8	30
On site frequency of death 9.9 x10 ⁻⁵ .yr ⁻¹ ; serious injury 1.0 x10 ⁻⁴ .yr ⁻¹							
Off-site frequency of death 9.1 x10 ⁻⁵ .yr ⁻¹ ; serious injury 1.0 x10 ⁻⁴ .yr ⁻¹							

Table 2: Illustration of consequence frequency expansion for scenario S12.

5.3 Population profiles on-site and off-site

The population inside and outside the site boundary are different, they have different levels of tolerable residual risk, societal risk; and very different occupancy profiles. These differences allow simplifying assumptions to be made for on-site populations, and require a different approach for off-site populations.

5.3.1 Population within the site boundary ['on-site' population]

The on-site population within the site boundary are normally employees of working age (~18 to 65), and considered to be predominantly healthy, not vulnerable or sensitive.

Whilst there may be a low percentage of disabled, sensitive or vulnerable people within the site boundary; their safety should have been considered in making reasonable adjustments, so no further consideration is required when carrying out the MAHS assessment.

Populations within the site boundary that are not directly employed

On some sites there are populations within the site boundary that are not directly employed or indirectly employed (contractors and sub-contractors) by the company, such as:

- enclave sites operated and/or owned by others;
- buildings let to third parties;

- on-site training centres shared with others; and
- divested elements of sites now operated by another company.

These populations within the site boundary, other than those who are directly employed or indirectly employed, are considered to be members of the public and should be considered together with any off-site populations.

On-site population determination of death and serious injury

It would be expected that a map indicating the on-site population would be produced which includes occupied buildings, and this would be supported by an occupied buildings list indicating the number of people present and fraction of time for which they are occupied.

Fatality

A pragmatic estimate of the dose that will lead to a fatality (Significant Likelihood of Death - SLOD) for the healthy population of working age on site, can be represented by the dose that would lead to 50% of the normal population (of normal distribution) being killed; this is often referred to as LD₅₀. This effectively represents the dose at which an 'average person' would be killed.

The figure for which it can be assumed that most people will be killed can be expressed as LD₉₅; the figure at which a few percent will be killed being LD₀₅. A pragmatic estimate for death can be taken by assuming that receiving a dose above the LD₅₀ (also known as the value for the significant likelihood of death, SLOD) results in fatality.

Serious injury

Dangerous dose is a level of harm that can be differentiated for different parts of the normal population in relation to the working population. The working population, as defined above, is the least susceptible fraction of the population; a dangerous dose is considered to give rise to serious injury.

For suggested harm criteria values, and more detailed guidance, see:

Annex 8 Suggested criteria to determine harm to the person from thermal radiation.

Annex 9 Suggested criteria to determine harm to the person from exposure to toxic gases and vapours.

Annex 10 Suggested criteria to determine harm to the person from overpressure (and impulse).

5.3.2 Population outside the site boundary, consideration of the public

The off-site population are viewed as occupying discrete developments of differing uses, containing differing population profiles. For the purposes of evaluating the risk to people, it is not necessary to describe the population beyond the largest hazard range determined. It would be unusual for the hazard range to extend much beyond 1km, so this should allow development types to be easily identified, listed, and recorded on a population map, **see Figure 8**.

The population location list (**see Figure 9**) should indicate the type of development. For development types, except general housing, an estimate of the number of people present should be given together with the population type, and whether present day or night. Where

large areas/numbers of domestic dwellings are present in a block, or an estate, any assumed population density or population per household should be given.

A full worked example is given in **Annex 17**, this is based on an imaginary site 'XML International', but in the context of an actual population present in 2024. Like many established sites, it has an 'enclave', this is where a portion of the land inside the site boundary is controlled by another company. The example has most of the development types that will be encountered in the UK. Development around a long-established site can appear confused and complex. This is because the land use has developed over many years; often before the regulation controlling development around Major Accident Hazard establishments was introduced.

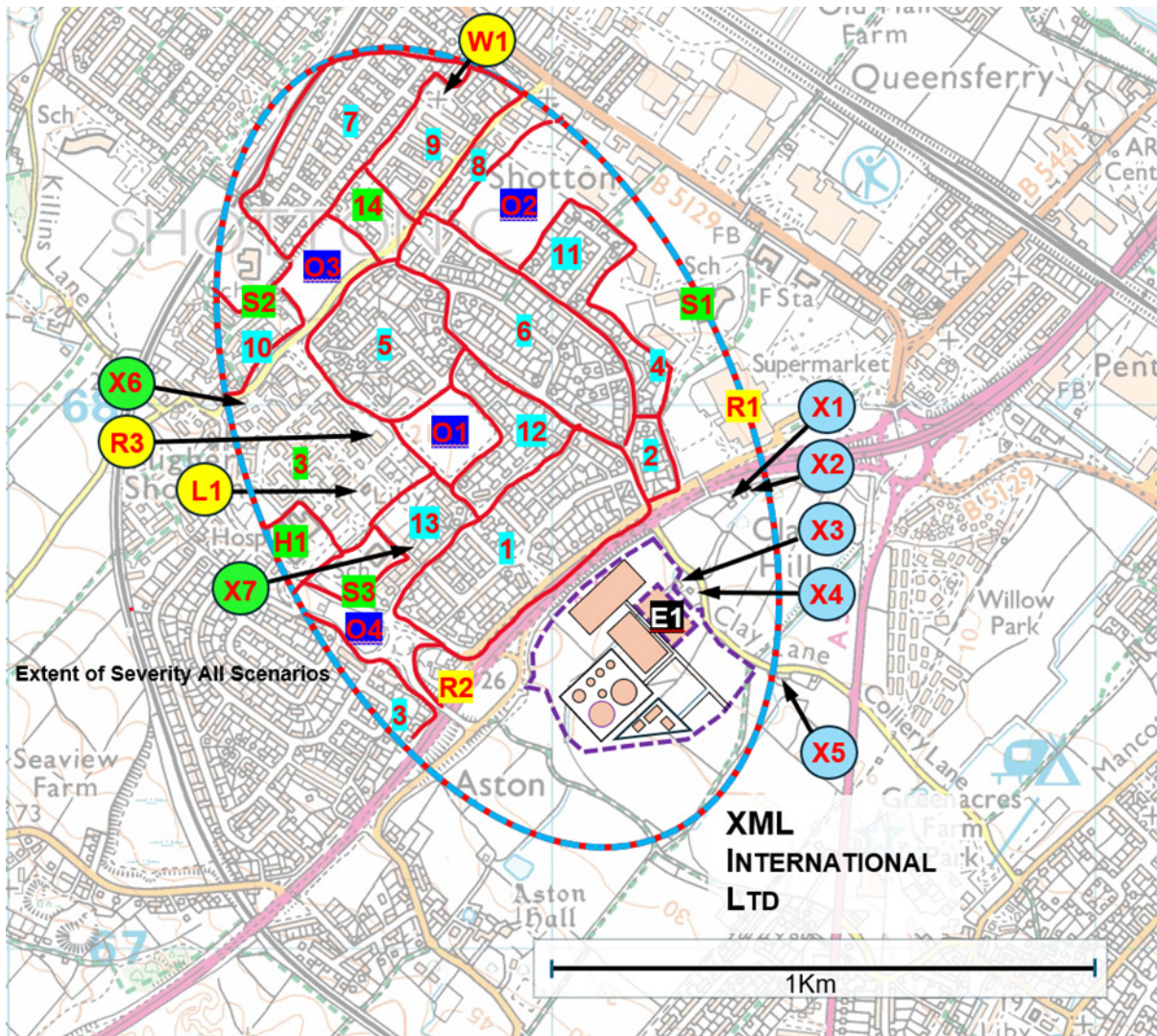


Figure 8: Population map (see Annex 17 for full example).

Example of development types that should be included:

Domestic dwellings – assumed full normal range of population present – young, old, people of working age, normal proportion of vulnerable and sensitive individuals. Assumed to be occupied day and night. Currently the Office for National Statistics (ONS) gives the average occupancy in the UK as 2.4 people per dwelling.

Schools – the majority have students which are below the age of 18, but this is a generalisation. Some schools have a particularly vulnerable population, for example

nursery schools. Unless schools are residential, they are normally considered to be occupied only during the daytime. If part of the building and curtilage are within the dangerous dose isopleth, it will be necessary to determine the actual occupancy.

Care home – predominantly vulnerable and sensitive individuals. Assumed to be occupied day and night. If part of the building and curtilage is within the dangerous dose isopleth, it will be necessary to determine the actual occupancy.

Workplaces – homogeneous, predominantly healthy, and of working age (~ 18 to 65 years of age). Occupancy as per use. If part of the building and curtilage is within the dangerous dose isopleth, it will be necessary to determine the actual occupancy.

Retail premises – full normal range of population present. Occupancy as per stated use.

Sports stadium – a judgement may need to be made on the number of people present, and the amount of time they are present for. Where different events are held at irregular intervals a time weighted average may need to be determined.

Hospital – normally occupied day and night with a vulnerable and sensitive population. If part of the building and curtilage is within the dangerous dose isopleth, it will be necessary to determine the actual occupancy.

The hazard ranges for fatalities and serious injuries are overlaid over the population maps, allowing the numbers of fatalities and serious injuries to be derived.

Development Category and block ref no	Area	Number people per dwelling/ housing density	Population Group	Occupancy	Building Type	Assessment Specific	
						Toxic air changes per hour	Blast limit of partial collapse/ limit of total collapse
Housing							
1	Terrig St Aston Rd (Clwyd St)	2.5 pe/dwelling 5.0 dwellings/ha	Normal	24hours	Mix of brick built Semi-detached, and four in a block, two storey houses		
2	Dee View (Chevrons Rd)	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
3	(Holly Grove) Coutland Dr	2.5 2.3 dwellings/ha	Sensitive & Vulnerable	24hours	Single storey brick blocks of two and 4 dwellings		
Outdoor Leisure							
O1	Higher Shotton Sports Field	20 (50)	Normal	08:00 to 21:00	Open field		
O2	Higher Shotton Sports & Community Centre	25 day	Normal	08:00 to 21:00	Open field		
School							
S1	Queensferry CP School	149 pupils day 10 staff	Sensitive	08:00 to 16:30	Steel frame concrete		
Retail							
R1	Asda Superstore	150 staff and shoppers	Normal	06:00 to 22:00	Aluzinc clad portal steel framed building, glass fronted		
Place of Worship							
W1	Biserica Creştină Penticostala Râul Vieţii	50	Normal	see further detail	Traditional brick		
Site Enclave							
E1	COB Industrial Gases Ltd	5 staff	Working age	07:00 to 16:30 Tue - Sat	Portakabin single storey		

Figure 9: Population location list (see Annex 17 for full example).

Fatality and serious injury for off-site populations

Fatality and serious injury for off-site populations depend on the particular populations present at the development types identified. Unlike the on-site population, those present are not just of working age; but may comprise young, old, vulnerable, and sensitive people. Noting that for domestic dwellings, the generalisations above can be used. Any methodology used must be able to differentiate between the different populations present. It is strongly suggested that the Health and Safety Executive (HSE) 'dangerous dose' is used for this purpose, as it is defined for thermal radiation, overpressure, and toxic exposure.

A dangerous dose would lead to 33% of a normal population (of normal distribution) being fatally injured, with the remainder seriously injured; 100% of the vulnerable or sensitive population would be fatally injured.

For those of working age such as would be encountered at industrial premises, a dangerous dose would cause a few percent to be fatally injured, and the remainder seriously injured. Dangerous dose is not sensitive enough to determine IROD for populations solely comprising those of working age. It is suggested for industrial premises that the SLOD (LD50) values are used to determine the IROD isopleth, and dangerous dose is used to determine the serious injury isopleth.

5.3.3 Review of proportionality

Before considering cumulative individual risk, the Operator should check if their initial estimates of extent and severity were greater than originally estimated. If they are, this could impact on proportionality and require a greater depth, resolution and robustness of assessment (see **Annex 2** on proportionality).

5.4 Cumulative individual risk and its relation to risk from the establishment to a person

In order to determine the maximum cumulative risk to the person, the risk profile of individuals needs to be examined. This is carried out by looking at the cumulative individual risk from all of the MAHS they are exposed to (**see section 5.1**).

Consideration of location when determining cumulative individual risk

As a person moves location they will move in and out of the hazard ranges of the various scenarios they are exposed to. Their total risk of death, and also serious injury, will be determined by:

- Geographical location of person with time;
 - locations of any activities undertaken;
 - time spent at each location performing that activity; and
 - transition from one location to another.
- Whether they are outside or inside a building that modifies the risk to the person.
- A person's opportunity to escape should an MAHS occur;
 - presence of refuge or shelter within escape limit; and
 - mobility.

When determining the hazard scenarios a person is exposed to, the hazard ranges used must differentiate for a person inside or outside a building. For example, where a person spends a significant fraction of time in the open, the scenario hazard ranges must represent outdoor exposure for that fraction. It would be inappropriate to just use global hazard ranges which already take into account the reduced exposure from being indoors, for both indoor and outdoor locations.

In addition, it would be inappropriate to use a global assumption that everybody can reach a refuge within the assumed escape distance, if this is not possible for the particular person being considered (escape and refuge are discussed in **Annex 8**). Noting that external factors which affect the person at risk, such as meteorological conditions (wind direction, humidity etc), should have already been considered when calculating scenario hazard ranges/isopleths.

Forms of cumulative individual risk

Cumulative individual risk (most often referred to in its contracted form as ‘individual risk’) is derived for death, and also separately, serious injury. It is the sum of the MAHS consequence frequencies that a person is exposed to that cause death, and serious injury, respectively. However, there is no consistently cited definition because it is used in different forms for different circumstances.

There are three basic forms which have very different meanings and are not normally interchangeable:

- **cumulative individual risk (hypothetical person);**
- **cumulative individual risk (job function);**
- **cumulative individual risk (named person).**

Within the limitations of available information, the form of cumulative individual risk selected must be appropriate for the particular person being considered. For example, it may not be possible to account for the movements of people outside the control of the Site Operator. For those under the control of the Site Operator, it is necessary to determine whether the person is based indoors at a fixed location, such as a dedicated control room operator; or does the person perform a set of tasks that takes them inside and outside to several areas of the plant? The following three sections outline how these different forms of cumulative individual risk should be used to properly determine the risk from the establishment to a person. (**See section above, Consideration of location when determining cumulative individual risk**).

5.4.1 Cumulative individual risk (hypothetical person) location risk

A ‘hypothetical’ person is defined by the HSE’s R2P2 document¹¹, which has now been withdrawn and archived, as: a ‘type of individual who is deliberately assumed to have some fixed relation to the hazard under consideration’.

Off-site

It is not normally possible or practical to determine the movements of a person off-site with time, given the many risk profiles that would be required to describe the surrounding population. To determine cumulative individual risk a hypothetical person who would be continually present at a fixed location is used to sample the various developments where people may be present. The reduced resolution created by this assumption is considered appropriate, as normally the off-site population is much further away from the location of the MAHS than the on-site population, and the cumulative risks are at least an order of magnitude lower.

The HSE document ‘Risk criteria for land use planning in the vicinity of major industrial hazards’¹² considers the individual risk from a major hazard is expressed as the probability that a typical user of the development would be harmed in the course of a year, due to the major hazard. Cumulative individual risk (hypothetical person) is simply the cumulative

¹¹ HSE, (2001) ‘Reducing risks protecting people: HSE’s decision-making process’. Now withdrawn and archived at: <https://webarchive.nationalarchives.gov.uk/ukgwa/20230703113731/https://www.hse.gov.uk/enforce/expert/r2p2.htm>

¹² HSE, ‘Risk criteria for land use planning in the vicinity of major industrial hazards’. HSE.

individual risk for a particular location outside the site boundary. It is therefore sometimes referred to as cumulative individual risk (location), or simply 'location risk'.

When used to assess off-site risk tolerability, the location where the cumulative risk to a person is at its greatest is taken. It is possible that this location could be different during the day or during the night. This is because higher risk activity such as filling a chlorine tank may be carried out during the day, and an adjacent retail park is only open during the daytime.

On-site

Where a particular on-site job function is static, such as a dedicated control room operator who rarely goes to the production plant, and only works from a particular control room; the cumulative individual risk (job function) for that person is the same as cumulative individual risk (hypothetical person). The intention is not simply to find the location on site with the highest risk, which will usually misrepresent the risk profile to the person, or to pass a threshold test; rather, it is to meaningfully determine the risk to the person such that the contribution of different scenarios is visible.

5.4.2 Cumulative individual risk (job function)

On-site

On-site, the maximum cumulative risk to the person is determined by the highest cumulative individual risk (job function). This is the numerical threshold by which risk tolerability to the person is judged, following on from the logical argument that RGP and the hierarchy of control have been considered, also the risks are broadly ALARP (subject to later consideration of possible further measures when the risks have been found to be below the tolerability threshold (**see section 6, Further risk reduction measures**)).

A job function is an existing, designated, defined role; normally subject to a formal job description, and associated with a particular area of plant such as 'Granulation Plant Operator' or 'Tank Farm 2 Operative'. The job may entail some of the time in the control room, and some of the time on the plant, or in an office. A job function is not a representative function or an arbitrary combination of tasks, it must be defined by a job description.

A job function may be exposed to a risk of fatality and/or serious injury from a number of MAHS (or representative MAHS if used). Cumulative individual risk (job function) is the total risk that the job function is exposed to. Where the job function is within the hazard range of a number of units which share a representative scenario, the frequency for that representative scenario is multiplied by that number of units.

Using the harm criteria consequence isopleths generated from the representative hazard scenario consequence analysis, it should be apparent which areas of site are likely to give rise to the greatest level of risk, and so which job functions are exposed to the most risk. Where practicable, a small number of representative job functions should be taken to represent the highest to lowest risk groups on site. An often overlooked job function is that of security guard who may roam the entire site in the course of their duties. In the case of very large diffuse sites, this may take a degree of trial and error. It could be advantageous to map risk density by area and job function, but this requires specialist techniques.

Unit 4 is operated by eight staff, two per eight-hour shift; comprising a control room operator, and an external operator. **Example risk summary tables for the external operator are given in Table 3** at the end of this section. Unit 4 is in the hazard range of two similar distillation columns. Therefore, the frequency for the representative scenario 'S5 Distillation Column Loss of Containment due to Overpressure' is multiplied by a factor of 2. A fractional time exposed is used as the operator moves from one part of an area to another, and is not exposed to all of the risks all the time. Equally, if all of the processes were not run all the time,

this too would affect the risk profile. Any shift time weighting should be applied after the scenario frequency has been calculated and tabulated.

It should be noted that limiting the number of hours run, or the duration to which a person is exposed, is not a basis of safety. This approach should not be used to bring a scenario, a group of scenarios, or job function, below the tolerability threshold unless it can be shown that: the system meets RGP, the system is already ALARP, and there are no further proportionate measures available.

Sharing tasks within a job function

A job function such as 'Tank Farm Operative' may include a number of tasks in the same area that are shared between a team on the same shift. Provided the tasks are in an area which is subject to the same MAHS and the tasks are randomly allocated rather than permanently assigned, the cumulative individual risk can be averaged among the team to produce a profile. Whatever treatment is used, it must consider the location of the person with time as discussed at the beginning of **section 5.4**.

5.4.3 Cumulative individual risk (named person)

'Cumulative risk (named person)' represents the share of risk that the named individual, (for example, Mike Smith) is exposed to as they move round the site. A job function will be performed by different people on each shift. So for an eight-hour shift system this could be three or more allocated staff due to weekends and holidays. In addition, the plant may also be subject to bi-annual shutdowns. The fraction of the cumulative risk (job function) to which the individual is exposed is calculated.

Cumulative risk (named person) could be used to determine risk tolerability on site by adding together the risk profiles from all those people who perform that job function. This is as long as the profile considers the different scenarios the people are exposed to, as they move around the site carrying out the tasks normally associated with the job function that they perform. Using the example given in **Table 3, External Operator (Unit 4) job function**, on the basis of eight named individuals: Mr A, Ms B, Mr C, Ms D, Ms E, Mr F, Ms G, and Mr H; on a three shift system, with two operators present on a shift; the cumulative risk (job function) would be the sum of the eight risk profiles divided by two. However, it is much simpler to derive the cumulative risk (job function) in the first instance.

5.4.4 Relationship between time on-site and cumulative individual risk

MHHHRA is only concerned with the immediate dose received when the MAHS occurs, the resulting harm response may be immediate or delayed. This differs from occupational risk, which is often concerned with cumulative exposure to substances harmful to health giving rise to adverse consequences; in such a case, it is the number of hours that a person has been exposed to significant concentrations that leads to the dose response. In contrast, a MAHS occurs over a few seconds or minutes, so any person present receives the full dose; it is not shared.

Appendix 1 of HSE's R2P2 (R2P2 is now withdrawn and archived) titled 'Some of the conventions adopted for undertaking risk assessments' discusses a person in good health, who works 40 hours a week, experiencing repeated occupational exposure to chemicals entailing adverse consequence for long periods (**see also section 5.5 for tolerability**). The focus is on occupational exposure, not exposure to MAHS. R2P2 discusses using a hypothetical person to compare the risks from different occupations. MAHS are only a part of the risk a person working on a major hazard site is exposed to, so this cannot be directly compared to the cumulative risk faced by people in other occupations. R2P2 set out the overall framework for HSE decision taking to ensure consistency and coherence across the full range of risks falling within HSWA. It was not intended as a risk assessment guide;

nevertheless, the concept of hypothetical person can be usefully employed when it properly represents cumulative individual risk.

For a job function that is continually present on site, risks to 'persons at work' is based on that continual presence, even though a different individual is present on each shift. This is because if there were an event that led to a fatality (or more than three serious injuries) in that area, there would always be a person present performing that job function.

5.4.5 Use of expectation values for risk tolerability

The 'potential loss of life' (PLL), also known as the 'expectation value' (EV); is the expected number of fatalities for a particular scenario, multiplied by the scenario frequency; then summed for all MAHS (sum of all F-N pairs). The PLL and EV metrics are not used routinely by the regulator when considering risk tolerability, as they lose the distinction between 'low-probability high-consequence events' and 'high-probability low-consequence events'. For example, ten fatalities at a frequency of 10^{-5} yr^{-1} , has the same expectation value as a single fatality at 10^{-4} yr^{-1} . However, expectation values are useful for converting the risk of death and serious injury to a cost that can be considered in cost-benefit analysis. This is discussed in **section 6, Further risk reduction measures**.

5.4.6 Determining Cumulative Individual Risk

Cumulative individual risk is determined by adding together the risk of death, and also separately serious injury, for the consequences of all the MAHS they are exposed to. For small sites with a low number of MAHS, it will normally be readily apparent which areas are at the most risk.

For large sites the hazard isopleths of the MAHS consequence outcomes associated with each scenario (pool fire, flash fire etc); for both death, and also serious injury; can all be plotted together on a site layout plan for the highest risk areas. This should assist the Operator in locating the job function at greatest risk.

Where a person is exposed to many scenarios which have a number of consequence outcomes, as there can be many permutations, it is recommended that the calculation to combine the risks is undertaken in a suitable spreadsheet. It should be noted that where an area has a number of similar unit operations which have been represented by the same representative scenario/sub-scenarios; the isopleths should be drawn for the locations of each of the unit operations represented in that area. This is because it is possible that a person could be in the isopleth for death of that representative operation close by, and only in the isopleth for serious injury of that representative operation further away.

For very large complex sites, such as refineries, the isopleths for the site MAHS consequences can be added together using software to produce a risk contour map for both death and also serious injury. The locations that the operator of interest is present can then be used to determine cumulative individual risk. Where operators can be present inside a building that is deemed to protect them, it may be decided to calculate a set of values for particular occupied buildings as the exposure to harm will be significantly different.

Whichever method is used, a summary table should be generated in order to show the contribution of the different MAHS to the individual at the highest cumulative individual risk.

It should be noted that the summary table is to illustrate what an appropriate output table may comprise. The consequences have been developed elsewhere, also noting that for some MAHS the risk of death and also serious injury may be only a small fraction of the MAHS frequency for the top event of loss of containment.

EXTERNAL OPERATOR (UNIT 4) CUMULATIVE RISK OF DEATH						
Relevant MAHS	Frequency of Scenario .yr ⁻¹	Frequency of Scenario leading to death .yr ⁻¹	Multiplier (number of times represent used)	Fractional Time Exposed To Scenario	Risk of Death .yr ⁻¹	Contribution %
S1	3.30 x 10 ⁻⁴	-	-	-	-	-
S2	2.50 x 10 ⁻⁶	1.00 x 10 ⁻⁶	1	1	1.00 x 10 ⁻⁶	1
S5	1.62 x 10 ⁻⁴	5.00 x 10 ⁻⁵	2	0.5	5.00 x 10 ⁻⁵	53
S6.2	5.42 x 10 ⁻⁴	-	-	-	-	-
S7.1	3.51 x 10 ⁻⁵	1.10 x 10 ⁻⁵	2	1	2.20 x 10 ⁻⁵	23
S7.2	5.00 x 10 ⁻⁵	1.06 x 10 ⁻⁵	2	1	2.12 x 10 ⁻⁵	23
S9	3.05 x 10 ⁻⁵	-	-	-	-	-
S10.5	7.60 x 10 ⁻⁵	-	-	-	-	-
Cumulative Risk (24/7 for 1 year) Job Function <i>Basis: 24 hour operation</i>					9.42 x 10 ⁻⁵	
Risk to Particular Person carrying out that job function <i>Basis: 8 hour shift pattern for 230 days [fraction present = 0.21]</i>					1.98 x 10 ⁻⁵	

EXTERNAL OPERATOR (UNIT 4) CUMULATIVE RISK OF SERIOUS INJURY(Consequence ≥3 Persons)						
Relevant MAHS	Frequency of Scenario .yr ⁻¹	Frequency of Scenario leading to Serious Injury (≥3 person) .yr ⁻¹	Multiplier (number of times represent used)	Fractional Time Exposed To Scenario	Risk of Serious Injury (≥3 person) .yr ⁻¹	Contribution %
S1	3.30 x 10 ⁻⁴	3.30 x 10 ⁻⁴	1	0.5	1.65 x 10 ⁻⁴	16
S2	2.50 x 10 ⁻⁶	2.00 x 10 ⁻⁶	1	1	2.00 x 10 ⁻⁶	<1
S5	1.62 x 10 ⁻⁴	1.00 x 10 ⁻⁴	4	0.25	1.00 x 10 ⁻⁴	10
S6.2	5.42 x 10 ⁻⁴	3.00 x 10 ⁻⁴	4	0.25	6.00 x 10 ⁻⁴	58
S7.1	3.51 x 10 ⁻⁵	2.23 x 10 ⁻⁵	2	1	4.46 x 10 ⁻⁵	4
S7.2	5.00 x 10 ⁻⁵	2.64 x 10 ⁻⁵	2	1	5.28 x 10 ⁻⁵	5
S9	3.05 x 10 ⁻⁵	2.10 x 10 ⁻⁵	1	1	2.10 x 10 ⁻⁵	2
S10.5	7.60 x 10 ⁻⁵	7.60 x 10 ⁻⁵	1	0.5	3.80 x 10 ⁻⁵	4
Cumulative Risk (24/7 for 1 year) Job Function <i>Basis: 24 hour operation</i>					1.02 x 10 ⁻³	
Risk to Particular Person carrying out that job function <i>Basis: 8 hour shift pattern for 230 days [fraction present = 0.21]</i>					2.15 x 10 ⁻⁴	

EXTERNAL OPERATOR (UNIT 4)

Cumulative Individual Risk of Death (Job Function) $9.42 \times 10^{-5} \cdot \text{yr}^{-1}$

Cumulative Individual Risk of Serious Injury (Job Function) $1.02 \times 10^{-3} \cdot \text{yr}^{-1}$

Basis: 24 hour operation, 7 days a week

Serious Injury - consequences ≥ 3 persons

Table 3: Example risk summary tables for a specific job function.

5.5 HSE's tolerability of risk (TOR) framework

The HSE 2001 publication 'Reducing risks, protecting people: HSE's decision-making process' (R2P2), set down the general approach used by the HSE for making regulatory decisions. The document made it clear that R2P2 was not intended as guidance for dutyholders. R2P2 also explained that those who want to emulate the regulators' approach, have to recognise the different contexts in which HSE applies its framework; taking this into account when applying it to their own decisions. This CDOIF guideline outlines an appropriate process for COMAH Operators to follow. The risk tolerability framework for 'major hazard human harm risk assessment' is explored below (also see **Figure 10**).

R2P2 principles are not sector specific, and could be applied to activities ranging from an individual carrying out a simple work activity, through to major accidents affecting many people in different locations. This means it does not specifically consider cumulative risks to the person from an establishment, with multiple scenarios driven by random failures. Also, its focus was on the risk of death, not serious danger as required by COMAH; this was problematic as many MAHS, as well as historic major accidents, do not result in death but in many seriously injured people.

R2P2 uses the concept of 'individual risk', but due to the document's general nature, in that context it can mean either a single risk, or cumulative risk. It does not specifically consider cumulative risk to people from multiple scenarios on larger sites, so it does not extend the definition to job function, but stops at the less specific, and therefore more onerous 'hypothetical person'. R2P2 is dealing with risk to an individual, not considering the person at the greatest cumulative risk in an on-site or off-site population.

R2P2 suggests that for risks where there is no viable alternative and no further measures are available, the threshold of tolerability is $1 \times 10^{-3} \cdot \text{yr}^{-1}$ for workers on site, and $1 \times 10^{-4} \cdot \text{yr}^{-1}$ for the public. The boundary for residual risk of death is considered higher on-site than off-site. This is because workers on site are considered to have an element of voluntary risk and benefit from the activities being carried out. It should be noted that there are few activities that would have a risk approaching $1 \times 10^{-3} \cdot \text{yr}^{-1}$, these would include a Deep Sea Trawler in remote waters. For comparison, one of the greatest onshore risks is mining, which has an individual risk (job function) of death of just over $1 \times 10^{-4} \cdot \text{yr}^{-1}$.

The cumulative risk (job function) on a site is normally between $1 \times 10^{-4} \cdot \text{yr}^{-1}$ to $5 \times 10^{-6} \cdot \text{yr}^{-1}$. If the residual risk of either a single scenario, or cumulative risk, is below $1 \times 10^{-6} \cdot \text{yr}^{-1}$, it does not mean that the scenario can be ignored, written off as 'not credible', or left undeveloped because it is 'broadly acceptable'; the scenarios still need to be developed and a case made. It is only where the total initiating event frequency is less than $1 \times 10^{-7} \cdot \text{yr}^{-1}$, that scenarios can begin to be considered as 'not credible'.

5.5.1 Consideration of TOR framework against serious injury

The 2001 HSE 'tolerability of risk' or 'TOR' framework only considered death; so does not fully consider 'serious danger' (or 'harm to people') which the Operator is required to assess. A 'dangerous dose' as defined by HSE represents at least a serious injury to even the most resilient in a normal population, and will lead to approximately 1/3 of the normal population being killed.

A reasonable basis for the application of the R2P2 'tolerability thresholds' for serious danger, is **'the cumulative risk from Major Accident Hazard Scenario(s) that lead to death, OR lead to three or more serious injuries occurring'**. (It should be noted that R2P2 has been withdrawn and archived.)

This approach is already used by some Operators. From an economic and social cost, it is also considered that a three to one ratio is appropriate. This ratio allows the frequency of serious injuries to inform decisions on the requirement for, and the assessment of, 'further measures'. Operators are free to use other approaches, as long as both death and serious injury are assessed, and an appropriate rationale is provided.

5.5.2 HSE's societal risk of death

It is accepted that society's concern increases with the number of people that are killed in a single incident. Also, that there is greater concern for multiple deaths at a single incident rather than the same number of deaths occurring over many separate incidents. This is sometimes described as 'aversion' or 'societal risk of death', but is often incorrectly shortened to 'societal risk'. Societal risk of death is often represented by a graph plotting frequency (F) of scenario against number (N) of fatalities to produce an FN curve often using a logarithmic scale.

R2P2 proposes that the tolerable thresholds for societal risk are given by a line with a slope of minus one on a log/log plot of Frequency vs Number of fatalities, passing through a point representing 50 fatalities at a frequency of $2 \times 10^{-4} \text{ yr}^{-1}$. The criteria are based on an assumption that the permitted likelihood of an incident which kills 100 people, or more; should be 10 times lower than an incident which kills 10 people or more. It should be recognised that in most cases FN curves are an artificial concept in that all scenarios do not normally affect all the people in and around site, so do not realistically represent societal risk. However, FN curves could be considered to be a cautious representation. There are no recorded cases where a site has a tolerable cumulative individual risk, but an unacceptable societal risk. However, given the ease of assembling the information, and a clear metric, it should be included.

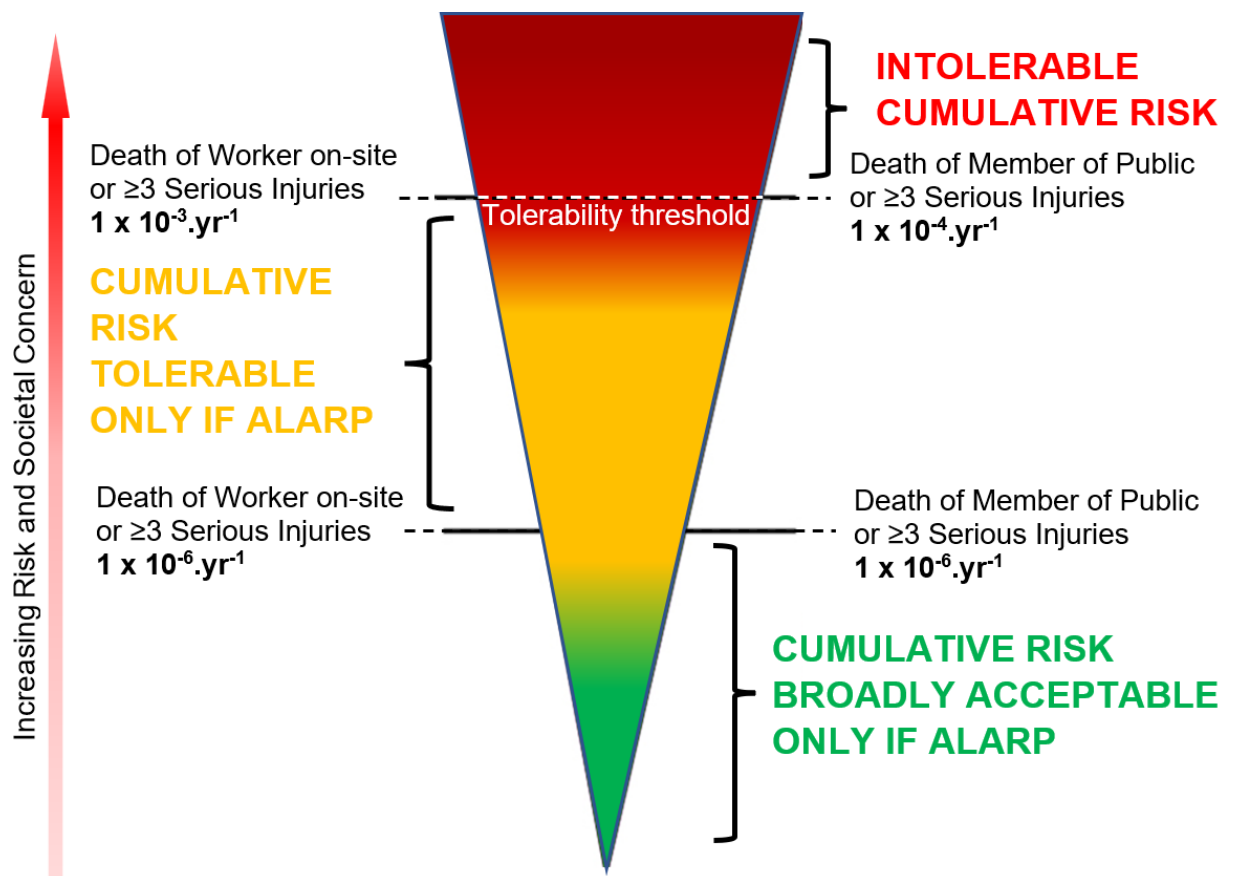


Figure 10. HSE 'tolerability of risk framework' showing the numerical boundaries between tolerability regions, for death, and also serious injury.

5.5.3 Assessing societal risk in terms of both death and serious injury

Major accident hazard scenarios may result in deaths, serious injuries, or a permutation of both. The R2P2 societal risk criterion only considers deaths. Where a MAHS results in more than a single death, or more than three injuries, the separate criteria above cannot be applied. It is required to be able to assess numbers of deaths and injuries in any combination as a continuum. As discussed in the previous paragraphs, if the societal impact of a single death is considered to be equivalent to three serious injuries, the severity of both deaths and serious injuries can be evaluated by:

$$\text{Equivalent number of deaths, } N' = \left(\begin{array}{c} \text{number fatalities} \\ \text{from that scenario} \end{array} \right) + \left(\begin{array}{c} \text{number serious injuries} \\ \text{from that scenario}/3 \end{array} \right)$$

The R2P2 societal risk of death criterion can then be extended to encompass both death and also serious injuries with the same degree of aversion. The societal risk criteria for both death and serious injuries becomes represented by a line with a slope of minus one on a log/log plot

of Frequency vs Number of fatalities, passing through a point representing '50 deaths or their equivalent' at a frequency of $2 \times 10^{-4} \text{ yr}^{-1}$; see **Figure 11** below.

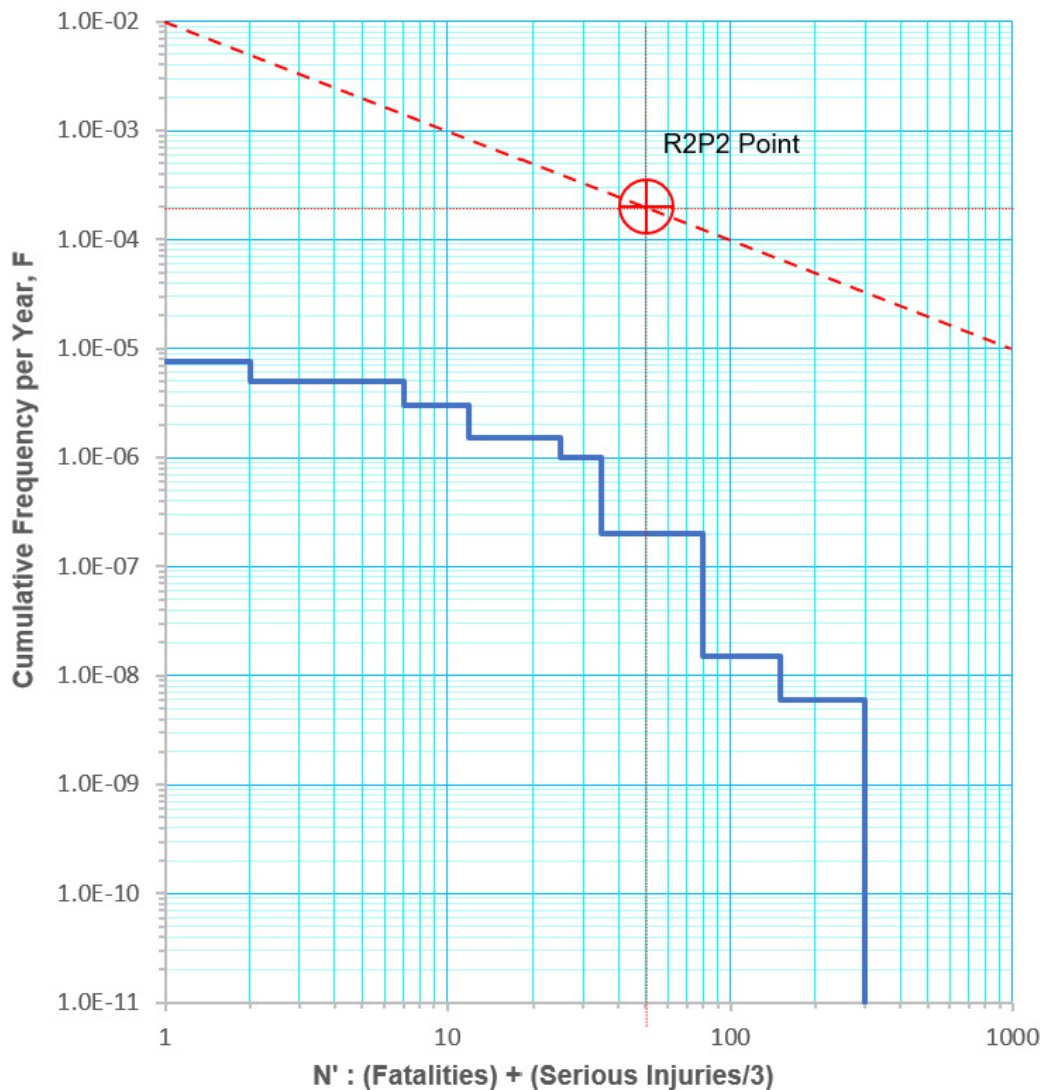


Figure 11: FN' curve and relation to R2P2 point.

5.6 Establishment cumulative risk summary

The assessment process should conclude with the following metrics:

On-site

- Job function which has the greatest cumulative risk of death.
- Job function which has the greatest cumulative risk from MAHS which result in three or more serious injuries occurring.

Off-site

- Location at greatest cumulative risk of death (hypothetical person).
- Location at the greatest cumulative risk (hypothetical person) from MAHS which result in three or more serious injuries occurring.

- Location at greatest cumulative risk of death (hypothetical person) **day-time**.
- Location at the greatest cumulative risk (hypothetical person) from MAHS which result in three or more serious injuries occurring **day-time**.
- Location at greatest cumulative risk of death (hypothetical person) **night-time**.
- Location at the greatest cumulative risk (hypothetical person), from MAHS which result in three or more serious injuries occurring **night-time**.

(for the purposes of assessment, it can be assumed 'day-time' is 7am to 7pm; 'night-time' is 7pm to 7am).

On-site and off-site

The following are normally included:

- Societal risk F/N' curve [(risk of death) + (serious injuries/3)].

It is suggested the following are also included in any summary:

- Representative MAHS risk table grouped by intuitive area (**see Table 1**).
- Risk summary for the cumulative individual risk (job function) for the job function at highest risk of death and/or serious injury if different (**see Table 3**).
- Risk summary for off-site resident at highest risk of death and/or serious injury if different (**See Table 4**). In some cases, the summary will require further subdividing into day-time and night-time MAHS/populations.
- Summary table of risk job functions sampled.
- Supporting population maps and lists.

OFF SITE RESIDENT (SYDNEY AVENUE) CUMULATIVE RISK OF DEATH						
Relevant MAHS	Frequency of Scenario .yr ⁻¹	Frequency of Scenario leading to death .yr ⁻¹	Multiplier (number of times represent used)	Fractional Time Exposed To Scenario	Risk of Death .yr ⁻¹	Contribution %
S7.1	3.51 x 10 ⁻⁵	1.10 x 10 ⁻⁵	1	1	1.10 x 10 ⁻⁵	100
Cumulative Individual Risk (Hypothetical Person) (Basis: Present 24 hours, fraction present =1)					1.10 x 10⁻⁵	

OFF SITE RESIDENT (SYDNEY AVE) CUMULATIVE RISK OF SERIOUS INJURY(Consequence ≥3 Persons)						
Relevant MAHS	Frequency of Scenario .yr ⁻¹	Frequency of Scenario leading to Serious Injury (≥3 person) .yr ⁻¹	Multiplier (number of times represent used)	Fractional Time Exposed To Scenario	Risk of Serious Injury (≥3 person) .yr ⁻¹	Contribution %
S7.1	3.51 x 10 ⁻⁵	1.10 x 10 ⁻⁵	1	1	1.10 x 10 ⁻⁵	34
S9	3.05 x 10 ⁻⁵	2.10 x 10 ⁻⁵	1	1	2.10 x 10 ⁻⁵	66
Cumulative Individual Risk (Hypothetical Person) (Basis: Present 24 hours, fraction present =1)					3.20 x 10⁻⁵	

OFF SITE RESIDENT (SYDNEY AVENUE)	
Cumulative Individual Risk of Death (Hypothetical Person)	1.10 x 10⁻⁵.yr⁻¹
Cumulative Individual Risk of Serious Injury (Hypothetical Person)	3.20 x 10⁻³.yr⁻¹
Basis: Present 24 hours Serious Injury - consequences ≥3 persons	

Table 4: Example risk summary tables for off-site resident.

Person at Risk	Exposure to Major Accident Hazard Scenarios	Cumulative Risk of Death (job function) .yr ⁻¹	Cumulative Risk of Serious Injury (job function) (≥3 person) .yr ⁻¹	Cumulative Risk of Death (named person) .yr ⁻¹
Main Control Room Operator (Seat C)	S2, S7.2	1.1 x 10 ⁻⁵	2.8 x 10 ⁻⁵	2.2 x 10 ⁻⁶
External Operator (Unit 4)	S1, S2, S5, S7.1, S7.2, S11	9.4 x 10 ⁻⁵	1.0 x 10 ⁻³	1.9 x 10 ⁻⁵
Security Guard	S1, S2, S4, S5, S6, S7.1, S7.2, S8	2.5 x 10 ⁻⁵	2.5 x 10 ⁻⁴	5.0 x 10 ⁻⁶
Main Office Block Staff	S4, S7.1	6.5 x 10 ⁻⁵	6.5 x 10 ⁻⁵	1.3 x 10 ⁻⁵
Off-Site Resident at most Risk (Hypothetical Person)	S7.1, S9	1.1 x 10 ⁻⁵	3.0 x 10 ⁻⁵	-

Table 5: Summary of individual risk job functions sampled.

5.6.1 If the cumulative risk tolerability threshold is exceeded

It is possible that there may be unexpected local risk 'high spots' of cumulative risk on site. This is normally an indication that either the risks are not tolerable, or that the assessment is not of sufficient resolution. For example, if a representative unit operation has some members operating at low pressure and some members operating at high pressure; when they are all represented by the high-pressure exemplar, this will increase the apparent risk. Using a high pressure representative, and a low pressure representative, could dramatically reduce the calculated levels of risk if there are multiple members represented by the same scenario.

It is clear that the risk of pipeline failure in a long continuous section, above ground, that is well supported, with no component penetrations; is different to a section that has many flanges, many valves, drains, branches, instrument tappings, and injection points. A simple failure rate per metre, 'loss of containment all modes', may over-estimate the risk in the first case, and under-estimate the risk in the second. Where many lines cross any conservatism is multiplied, sometimes to the point where the risk appears unacceptable. This can be simply because a low resolution study may use a loss of containment 'all modes' expressed as a failure rate per metre. In these cases, it may be required to go down to a greater degree of resolution, by carrying out the analysis at the level of pipeline components, though this is not commonly required.

If the risk from the establishment is found to be intolerable, **see Figure 10**, it is suggested that the Operator should first review the site risk profile, and also the individual cumulative risk summary tables. The tables should indicate the scenarios contributing the greatest risk, which may be due to either, sole MAHS, or representatives which represent a number of similar unit operations in one location. The largest contributors can then be re-examined in greater detail, in order of their contribution. If the risk from the establishment is still intolerable, the operator should then consider if all appropriate measures are in place for the high contributors, particularly where there are multiple similar unit operations in close proximity. In

extreme cases, it may require modifying or replacing a unit operation, or even using a new technology which is becoming best practice.

5.6.2 If cumulative risk tolerability threshold is not exceeded

If it is found that the cumulative individual risk of both death and serious injury, from the establishment are broadly acceptable (**see Figure 10**); this does not on its own show that the risk has been reduced so far as is reasonably practicable (ALARP). To achieve ALARP, possible credible further measures must be determined, then the reduction in risk achieved by those measures balanced against the additional costs; this process is considered in **section 6, Further risk reduction measures**.

5.7 Periodic review and revision

Section 7 of this guideline outlines the general requirement that the Operator's SMS must be based on an assessment of the risk, and should include an outline of the Operator's approach to achieving a suitable and sufficient MHHRA, for all unit operations at the establishment.

For assessment, review is expected as new information (for example, from the identification and analysis elements of MHHRA) becomes available.

6. Further risk reduction measures

MAHS analysis and assessment should have demonstrated that:

- the unit operation's design has properly considered the hierarchy of control measures;
- the unit operation at least meets relevant good practice (RGP), **refer section 4.10**; or employs an approach from first principles which identifies MAHS event combinations, and shows how these are prevented by the control measures and systems of safety;
- cumulative risk from the establishment to a person on-site or off-site is shown to be below the tolerability threshold.

Though the cumulative risk from the establishment may have been shown to be below the tolerability threshold, the risks may not necessarily have been reduced to be 'as low as reasonably practicable' (ALARP). This section discusses the test of 'reasonable practicability', how further measures could be identified, shortlisted, then evaluated.

6.1.1 What is a MAHS further measure?

Section 4.10 explains that Operators should have identified the appropriate measures needed for each of the event combinations that can lead to a MAHS. **Section 6.2.1** highlights the need for existing establishments to do a gap analysis against RGP, when RGP or supporting standards have changed. An additional measure needed to meet current RGP is not considered a further measure.

In the context of this guidance: a 'further measure' is any additional, reasonably practicable control, safeguard or mitigation; that has not already been implemented; that would lead to an additional reduction in risk, or a reduction in the number of people which would be killed or seriously injured. In cases of high proportionality where single scenarios give rise to a high risk of death $\sim 0.5 \times 10^{-4} \text{ yr}^{-1}$, or multiple off-site fatalities, consideration of further measures should also include replacing the unit operation with a process which is inherently safer.

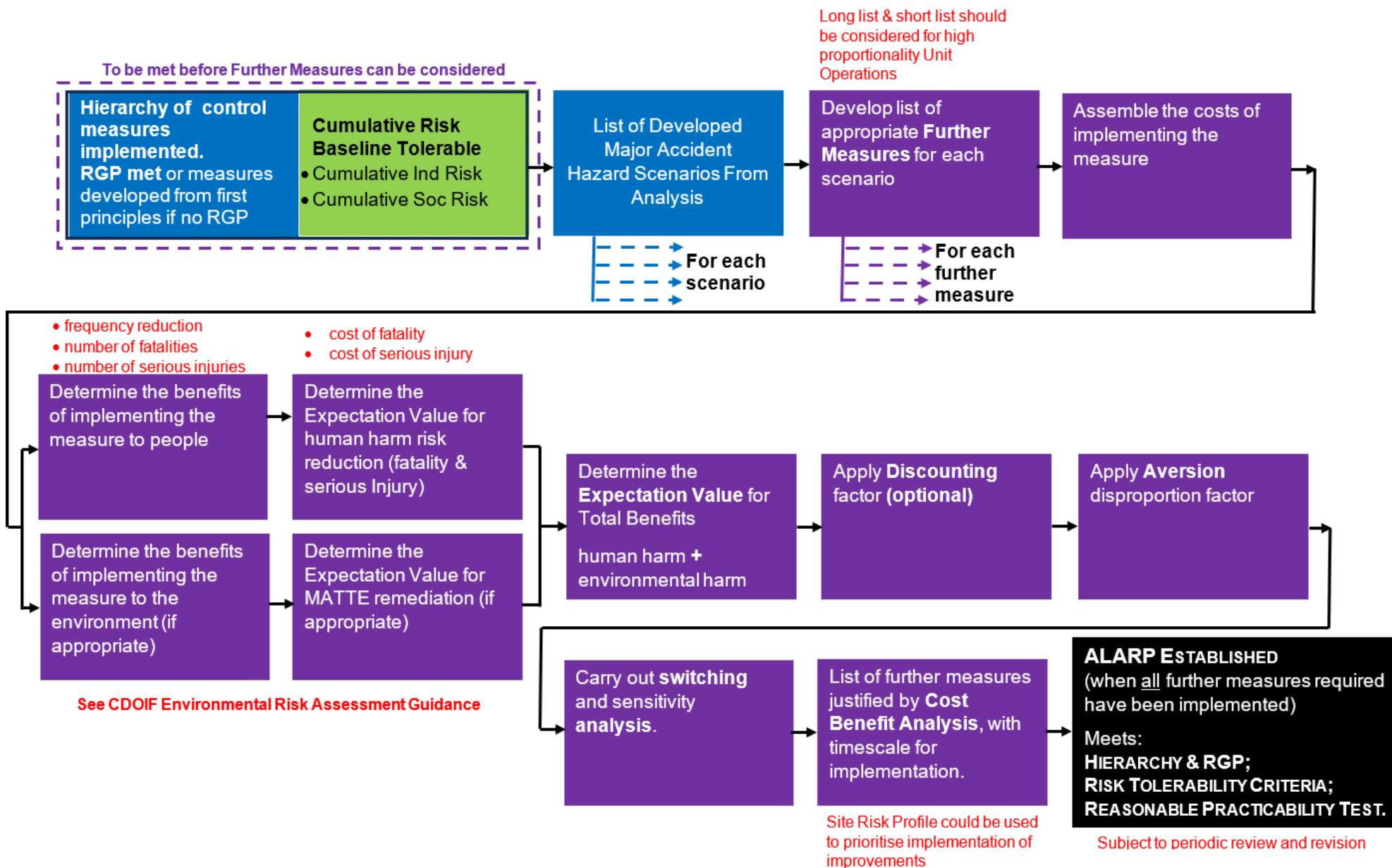
As part of MHHHRA, further practical risk reduction measures should be considered, listed, and evaluated (this includes MAHS occurring in both new and existing unit operations, major vessels, and major equipment items). Replacement of an asset when it is life expired, or when it reaches a point where degradation before failure cannot be reliably detected or revealed, is not a further measure.

Only when the 'analysis' of the MAHS has been completed, and the 'assessment' of 'cumulative risk from the establishment to a person on-site or off-site' has also been completed, should further measures be evaluated. This is because the degree of consideration should be in proportion to the contribution to individual risk, the number of people that are exposed to that scenario, and the number of people that would be subject to death or serious injury should the scenario occur.

As most MAHS lead to loss of containment, the consequences often result in a corresponding major accident to the environment (MATTE). Whilst this section predominantly deals with harm to people, the evaluation of further measures also includes the benefits of reducing any associated risk of MATTE (refer as necessary to the CDOIF 'Environmental Risk Tolerability Guideline for COMAH Establishments', and COMAH Competent Authority (CA) 'All measures necessary - Environmental aspects guidance'¹³).

¹³ COMAH CA, 'All measures necessary – Environmental aspects guidance'. COMAH CA.

IDENTIFICATION → ANALYSIS → ASSESSMENT → FURTHER MEASURES



Flow Diagram 7 – Further Measures

6.1.2 Are further measures still required if a system meets RGP?

Where MAHS can occur in packaged units, such as boilers and fired heaters, which have been designed to specific current standards; supply a service main (are not a direct part of a unit operation); and fully comply with current standards, including 'The Supply of Machinery (Safety) Regulations 2008': this would then give the assurance needed that appropriate measures are in place and it is not necessary to consider further measures. However, where the packaged unit directly interacts with the process, such as gas/vapour compressors, or may require emergency disburdening or shutdown, then further measures should still be examined, taking reasonable action as necessary.

6.1.3 The relationship of further measures to reasonable practicability and 'all measures necessary'

The 'Health and Safety at Work etc. Act 1974' states that:

- 'It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees' (section 2(1)).
- 'It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety' (section 3(1)).

HSE uses case law to understand the legal interpretation of 'reducing exposure to risks so far as is reasonably practicable' (SFAIRP). Case law is the set of rulings from court judgements that set precedents for how the law has been interpreted and applied in certain cases. Case law in this area includes *Edwards vs Coal Board* [1949].

HSE's guidance on risk assessment for dutyholders states that reasonably practicable means balancing the level of risk against the measures needed to control the real risk in terms of money, time, or trouble. However, dutyholders do not need to take action if it would be grossly disproportionate to the level of risk.

This effectively means that further measures beyond the hierarchy of control, RGP, or the appropriate measures from a first principle (if RGP is not available); are to be implemented unless the cost passes a point where it is not proportionate to the benefit (a reduction in risk to people). The Health and Safety at Work Act (HSWA) sets down the guiding principles; it is not sector specific, and could be applied to activities ranging from an individual undertaking a simple work activity, through to undertakings where major accidents can affect many people in different locations. HSE refers to the legal requirement for risks to be reduced SFAIRP, as the 'as low as reasonably practicable' principle, or ALARP.

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.' For major hazards resulting in human harm, COMAH sits within the HSWA framework and 'all measures necessary' requirements are under SFAIRP (ALARP principle).

It is a commonly held misunderstanding that ALARP is solely based upon reaching the stated risk threshold (for example, those given in **section 5, Figure 10**), and that there is no requirement to go beyond. This is incorrect, there is still the requirement to apply SFAIRP (ALARP principle), and to consider if it is reasonably practicable to adopt further measures for the given unit operation being considered.

6.2 Producing a list of further measures

For each MAHS, a list of further measures should be assembled and evaluated. At this stage, inherent safety and appropriate measures should have already been considered (**see section 4.10**). In accordance with the hierarchy of control measures, emphasis should first be placed on increasing effective control to reduce demand on safety systems.

The nature of the further measures considered will depend on the process, the age of the plant, cumulative risk, and appropriate measures already in place. The list is normally generated by a team considering general areas such as:

- current standards/approved codes of practice (ACOP)/industry guidance reviewed against those in place at the time of installation;
- additional loss of containment measures not already in place;
- known additional/further measures already in use at another establishment operating the same or similar process;
- additional measures raised in previous periodic reviews/assessment;
- automation of a safety critical manual operation;
- process improvements leading to significant risk reduction;
- relocation or protection of occupied buildings; and
- consideration of additional control measures and diagnostics.

6.2.1 Gap analysis: standards, ACOP and industry guidance (SAIG)

SAIG tend to be revised with changes in industry practice, technology, and in response to international major accidents. It would be expected that the Operator has a mechanism embedded in their safety management system to monitor pertinent standards for their high hazard unit operations and equipment. As part of that process, it would be expected that a gap analysis be undertaken when revised SAIG are published.

It may not be possible to make retrospective changes to an existing system, such that it fully meets a new, or revised, SAIG. Alternative systems may need to be installed which achieve the same end through a different mechanism. If it is found that there is no significant reduction in risk between the measures already in place, and the necessary changes needed such that the system complies with SAIG (or has equivalence), the gap analysis should record those reasons.

If it is found that additional measures are required to satisfy the revised SAIG in order to then meet RGP, these are not considered further measures, but are appropriate measures that should be in place, see also **section 4.10.1**.

6.2.2 Some examples of common improvements considered

The following lists of some common improvements are only intended to illustrate the general areas suggested, they are neither exhaustive or prescriptive. Further measures considered will depend on the particular site, the specific processes performed, and the actual event combinations that lead to the MAHS.

Additional loss of containment measures not already in place

These could include:

- change from a single to double mechanical pump seals for high hazard materials;
- change from mechanical seals to a magnetic drive seal-less pump for very toxic materials;
- reduction of inventory held in movable containers or container size;
- inventory reduction of process intermediates;
- earth berm bund replacement;
- use of separate emergency shut-off valves (ESD system) to isolate or limit source term on loss of containment;
- mechanical overflow system;
- independent high level detection and shut-off;
- automated remote isolation;
- automated valve routing with position feedback for storage tank systems;
- use of double wall piping for very toxic substances, in sensitive areas; and
- move to total containment (hierarchy of control measures).

Storage tanks:

- floating roof tank 'roof tilt' detection;
- bund hydrocarbon detection;
- high integrity protection systems (HIPS) overfill protection; and
- reducing fill rate below that at which overfill will create conditions for vapour cloud explosion (VCE).

Process improvements leading to significant risk reduction

These could include:

- move from an 'all-in' batch process to a feed rate limited regime;
- change from batch to continuous operation;
- change to an inherently safer chemical reaction route;
- dedicated emergency cooling water supply;
- inerting;
- addition of a recipe handler to a batch control system handling multiple exothermic reactions;

- dump tanks, or injection of an inhibitor; and
- new technological developments.

An example of new technology is the use of ionic liquids for alkylation to replace hydrofluoric acid in existing Hydrogen Fluoride (HF) Alkylation units, often referred to as ISOALKY technology.

Relocation, or protection, of occupied buildings

Many older establishments have offices and control rooms which are connected to, or contiguous with, the process plant building; in some cases these are separated only by an internal window. Wherever possible, people should be separated from the risk. The occupants of offices that are part of plant buildings could be moved away to an administration building away from the process area. Control rooms could be moved to a safe distance, or further protected against the particular hazard. The location of the control system and control room should consider the requirement to return the plant to a safe stable state after an MAHS has occurred.

Consideration of additional control measures and diagnostics

These could include:

- change to dual diverse measurement on control and safety systems;
- change from relief valves to a high integrity pressure protection system (HIPPS); and
- move from 'indirect' to 'direct' detection of a measured variable used to ensure the plant is in the safe operating envelope.

For example, the outlet stream from a water-cooled condenser may be fitted with a temperature sensor to detect condenser failure, and ensure the condensate is sub-cooled to a temperature below which it can create a flammable atmosphere. A more direct indication of cooling water failure would be to fit a flow switch in the cooling water outlet, as well as measuring the temperature. This would give a much earlier indication that the cooling water supply has failed and give more time to bring the plant back to a safe stable state.

6.2.3 Extent to which further measures should be explored

There is no target number of further measures that must be found, then evaluated. Clearly the extent to which further measures should be explored is proportionate to the importance of each particular scenario. An MAHS that leads to multiple on-site and off-site fatalities with a frequency of $10^{-4} \cdot \text{yr}^{-1}$, clearly should have much more time spent on investigating possible further measures and evaluating them, than an MAHS that leads to two serious injuries with a frequency of $10^{-6} \cdot \text{yr}^{-1}$. In many cases a further measure will contribute to risk reduction in many scenarios associated with the same unit operation, therefore the proportionality of the unit operation itself should also be taken into account when considering further measures (**see section 2.3**).

Identifying and evaluating further measures should be defined as a specific part of the safety management system (SMS), by procedure or other. To show that a conscious effort has been made to identify possible further measures, then to evaluate them as thoroughly as the proportionality of the measure warrants, the application of this process should be demonstrated. This is best achieved with examples given for a sample of MAHS, showing how the range of individual risk and consequence has determined the depth, resolution, and

robustness of the evaluation performed. Perhaps for a site with a large number of scenarios, the development of further measures for a sample of those MAHS, should be given in full.

6.2.4 Longlisting and shortlisting

Longlisting and shortlisting are not necessary for every scenario. The aim of longlisting and shortlisting is not to show exhaustion, but to transparently show how many possible practical measures for a high proportionality scenario have been effectively reduced to a small number of measures which will be subject to detailed evaluation. It is suggested that this is carried out in a tabular form, scoring against simple criteria, sometimes referred to as 'critical success factors'. If a scoring system is used, it is important that it is not accidentally constructed to be biased against introducing further measures. It is the Operator's responsibility to develop the rationale for the process put in place to move from the longlist to the shortlist. The Operator should also consider using 'disproportion factors' where appropriate. These are discussed further in **section 6.8, Aversion**.

Bundling of measures

Further measures may be overlooked or dismissed if they are 'bundled' together into a scheme. This can be because those measures of greater cost and corresponding low risk reduction within that same bundle, may negate those of lower cost and greater risk reduction. By the same token, a single trip when evaluated on its own could have a disproportionately high cost, as it requires not just a sensor and valve, but a logic solver and all the associated marshalling. However, if it is evaluated with other further trips and interlocks on the same unit operation (or system), then they share the cost of marshalling and the logic solver, so changing the relative cost.

Shortlists

For high-risk MAHS, or where the scenario leads to large numbers of deaths and/or serious injuries; it would be expected that there is a second more detailed consideration of further measures known as a 'shortlist'. Shortlisting would only be necessary where a large number of competing solutions needs to be reduced, before more in-depth consideration is made. Evaluation of shortlisted measures should be proportionately detailed, and not based on a simple scoring table.

6.3 Evaluation of further measures

It was explained in **section 6.1.3** that reasonable practicability is judged to be the point at which the cost of the measure is not disproportionate to the risk reduction achieved. The point beyond which the measure could be considered disproportionate can be expressed as when the 'cost of implementing the measure' begins to exceed 'the benefits of the risk reduction'.

Monetisation

To enable the comparative evaluation of the measure, the risk reduction must be expressed in the form of currency, so it can be balanced against the total cost of implementing the measure; this is sometimes referred to as 'monetisation'. If the addition of the measure is obvious and the Operator is going to implement it, then a cost-benefit analysis (CBA) is not needed. However, if the Operator is arguing not to implement a measure, a CBA is required, with an explanation of why a measure has been discounted.

Cost-benefit analysis

The process of comparing the 'costs' of implementing the further measure, with the 'benefits' gained (reduction in human harm and damage to the environment), is usually referred to as 'cost-benefit analysis' (CBA). When the benefits outweigh the costs, the further measures

should be implemented. For MHHHRA this benefit is normally expressed as a net present value in pounds sterling.

$$\text{Cost-benefit (at net present value)} = \frac{\text{total human harm and environmental benefits of introducing the safety measure}}{\text{}} + \frac{\text{*third party costs, *damage to the establishment, *business interruption costs}}{\text{}} - \frac{\text{total costs of introducing the safety measure}}{\text{}}$$

In this guideline, the 'benefits' must include both the reduction of human harm and damage to the environment. The 'costs' include the capital cost of installing the measure, and if applicable, any associated increased operational costs. It is recommended that the 'benefits' also consider the costs that would be associated with avoiding or reducing: *damage to the establishment, *business interruption costs (**see section 6.3.2**) and also *third party costs (**see section 6.4.4**). It should be noted that CBA can also be expressed as a ratio of costs to benefits, though this is not recommended as it does not give the transparency of declaring the present value gained from implementing the measure.

In practice, it is essential to ensure all the costs and benefits are included and explained. It is likely that the regulator will challenge where: the costs appear extraneous or excessive, if all the benefits are not included or they are underplayed. It is therefore important to give a logical justification that is transparent and reflects the proportionality (**see section 2.3**) of the MAHS under consideration. Nothing that where the further measure can prevent more than three deaths, or more than six people being seriously injured, aversion should be considered (**see section 6.8**).

6.3.1 Assembling the costs of implementing the further measure

The costs to introduce the further measure, should only be those 'necessary and sufficient' for the purpose of implementing the risk reduction measure. These will normally be:

- capital cost of the equipment package;
- capital cost of installation;
- change in revenue cost of basic operation/production;
- change in revenue cost of maintenance;
- change in revenue cost of training;
- decommissioning of any plant replaced by the measure.

It should be noted that the 'decommissioning' cost, does not include the future cost of decommissioning the further measure itself.

Cost of installation

The complete costs of installation of the further measure should be included; this may not just include the physical modification or installation of plant. The costs of installation can include bridging the gap in production by building stock in advance, or loss of profit from lost or deferred production. In the case of building stock in advance (either of the final product, or intermediates stockpiled to allow production to continue), this would include the interest on any money invested between expenditure and return.

The cost of lost production when the further measure is installed as part of a general outage should not be included. If the lost production costs are a strong influence on a decision not to implement, the Operator should show that phasing or scheduling the work to coincide with

planned downtimes (for example, maintenance) would not change the balance in favour of implementation. Costs for routine replacement of equipment alongside the further measure, that would not significantly reduce risk, should not be included in the cost.

Example: fitting a vacuum relief valve to a storage tank normally let for commercial storage. If a storage tank is emptied and inspected routinely, then there would be no lost profits due to the installation of a vacuum relief valve during that inspection. However, if the tank must be taken out of service just for the installation of the valve, lost revenue may be taken into consideration.

Change in cost of basic operation/production

The further measure could increase production costs, for example: because of more expensive raw materials, lower rates of production, or reduced capacity. If a decision was made not to hold consignment stock of raw materials in order to reduce the amount of hazardous material at risk, and this led to increased raw material costs; this would also be taken into consideration.

Change in cost of maintenance

If the further measure increases the cost of maintaining the plant, over the current system, due to the increased frequency required, and/or its complexity; this should be included in the costs. Similarly, if a measure reduces a maintenance requirement this should be seen as a benefit.

Training costs

If retraining of staff is necessary to deploy the further measure, or further training would be required, this should be added to the cost of the measure. However, if this is part of routine training, then it should not be included.

6.3.2 The benefits of implementing the further measure

The benefits of implementing the measure are the potential costs saved due to the consequence(s) of the MAHS not occurring.

The stated scope of this document is MHHHRA (with links to the CDOIF Environmental Assessment Guidance as appropriate). However, when evaluating further measures, this differs from the analysis and assessment of MAHS, in that the reduction in risk of a MATTE must be included as well as the reduction in harm to people. This approach is further supported by the COMAH definition of 'serious danger' which includes MATTE, as well as death and serious injury. If a CBA study were to consider 'harm to people' and 'damage to the environment' separately, further measures that give benefits to both may not meet the reasonable practicability test; but may when the benefits are considered together.

The following costs are considered when evaluating benefits:

- fatality,
- serious injury,
- business interruption,
- rebuilding/replacing plant, and
- damage to the environment.

It should be noted that the inclusion of business costs could be beneficial to the CBA, but that the focus of this guidance, and the following examples in this section, is on safety and environmental costs.

Cost of a fatality

The cost of a single fatality has been calculated from data submitted by HSE using the 'Cost To Britain Model'. This value is recognised by the UK Government, and used in Cost-Benefit Analysis by the Treasury. The data is available in the form of an annual report 'Costs to Britain of workplace fatalities and self-reported injuries and ill health'¹⁴ published on the HSE website, **see Table 6** below. The figures contained in 'Costs to Britain' are based on a three-year rolling average. *As such, the latest average figures are for 2023/24, this being the middle of the three-year interval, and are set in 2024 prices². The Operator should project the cost to the date the further measure would be installed, using the current rate of inflation.

	Human cost (rounded)	Financial cost (rounded)	Total cost (rounded)
Fatal injuries	1 632 000	553 100	2 185 000
Non-fatal injuries	6 000	4 000	10 000
7 or more days absence	27 700	16 600	44 300
Up to 6 days absence	450	740	1 190
Ill health	12 800	11 300	24 200
7 or more days absence	26 600	23 000	49 500
Up to 6 days absence	440	810	1 250

Table 6: Cost to Britain per case 2023/24 - average appraisal value estimates (2024 prices* in £ Sterling).

The Operator could use an alternative value, but its derivation should be justified. It should be noted that this is likely to be compared to the Cost to Britain Model by the regulator.

Cost of a serious injury

The Treasury 'Green Book'¹⁵ considers all of the associated costs that would occur if the employee(s) involved in the incident were absent as a 'benefit', to be balanced against the 'costs'. These can include:

- time taken for a replacement to learn the new role and become productive;
- possible diminished services and product quality;
- loss of business, continuity and reputation;
- recruiting temporary or replacement staff;
- training and providing support to other staff;
- paying the salary of the absent employee;
- overtime incurred by other employees covering for the absent employee;
- loss of output incurred by the absent employee; and
- cost to the public sector of any care (hospital, social benefits etc.).

¹⁴ HSE, 'Costs to Britain of workplace fatalities and self-reported injuries and ill health'. HSE.

¹⁵ HM Treasury, (2026) 'The Green Book'. HM Treasury.

Of course, the cost of employee absence would be dependent upon the degree of injury and the time absent from work. A serious injury could require an extended period of absence, or result in the employee never returning to work due to permanent injury; or in an extreme case, a person may never return to work, and need round the clock care.

It is suggested that the cost of a serious injury is based on a person never returning to work, but not requiring round the clock care. The Operator may use an alternative figure for the value of a serious injury. However, it should, as a minimum, represent the mean cost of a serious injury, and take the aspects listed above into consideration.

6.4 Expectation value estimation

In order to monetise the benefits that accrue over the lifetime of the improvement, it is necessary to determine the expectation value of the reduction being considered over a specified period of time (this is often also referred to as the 'expectation value' (EV), its precise meaning depending on the context).

The benefits of the further measure may be to reduce any combination of the following:

- number of fatalities,
- number of serious injuries,
- MATTE,
- business interruption costs, and
- rebuilding costs.

The time being considered is from when the measure is to be introduced, to the remaining lifetime of the unit operation; this is known as the 'time horizon', and is considered further in **section 6.5**.

6.4.1 Expectation value estimation for human harm

Serious injury

Considering a scenario which just leads to serious injuries, the expectation could be expressed as:

$$EV_{FMS} = t_h \times F_{Sred} \times N_{Si} \times V_{Si}$$

With

EV_{FMS}	Expectation value, serious injury(ies) for particular scenario	£
t_h	time horizon for scenario	yr
F_{Sred}	MAHS frequency reduction after further measure implemented	yr ⁻¹
V_{Si}	Current value of a serious injury as defined	£
N_{Si}	Number of serious injuries should the MAHS occur	unitless

Death

The EV for fatality being given by substituting the subscript 'D' for death:

$$EV_{FMD} = t_h \times F_{Sred} \times N_D \times V_D$$

Human harm

So, the expectation value for human harm which is both death and serious injury is:

$$EV_{FMHH} = EV_{FMD} + EV_{FMS}$$

Intersection between numbers of fatalities and serious injuries

In terms of dose received, serious injury is a subset of the dose that would give rise to a fatality. A person who receives a fatal dose, has also in the process received a dose that would cause serious injury. If fatality and serious injury have been calculated separately, then the number of deaths should be subtracted from the number of serious injuries for the purposes of calculating EVs. If a scenario with a single consequence gives rise to 2 fatalities and 7 serious injuries, but not a MATTE; then a value of 2 would be used for the number of fatalities, and a value of 5 for serious injuries. Noting there is no EV intersection of human harm with a MATTE.

6.4.2 Calculating EVs for scenarios that give rise to multiple consequences

As discussed in **section 3** on MAHS identification, the top event for most scenarios is loss of containment. This can lead to many different consequences, especially when the dangerous substance is both flammable and toxic. Dependent upon the material, its release temperature and pressure, this may lead to: vapour cloud explosion, flash fire, pool fire or toxic exposure. Each consequence could have different numbers of fatalities or serious injuries.

A common simplification when ranking scenarios is to state the maximum number of fatalities and serious injuries from the possible consequences. If this is considered to be overly conservative, then the Operator can calculate an expectation value for each consequence and sum them. For example:

given -

scenario frequency before measure:	$3.2 \times 10^{-4} \cdot \text{yr}^{-1}$
scenario frequency after measure:	$4.01 \times 10^{-5} \cdot \text{yr}^{-1}$
value of a life:	£2 185 000
value of a serious Injury:	£90 000 (no return to work)
time horizon:	25 years from the installation date

S4. Large Loss of Containment HF Alkylation Unit (Toxic & Flammable) Human Harm EV_{FMHH}							
Scenario Frequency Reduction per year	Consequence	Consequence Frequency Reduction per year	Fatalities	EV _{FMD}	Serious Injuries	EV _{FMS}	Consequence Expectation Value Reduction
2.8 x 10⁻⁴	Pool Fire	2.8 x 10 ⁻⁵	2	3059	10	630	3689
	Flash fire	7.0 x 10 ⁻⁵	5	19119	20	3150	22269
	VCE	4.2 x 10 ⁻⁵	10	22943	20	1890	24833
	Toxic Exposure	1.4 x 10 ⁻⁵	40	30590	90	2835	333425
	Total Scenario (S4), Human Harm Cost Benefit, EV_{FMHH} =						£84 216

Table 7: Calculation of expectation value for human harm.

Please note that establishment and third party, business interruption and rebuild costs have not been included in this example, as this guidance is focused on human harm; a suggested approach is given in the text.

6.4.3 Expectation value for MATTE remediation

Guidance on the evaluation of MATTE scenario expectation values for environmental remediation, EV_{FMM}, is given in **section 5.5** of CDOIF Guidance 'Environmental Risk Tolerability for COMAH Establishments'.

6.4.4 Expectation value for business interruption and rebuilding costs

Establishment costs

The inclusion of establishment business interruption and rebuilding costs in the CBA is considered a holistic approach, as these costs would be borne by the Operator should the MAHS occur. However, the focus of this guidance is on human harm, so it takes the view that establishment business interruption and rebuilding costs, whilst beneficial to the Operator, are a supplementary consideration. If these costs are omitted, it is recommended that the Operator discusses the financial risk with their insurance company and/or board if self-insured.

Establishment business interruption and rebuilding costs would include:

- loss of inventory of product, intermediates, and raw materials;
- any compensation due to customers for failure to deliver;
- loss of profit on products not produced;
- any additional cost of providing alternative product from another supplier;
- cost of repair to bring the plant back into full production.

$$EV_{FME} = t_h \times F_{Sred} \times V_{IE}$$

V_{IE} Current value of establishment business interruption and rebuild £

Third party costs

In most cases damage caused by the MAHS to a third party outside the site boundary will be relatively minor compared to that experienced at the establishment. However, where businesses are co-located, or are an enclave, it would be expected that third party business interruption and rebuilding costs would have already been discussed with the Operator's insurance company and then included in the CBA; as if 'reasonably foreseeable' the Operator would almost certainly be liable. The estimate of the third party rebuild and business interruption costs should be included where they are significant. It is strongly suggested that the Operator discusses legal liability and any required provision/remedy with their legal team.

$$EV_{FMI_T} = t_h \times F_{Sred} \times V_{I_T}$$

V_{I_T} Current value of third party business interruption and rebuild £

6.4.5 Total expectation value for further measures

Total expectation value for the further measure is given as:

$$EV_{FMB} = EV_{FMHH} + EV_{FMM} + *EV_{FMI_T} + *EV_{FMI_E}$$

benefits human harm MATTE (Third party + Establishment)
business interruption & rebuild

**Business interruption and rebuild costs are outside the immediate scope of this guidance but are included here for completeness, the requirement to include them should be determined by the Operator.*

It should be noted that aversion should also be considered at this stage (**see section 6.8**).

6.5 Time horizon

The time horizon is the time period for which 'costs and benefits' from the further measure are accrued. In many cases, the projected lifetime of a unit operation involved will have been determined at the onset of the project to facilitate its construction. However, the time horizon is often only to determine returns from expenditure, and is not normally the operational lifetime.

The normal time horizon for consideration of a future measure on an existing plant is 20 years; for new plant a time horizon of 40 years should be taken. For time periods shorter than these a full justification should be given. Short-term horizons because of 'imminent closure' may be subject to scrutiny by the regulator.

Where the time horizon is uncertain, or leads to borderline rejection; sensitivity analysis should be carried out to assess the impact of the core assumption on the overall analysis.

The 'Green Book' contains further guidance and explains how to choose an appropriate appraisal period according to the type of improvement.

6.6 Discounting

Discounting is an accounting method used to compare costs and benefits that arise in different time periods. There is often an initial capital outlay in the first year of the appraisal

period, frequently referred to as 'year 0'; followed by flows of costs and benefits in subsequent years. The benefits from further measures are normally deemed to occur year on year. It is not necessary to apply discounting when evaluating further measures; but if discounting is applied, then it must be applied to **both** costs and benefits.

'Present value' is defined as the future value in today's terms.

'Net present value' (NPV) is defined as the sum of a stream of any future values that have been discounted to bring them to a present value.

Discounting is performed to account for the time preference of money. People have a preference to receive goods and services now rather than in the future. For instance, if offered £1 today, or £1 in five years' time; it would be much preferred to accept it today. To account for catastrophic risk, society will accept money today over the future, controlling for inflation. To account for this desire to consume today, a consistent weight is given to earlier rather than later costs/benefits by applying a 'discount rate'.

Using a discount rate to calculate NPV

Discount rates are used to calculate the NPV of a future cash flow, and are determined by the 'Green Book'.

There are two discount rates to consider when calculating further measures:

- i) **3.5%** where general costs are incurred i.e. capital;
- ii) **1.5%** for harm to the person, injury and ill-health.

6.6.1 Discounting the capital cost for the further measure

Applying a 3.5% discount rate, the table below shows the discount factors to be used in years 0 to 9 (over a ten-year appraisal period).

Year	0	1	2	3	4	5	6	7	8	9
Discount Rate	0.000%	3.500%	3.500%	3.500%	3.500%	3.500%	3.500%	3.500%	3.500%	3.500%
Discount Factor	1.0000	0.9662	0.9335	0.9019	0.8714	0.8420	0.8135	0.7860	0.7594	0.7337

Important note: for longer appraisal periods, up to 125 years, please refer to **Annex 15**. From 'Year 31', the discount rate for financial costs becomes 3.0%. From 'Year 76', the discount rate becomes 2.5%.

For the present value, take the total cost and multiply it by the discount factor of a given year.

For example, a £5 000 000 cost:

In Year 0, the present value will always be £5 000 000 as the discount factor is 1.

Year 1: £5 000 000 x 0.96662 = £4 831 000

Year 2: £5 000 000 x 0.9335 = £4 667 500

and so on....

...Year 31: £5 000 000 x 0.3459 = £1 729 500

....Year 76: £5 000 000 x 0.0919 = £459 500

6.6.2 Discounting the benefits of preventing harm to the person or the environment

The benefits for harm to the person or the environment are discounted in the same manner as capital cost, but using the initial discount rate from the Green Book of 1.5%. The rate is reduced from 'year 31' and 'year 76' in the same way. For longer appraisal periods, up to 125 years, please refer to **Annex 16**.

6.7 Bias

When calculating costs, previous project capital estimates may be used to derive a value. In order to allow for general inflation, together with specific changes in prices that are greater than inflation (such as the cost of stainless steel piping increasing due to the price of nickel), the costs may be inflated by more than inflation. Where costs have been inflated to account for 'unknowns', or items subject to dramatic cost increases, this should be explained. If this bias causes the rejection of the measure because the CBA is borderline, revised costs should be obtained.

Where costs are certain, no bias adjustment is required, however strong evidence should be presented to demonstrate why there is certainty. The principle of optimism bias is discussed in the 'Green Book'.

6.8 Aversion

It is often thought that a further measure is considered to be disproportionate, simply if the sum of the costs at present value, is greater than sum of the benefits at present value. However, it is also required to reflect the degree of aversion society has to the level of harm to people and/or the environment (see also the 'Green Book'). It is acknowledged that society is much more concerned about a single high consequence event, such as the Flixborough disaster which killed 28 people and seriously injured 36; than multiple single incidents that only lead to 1 or 2 fatalities. The greater the number of people killed or seriously injured in a single incident, the greater is society's concern or 'aversion'. This may be because it is immediately more abhorrent; or it is considered that it is much more difficult and costly to prevent multiple single incidents, than it is to prevent a single MAHS. The principle of aversion was established during the 1986 inquiry into the Sizewell B nuclear power station, and in the consequent HSE report, (1988) 'The tolerability of risk from nuclear power stations'. HMSO

Aversion is normally incorporated by using a 'disproportion factor', this is a multiplier applied to the benefits, determined by the presumed level of public aversion to the risk.

This could be expressed as:

$$\text{Disproportion factor} = \frac{(\text{Sum of Costs at present value})}{(\text{Sum of the Benefits at present value})}$$

There are currently no fully developed criteria to determine the appropriate disproportion factor, only guiding principles. It is suggested that as an absolute minimum the lowest disproportion factor to be used is one, and that for cases where there are three fatalities (or nine serious injuries) then the minimum disproportion factor to be used is two.

Suggested values are given in **Table 8** below, noting that the disproportion factor for high numbers of fatalities and serious injuries is highly dependent on the specific circumstances. Those in the high disproportion category may also need to take into consideration, among other things: wider societal benefits, national security, and national economic importance.

The reason for selecting the particular disproportion factor used should be recorded with the further measure evaluation. When a MAHS can result in human harm or a MATTE, the highest relevant disproportion factor of the two should be adopted.

Disproportion class/factor		Consequence to Populations On-site, and Off-site
Low	1	≤ 2 fatalities on-site ≤ 6 serious injuries on-site single fatality off-site ≤ 3 serious injuries off-site
Medium	2	$2 < \text{fatalities on-site} < 6$; $6 < \text{serious injuries on-site} < 18$; $1 < \text{fatalities off-site} < 3$; $3 > \text{serious injuries off-site} > 9$;
High – Very High	3 - 10	Dependent upon circumstance but: ≥ 6 fatalities on site, ≥ 18 serious injuries on-site, ≥ 3 fatalities off site, ≥ 9 serious injuries off-site,

Table 8: Disproportion factor criteria.

6.9 Sensitivity analysis, Identifying ‘switching values’

When carried out correctly, cost-benefit analysis provides an estimate with a degree of resolution in proportion to the benefits. As the estimates are not absolute, professional judgement is needed to consider the tolerance/variance (+/-) in the calculated value.

Sensitivity analysis (SA) is discussed in the Green Book and described as ‘*exploring the sensitivity of expected outcomes of an intervention to potential changes in key input variables. Sensitivity can be used to test the impact of changes in assumptions and should be clearly presented in the results of appraisal*’. Some values used in the cost estimate will have stronger influence than others. Varying these input values by a small increment can show how much larger, or smaller, they would need to be to change the outcome toward adopting the measure, or conversely rejecting it.

The inflection point in the particular value being considered which changes the decision to implement or not, is known as a ‘switching value’. Where a shortlist has been assembled for

a high proportionality MAHS, it would be expected that sensitivity analysis should be performed to identify the key switching values.

Sensitivity analysis should also be used when duty holders have limited information about some of the key inputs, and/or the number of fatalities and/or serious injuries.

6.10 ALARP Conclusion

It is a common misunderstanding that the principles of reducing risk to 'As Low as Reasonably Practicable' is solely based upon applying appropriate measures until stated risk thresholds are reached (such as those given in **section 5, Figure 10**); and that there is no requirement to go beyond this. However, this in itself is not sufficient, there is still the legal requirement to reduce risks 'so far as is reasonably practicable'. This is completed by applying the 'reasonably practicability test' to possible further measures in order to show that the risks have been reduced to ALARP. This successive test is illustrated in **section 5, Figure 7**, 'the pivotal role of risk tolerability'.

Once the MHHHRA process is completed, there should be a conclusion at the end of the assessment stating that for all unit operations: appropriate measures are in place; and all reasonably practicable further measures have been implemented. Where it cannot be shown that both appropriate measures are in place, and necessary further measures have been implemented; a time bound improvement programme should be put in place through the SMS. It is strongly suggested that the content of any improvement plan required, is discussed with the regulator at the earliest opportunity.

6.11 Periodic review and revision

Section 7 of this guideline outlines the general requirement that the Operator's SMS must be based on an assessment of the risk, and should include an outline of the Operator's approach to achieving a suitable and sufficient MHHHRA, for all unit operations at the establishment.

For further measures, review and revision is expected as new information becomes available. For example, from the identification, analysis, and assessments, elements of MHHHRA. Consideration should also be given to updates of the base information used when undertaking CBA, including the cost of a fatality, or cost of serious injury. These changes could greatly affect marginal cases.

7. Arrangements for ensuring a suitable and sufficient risk assessment is in place, and adequately maintained

This section is intended as a general summary, some specific examples are also given in the preceding sections.

7.1 Safety management system

The Operator's safety management system (SMS) must be based on an assessment of risk. It is suggested that the SMS should follow the relevant good practice outlined in HSE's publication 'Managing for health and safety' (HSG 65)¹⁶, or an equivalent; and also the COMAH 2015 L111 Guidance on SMS given in the section regarding Schedule 2. HSG 65 describes the 'Plan, Do, Check, Act' approach; which achieves a balance between the systems in place, and the behavioural aspects of management. It emphasises the importance of making the health and safety management system an integral part of good management, rather than as a stand-alone system whose output is not effectively utilised.

7.1.1 Implementation

The SMS should include an outline of the Operator's approach to achieving a suitable and sufficient MHHRA for all unit operations at the establishment. Key assessment procedures should be listed, together with the arrangements for how their effective implementation is managed, audited, and reviewed. It should also explain how the Operator will collect intelligence on pertinent accidents/incidents and act upon them.

The SMS should also describe how the Operator's MHHRA approach is applied throughout the process lifecycle of the establishment's unit operations, from project conception through to decommissioning. It is suggested that the SMS embeds the key aspects of the IEC 61511 functional safety lifecycle. Particular emphasis should be placed on modification, linking this to 'management of change' procedures; specifically requiring the Technical Folder to be updated, including adding the assessments performed, and updating the individual and societal risk profile if changed.

The Operator's SMS should include:

- a general management system, including the organisational structure and implementing the major accident prevention policy;
- the responsibilities of all the people involved in the management of major hazards;
- how MAHS identification, analysis, assessment, and determination of further measures, are applied to all relevant stages of the process safety life cycle from project conception through to decommissioning;
- arrangements for considering lessons learned from current and previous incidents and accidents;
- documented procedures to ensure safe design and operation;
- internal change management procedures;
- ensuring risk assessment is revised to reflect any changes in on and off-site populations (**see section 7.2**);

¹⁶ HSE, (2013) 'Managing for health and safety (HSG 65)'. HSE.

-
- ensuring revised MAHS are considered in the emergency response plan (see section 7.3).

7.1.2 Ensuring performance

The SMS should outline the timescales for the periodic review of:

- MHHHRA policy, to ensure that it still meets good practice, and also current legal requirements;
- MHHHRA approach, ensuring that it has been properly implemented, and is kept current; this includes ensuring that a management of change has been completed when required;
- measurement of how well the risks are being controlled, through both leading and lagging indicators; using near miss reports, failed proof tests, plant breakdown records, alarm and trip logs;
- investigating the root causes of recent accidents, incidents and near misses; feeding back and updating MHHHRA as the findings dictate;
- Technical Folder for all unit operations, maintained and up to date;
- standards pertinent to the site operations, tracking changes to relevant good practice (RGP) and existing standards used; carrying out an appropriate gap analysis, then updating the MHHHRA as necessary;
- CBA cases using updates to 'value of a life' and 'value of a serious injury';
- failure frequencies derived from, or corroborated by, on-site data (break-down reports, proof-test logs and routine inspection and maintenance reports).

7.2 Change in on-site and off-site populations

Changes to the on-site population may not be linked to unit operations but may affect site risk profiles and cumulative individual risk. For example, new canteens, and changes in office accommodation; should be reflected through management of change procedures, with the MHHHRA updated as appropriate. It should be noted that if another company takes over the operation of part of the site, or creates an enclave within the site boundary; the workforce in these areas are treated as off-site members of the public. Again, these changes would require the MHHHRA to be updated.

Changes in the off-site population within the hazard isopleths may take place even though the Operator has expressed an objection to the development. This could include significant housing developments or retail parks. Any significant change to the off-site population may affect the cumulative individual risk, or societal risk. MHHHRA should be updated if there are significant new populations within the hazard isopleths. Periodic updates may also be required if there has been a number of small developments over a long period of time.

7.3 Internal emergency plan

When the establishments MHHHRA changes, this is likely to lead to the need to review and revise other arrangements. For example, there is a requirement to review the adequacy and accuracy of the internal emergency planning arrangements following any modifications or other significant changes to the establishment. In carrying out a review of an internal

emergency plan, the Operator must take into account any changes at the establishment or within the emergency services concerned; any relevant new technical knowledge; and any relevant new knowledge concerning the response to major accidents. Operators should not wait until the three-yearly review of their emergency plans if a significant change to the establishment has been made.

A process for conducting periodic reviews of the internal emergency plan should be part of the SMS, with any review including the current MHHHRA and the technical information used to produce it.

Annex 1 - Regulatory context

Under the Health and Safety at Work etc. Act (HSWA) 1974, it is the duty of every employer to ensure, so far as is reasonably practicable (SFAIRP), the health, safety and welfare at work of all their employees. The employer also has to conduct their undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in their employment who may be affected thereby are not exposed to risks to their health or safety. The Health and Safety Executive (HSE) calls the legal requirement on SFAIRP, the 'as low as reasonably practicable' (ALARP) principle (**see section 6.1.3**).

Undertaking a suitable and sufficient MHHHRA is part of the assessment of risk required by Regulation 3(1) of the Management of Health and Safety at Work Regulations 1999 (MHSWR). This regulation requires employers, including the Operator (employer) of a COMAH establishment: to carry out a risk assessment for the purpose of identifying the measures needed to be taken, in order to comply with the requirements under the relevant statutory provisions. These provisions include COMAH, where an assessment of major hazard human harm risks, is required to identify all the measures necessary to comply with COMAH Regulation 5(1). It should be noted that MHSWR does not apply to risks to the environment.

This CDOIF guideline outlines the essential elements and suggests current good practice principles in relation to identifying, analysing and assessing major accident hazard scenarios (MAHS), and then considering further measures in order to satisfy MHSWR 3(1), also captured by COMAH Regulation 5(1).

By implementing the good practice in MHHHRA outlined in this CDOIF guideline, or equivalent approaches that satisfy the guiding principles, an Operator will be in a position to adopt all the measures necessary required by COMAH (for example, hierarchy of control, relevant good practice (RGP), the control measures required for each scenario event combination, and further measures), and to reduce their major hazard human harm risks to be 'as low as is reasonably practicable' (ALARP).

Other aspects of this MHSWR assessment (for example, occupational health and safety), and the more specific assessments required by other relevant statutory provisions (for example, Dangerous Substances and Explosive Atmosphere Regulations 2002); still need to be undertaken. It is up to Operators to decide how they will manage the delivery of such risk assessments, but they should avoid duplication.

The MHSWR also requires that a Regulation 3(1) risk assessment be completed before the Operator starts to consider their duties under Regulation 5 of the MHSWR. This is because a suitable and sufficient risk assessment will have identified the required preventative and protective measures the employer needs to take to comply with the requirements and prohibitions imposed upon him by or under the relevant statutory provisions. Regulation 5 creates a duty to make and give effect to such arrangements as are appropriate, having regard to the nature of his activities and the size of his undertaking, for the effective planning, organisation, control, monitoring and review of the preventative and protective measures. This, in turn, requires the arrangements (including management arrangements relating to these measures and requirements under other relevant statutory provisions) to be put in place.

Regulation 5(1) of COMAH is a broad all-encompassing regulation that applies to the Operators of all COMAH establishments. It requires that every Operator must take all measures necessary to prevent major accidents and to limit their consequences for human health and the environment. This includes carrying out a suitable and sufficient MHHHRA of the establishment's unit operations. As COMAH is a relevant statutory provision under the HSWA, the MHHHRA is seen as one part of the range of risk assessments required under the Regulation 3(1) of the MHSWR. In a similar manner to MHSWR, COMAH requires that the Operator's safety management system is based on the assessment of the risks.

COMAH also requires all Operators to have a Major Accident Prevention Policy (MAPP) which should be proportionate to the major accident hazard scenarios identified for that establishment. The MAPP should ensure a high level of protection to both human health and the environment. It must be implemented through a safety management system (SMS). The SMS must be based on an assessment of the risk (Schedule 2 (1)(b)) and will outline, among other things, how the Operator will identify, analyse and assess the major accident hazard scenarios (MAHS) associated with their unit operations.

Considering Regulation 7 and Schedule 2 of COMAH, together with Regulation 5 of the MHSWR; the SMS should outline the Operator's approach for systematically assessing the major hazard human harm risks arising from both normal, and abnormal operation, of their processes and unit operations. This will include how this approach will be implemented, monitored, reviewed and updated as necessary (for example, routinely or part of change management procedures). The SMS will also describe how MAHS identification, analysis and assessment will be effectively applied to all relevant stages, from project conception through to decommissioning. The SMS should also ensure the findings of a MHHRA are implemented.

Operators of both Upper and Lower Tier establishments, must not only undertake, and record a suitable and sufficient MHHRA; but must when requested by the competent authority (CA), demonstrate that they have done so. This will include a clear description of their approach, together with the findings of the suitable and sufficient MHHRA carried out to comply with MHSWR – Regulation 3 and COMAH Regulation 5(1). The demonstration will also outline the appropriate management arrangements to ensure that the MHHRA for COMAH is implemented, monitored and reviewed.

COMAH requires all Upper Tier establishment Operators to submit a safety report to the CA; for the purposes of demonstrating that MAHS in relation to the establishment have been identified, and that the necessary measures have been taken to prevent such accidents and to limit their consequences for human health and the environment. The Operator's MHHRA will be part of this demonstration. Their demonstration should be proportionate (**see section 2.3**) and provide a clear link between the various MAHS identified and the measures which are in place to defend against them. The safety report should show how the necessary measures will prevent foreseeable failures which could lead to major accidents, and to limit the consequences of any that do occur. For all establishments (Upper and Lower Tier), documents such as the MAPP, operating instructions and training material will be necessary as part of the overall demonstration. Under the MHSWR, all Operators of COMAH establishments employing 5 or more employees are also required to record the significant findings of their risk assessments. The CA could ask to see these findings before carrying out inspections or investigations.

Please note that there are two key differences between the risk assessment requirements in COMAH 2015 and MHSWR 1999. The first is that COMAH requires the consideration of both consequences for human health and the environment. Therefore, in some sections of this guideline we make the links with appropriate major accidents to the environment (MATTE) risk assessment approaches. Sometimes, risk assessment approaches that require both human health and environmental considerations (for example, CBA) are also highlighted. The second difference is that, as outlined above, COMAH requires the Operator to demonstrate to the COMAH Competent Authority (CA) that it has undertaken a suitable and sufficient risk assessment, rather than just recording significant findings.

When undertaking a suitable and sufficient MHHRA, and demonstrating that the major hazard human harm risks to people, both on-site and off-site, have been reduced to ALARP, this should focus on making a logical demonstration that all reasonably practicable measures have been taken, not simply that some value for a scenario or individual risk has been met. An Operator will need to show that they have applied the hierarchy of control measures, and adopted relevant good practice or equivalent when available, or identified the controls

required for each event combination that can lead to a MAHS using first principles when it is not. Consideration of both appropriate and further measures should also be seen as an iterative process, where the inputs and findings are reviewed, and updated, as necessary (for example, in line with the Operators SMS).

Annex 2 -Consideration of MAHS proportionality

Proportionality

Proportionality in the MHHHRA context is used to describe the relationship between the severity of the hazard to people, to the 'depth, resolution and robustness' expected of the risk assessment performed; it is an indicative metric not an absolute measure. In this guide proportionality is used to inform the appropriate depth, resolution and robustness of analysis for a particular major accident hazard scenario (MAHS). Quite clearly the degree of depth, resolution and robustness in the assessment of a MAHS, which has the potential to lead to more than a dozen deaths, would be expected to be very much greater than one which would lead to three serious injuries (**see section 5.4.4** for the relationship between deaths, and the number of serious injuries).

In this sense, 'depth, resolution and robustness' principally refer to the depth of the numerical analysis required to support the logical argument that has been made. Whatever the proportionality, it would be expected that a logical demonstration has been made, showing how the appropriate measures prevent the scenario initiating and propagating events occurring.

An establishment which exceeds the threshold at which COMAH applies, and also presents potential-MAHS leading to serious danger to the person, is already considered of high proportionality. Here, we are considering whether a site is on the cusp of high proportionality; or is of the 'highest' proportionality. The two ends of the spectrum could be represented by: 500 tonnes of methanol, stored in 1 tonne movable bulk containers, held under ambient conditions, stored close to an occupied building; through to a site storing over 20 tonnes of acrolein, and processing large quantities of acrolein at elevated temperature and pressure, located near a centre of population.

The proportionality of MAHS around the two ends of this spectrum are normally relatively easy to classify. The problem is determining the level of proportionality when a unit operation is between these two extremes, then setting down how that proportionality is expressed during the assessment process. In most cases, this will require quantitative risk assessment, determining the frequency and severity through a numerical analysis; not qualitatively, or semi-qualitatively.

It is not possible to give a list of unit operations and their MAHS, together with a 'proportionality level'. This is because unit operations may be carried out in different configurations, stream compositions, scales, and have differing surrounding populations.

Where the consideration of proportionality is not necessary

There are some external MAHS, initiated by events such as aircraft impact, which even though they are of very high severity, the Operator has no direct control over the initiating and propagating events, or their possible elimination. This would not discharge the responsibility for the Operator to take necessary measures, in the case of aircraft impact, this would include informing the Civil Aviation Authority of the presence of the establishment, and making the request that the establishment is not normally overflown. In addition, the Operator would need to ensure that statutory requirements were fully implemented, such as the appropriate illumination of tall structures to make them visible to aircraft.

Determining proportionality

Proportionality is initially established using 'severity'. Severity is the number of fatalities and/or the number of serious injuries expressed as fatalities, predicted before, not after, all measures necessary have been applied.

$$\text{Scenario severity score} = \left(\begin{array}{c} \text{number fatalities} \\ \text{from that scenario} \end{array} \right) + \left(\begin{array}{c} \text{number serious injuries} \\ \text{from that scenario} / 3 \end{array} \right)$$

The proportionality of the MAHS is ranked as High, Very High or Extremely High. If present, factors that would suggest a greater proportionality are considered collectively, then used to adjust the initial ranking.

Initial proportionality category

The initial proportionality category is determined by the initial severity score for the MAHS using the severity score table A2-1 below.

Proportionality category	Scenario severity score <i>[(number fatalities) + (number serious injuries ÷ 3)]</i>	
	On-site	Off-site
High	≤ 2	≤ 1
Very High	2 > to 6	1 > to 3
Extremely High	> 6	> 3

Severity Score Table A2-1

Adjustment factors which increase proportionality

Common factors which suggest an increase in proportionality are given below; three or more factors present are considered to increase the proportionality by one category.

(i) Scenario ranks in the upper quartile

If a scenario has a high contribution to a site's risk profile, and is in the top quarter when scenarios are ranked, it would be expected that proportionately more emphasis would be placed upon the depth of analysis performed due to its influence.

(ii) Degree of complexity

The greater the complexity, the more difficult it is to represent the system by simple treatments such as layer of protection analysis (LOPA). For example, many dynamic systems such as a distillation column are dependent upon a number of interrelated parameters; such as feed rate, boil-up rate, reflux ratio, pressure, and temperature. There are often control level trips

which only affect a particular sub-system, such as the reboiler, reflux system, or feed control. There may also be safety level trips for specific sub-systems. There can also be a global Emergency Shutdown System (ESD), which is triggered by a number of scenarios, that completely shuts the unit down. In this case, a simple LOPA may not represent the system relationships, as the demand on the ESD will usually be triggered by a number of scenarios, not just one. It is still possible to use a table, but probably not a simple LOPA package. In some complex cases a fault tree may be needed in order to properly allow the representation and calculation of the top event frequency.

(iii) Escalation is likely

Escalation may considerably increase the extent and severity of the MAHS. For example, a pool fire in a gasoline storage tank farm could rapidly propagate from storage tank to storage tank. The probability of escalation can often be difficult to determine, however the potential to escalate should be a factor when considering proportionality, as it could lead to an order of magnitude increase in the extent and severity, than the MAHS itself. This should also consider any likely escalation to surrounding COMAH establishments; these are sometimes referred to as 'domino' sites.

(iv) Scenario multiplier greater than 3

Where an MAHS is used to represent a number of other similar scenarios (referred to as a representative scenario), and it appears more than three times in an individual cumulative risk profile (multiplier of 3), this is indicative of its elevated importance, and so warrants greater proportionality. For an example of this see **Table 2, section 5.2.1**.

(v) Dangerous substances which are 'H1' acute toxic, and gases which are both acutely toxic and highly flammable

Dangerous substances categorised as 'H1' acute toxic, such as acrolein, are toxic at very low doses. High sensitivity dispersion models should be used, and normal assumptions may not hold. Dangerous substances which are both acutely toxic and flammable are particularly hazardous, as they may give rise to vapour cloud explosion, pool fire, flash fire, jet fire, or toxic exposure. Treatments should ensure that combined risk from these consequences is considered, in order to capture the uncertainties. The presence of dangerous substances which are 'H1' acute toxic, and those which are both acutely toxic and flammable, suggests a higher proportionality is required.

(vi) Single exposure carcinogen/mutagen

This group of dangerous substances are particularly hazardous and may give rise to serious injury at very low doses. Due to the uncertainty of the dose response for this group, a higher proportionality should be considered.

(vii) Public permitted or resident on site

Though not normally associated with COMAH sites, the presence of tourist visitors and dwellings is not uncommon at some establishments, due to the past 'deeming' of Hazardous Substance Consent and historic precedence. The harm criteria for on-site individual risk are based upon the presence of a working age population who are engaged in a work activity. The presence of a wider population distribution, including the old and young, and those who are sleeping, may change the site risk profile. Where the presence of the public is routinely permitted, or there are dwellings on site, this suggests a higher proportionality is required. This is because residents on site are treated in the same way as the off-site population, therefore, their risk tolerability is a factor of 10 less than the on-site population.

(viii) Associated with high risk non-COMAH activity (i.e. bulk LNG ship off-loading)

There are some high hazard installations that are not encompassed by the COMAH 2015 regulations, in close proximity with other high hazard installations. These may be severely impacted by a MAHS. An example of this is bulk liquified natural gas (LNG) imported by shipping tankers with capacities of up to 266 000 m³. A tanker may be present almost constantly, as one leaves, another docks. However, the ships and docking facilities are normally regulated by the Maritime and Coastguard Agency, and are therefore not controlled under the 2015 COMAH regulations. Off-loading facilities, onshore piping, including emergency shut-off block valves are included within COMAH. The failure of the off-loading system may lead to consequences which could escalate to the shipping tanker. The large inventory of LNG may give rise to very high extent and severity. The presence of the shipping tanker, though not part of the legislation, should still be considered when considering proportionality. This may mean that extent and severity is considerably increased, therefore the degree of depth, resolution and robustness must be increased accordingly if this is the case.

(ix) Escape is not possible

In many scenarios, the ability to escape is an important factor when determining fatality, as well as serious injury. For those scenarios from which escape is not possible, due to either the nature of the consequence, such as an explosion; or the operator being in an area where they cannot make an effective escape; this would suggest an increased proportionality. In addition, when those whose movements are restricted are vulnerable, a higher proportionality should be considered.

(x) Establishment fed by pipeline over which the site has limited control

Where a site is fed by a high flowrate bulk pipeline carrying a dangerous substance (for example, supplying gasoline to a distribution terminal, or ethylene for plastics manufacture), and the site cannot directly implement emergency shutdown such that flow is completely stopped, this should be taken into consideration when determining proportionality. As the source term duration is critical to determining extent and severity, this may require the use of detailed human task analysis and/or detailed 'LOPA'/Fault Tree Analysis'; simple failure rates and duration assumptions are insufficient.

(xi) No secondary containment

Where a vessel or unit operation containing a dangerous substance has an approximate volume of greater than 25 m³, and has no secondary containment, this should be taken into consideration when determining proportionality. Increased resolution should be used to properly determine the extent of the spreading pool, by examining the actual topography rather than just a simple spreading pool model.

(xii) Sensitive or vulnerable population within the hazard range

Where there are sensitive and vulnerable populations within the site hazard range, such as schools, care homes, or hospitals; this should be taken into consideration when determining proportionality.

(xiii) No RGP available for the unit operation

There may be no developed RGP and standards for some unit operations, typically those which are new or novel. In this case, it would be expected that the degree of proportionality would be increased to reduce the level of uncertainty.

(xiv) Equipment is beyond its stated original design life

Reliability modelling is dependent upon the equipment having a constant failure rate and known failure modes. If equipment is beyond its stated original design life it may begin to exhibit non-predictable modes of failure, or known localised issues predominate. Ageing pipework can be particularly susceptible to localised erosion and corrosion, to a point where prediction of corrosion rates and statistical treatments are not sufficiently conservative. In these cases, a proportionately more detailed analysis would be expected.

(xv) Unit operation requires active intervention to return plant back to safe stable state after a predicted process excursion

Where a unit operation requires further steps to return it to a safe stable state, such as further manually initiated intervention, in addition to an automated emergency shutdown system; this suggests greater proportionality due to the increased complexity of the recovery. This can be seen on polymerisation reactors where the feed may be stopped, however the reaction continues in the reactor. This requires the injection of an inhibitor, or a quench, to prevent the accumulated reactants and intermediates continuing to participate in the runaway reaction. In these cases, a comprehensive study would be taken to the same level as a high integrity protective system (HIPS).

(xvi) High level of manual control

Some unit operations may require a high degree of manual control, particularly if they are being used to pilot a new process. In these circumstances, it would be expected that the degree of human factor analysis would be high, to ensure the safe operation of the plant. It is not sufficient to simply state the process is temporary, or will only be undertaken occasionally, analysis must be commensurate with the potential severity.

Adjustment factors which may reduce proportionality

The following factors could be considered to reduce proportionality if properly justified.

(a) Common package unit (boilers, refrigeration units etc.)

Where common package units are constructed to recent, current, detailed, unit operation specific standard(s), and do not use novel fuels such as hydrogen, or ammonia; then reduced proportionality could be considered.

(b) Basis of Safety is total containment under all fault conditions

Where the basis of safety is total primary containment (not secondary containment) under all fault conditions; reduction in proportionality could be considered, as long as the control and safety systems are not required to return the system to a safe stable state after a process excursion.

(c) No escalation possible

Where escalation is not possible, there is no surrounding off-site population within the hazard range, and the on-site population is only present for a short time; reduction in proportionality could be considered.

(d) Explosives COMAH establishment.

Where an establishment is subject to the requirements of a licence granted under the provisions of the Explosives Regulations 2014, reduced proportionality can be considered due to the additional measures required by the licensing regime.

Annex 3 -Determination of chemical behaviours and interactions

Identification → **Analysis** → **Assessment** → **Further measures**

1. Introduction

To support the assessment of whether a process has the potential for a major accident to occur, and to assess its consequences; it is essential that the properties of the materials present, and their interactions, have been fully investigated and are understood.

Section 3.5.3 of this guideline highlights that sometimes for simple, and/or well-established processes and unit operations, some of this information is incorporated into codes of practice and sector guidance. You can use this information where relevant and current. However, when codified chemical behaviours and interaction information is not available, Operators will need to obtain this by undertaking the studies outlined below.

Composition and contaminant profiles for raw materials/intermediates/products vary with source and production method. As a basic underlying principle, it is expected that production materials will be used for all tests and analysis; unless it can be shown not to be reasonably practicable. Where tests have not been undertaken using production materials, unless it can be shown otherwise, it may be considered that the analysis does not constitute a suitable and sufficient risk assessment.

Figure A3-13 outlines a model which shows the relationship of aspects that determine chemical behaviour and the tests/information that, where appropriate, may be used to establish relationships and interactions. **Figure A3-13** aims to give an overview of the properties and tests which may be necessary, and to indicate the order in which they are normally carried out.

This MHHHRA guideline is predominantly based on the risks from processing liquids, vapours, and dissolved solids. Powders and their processing plant have their own unique set of hazards which are not considered by this annex.

The European Chemicals Agency (ECHA) and its associated database is principally focused on labelling and packaging. However, it does provide a recognised source of information on the chemical hazards of most raw materials. It is also a good starting point for collecting basic information and screening for known hazardous behaviour. It should be noted that this annex is not intended to give any guidance for the classification of substances and mixtures for the purposes of labelling and packaging. The ECHA currently operate a comprehensive open access website.

It should be noted that there are many different processes and unit operations that can be utilised to achieve the same end, often with a number of possible reaction routes. As there are so many different reaction systems and unit operations in which reactions are carried out, this annex only attempts to outline general principles.

The examination and review of chemical behaviours and interactions for a process is often iterative throughout its lifecycle. To ensure chemical behaviours and interactions studies remain pertinent and current, they should be reviewed and updated as necessary.

1.1.1 Process lifecycle

Most processes go through several defined phases, often in terms of scale. These are:

- Theoretical proposal.
- Initial 'test tube scale' appraisal.

-
- Laboratory scale development.
 - Semi-tech scale development.
 - Pilot plant scale.
 - Full scale.
 - Full scale modification and further plant development/expansion.

It may be self-evident but changes in the process route, unit operations, feedstock, and basis of safety, will require a detailed review of fitness for purpose of the existing chemical behaviour and interactions assessment. This should highlight any new hazards as part of the hazard identification process and change control within the safety management system (SMS).

1.2 Scale and proportionality

The minimum assessment requirement before any physical reaction work is carried out at any scale is to complete the assessments where appropriate at least down to the point identified by the red line on the model at **Figure A3-13**. These assessments will involve pertinent literature studies or tests. The results of the literature studies will help to determine which experimental studies should be completed. Higher hazard potential will require proportionately more experimental studies at an earlier stage.

Existing production process (including pilot plant)

It is expected that as part of the hazard identification process for an established chemical process, a screening protocol would have been conducted to establish 'chemical behaviours and interaction'. This is relevant to all scales of production as even small scale may be of very high hazard. The minimum studies expected have been outlined in many established texts such as the industry accepted Barton and Rodgers¹⁷ and Jorg Steinbach¹⁸. Further studies may be required for stability as will be addressed in **section 5** of this annex. The Operator of a COMAH establishment should, as a minimum, carry out the studies at least down to the point identified by the blue line on the model.

Where a chemical behaviour and interaction screening process has not been carried out previously, or it is incomplete, it cannot be shown that all potential major accident hazard scenarios have been identified. Therefore, it will not be possible for an Operator to demonstrate that all necessary measures have been taken.

¹⁷ Barton, J. and Rodgers, R. (2004) 'Chemical Reaction Hazards – A Guide', 2nd edition. IChemE.

¹⁸ Steinbach, J. (1999) 'Safety Assessment for Chemical Processes'. Wiley-VCH.

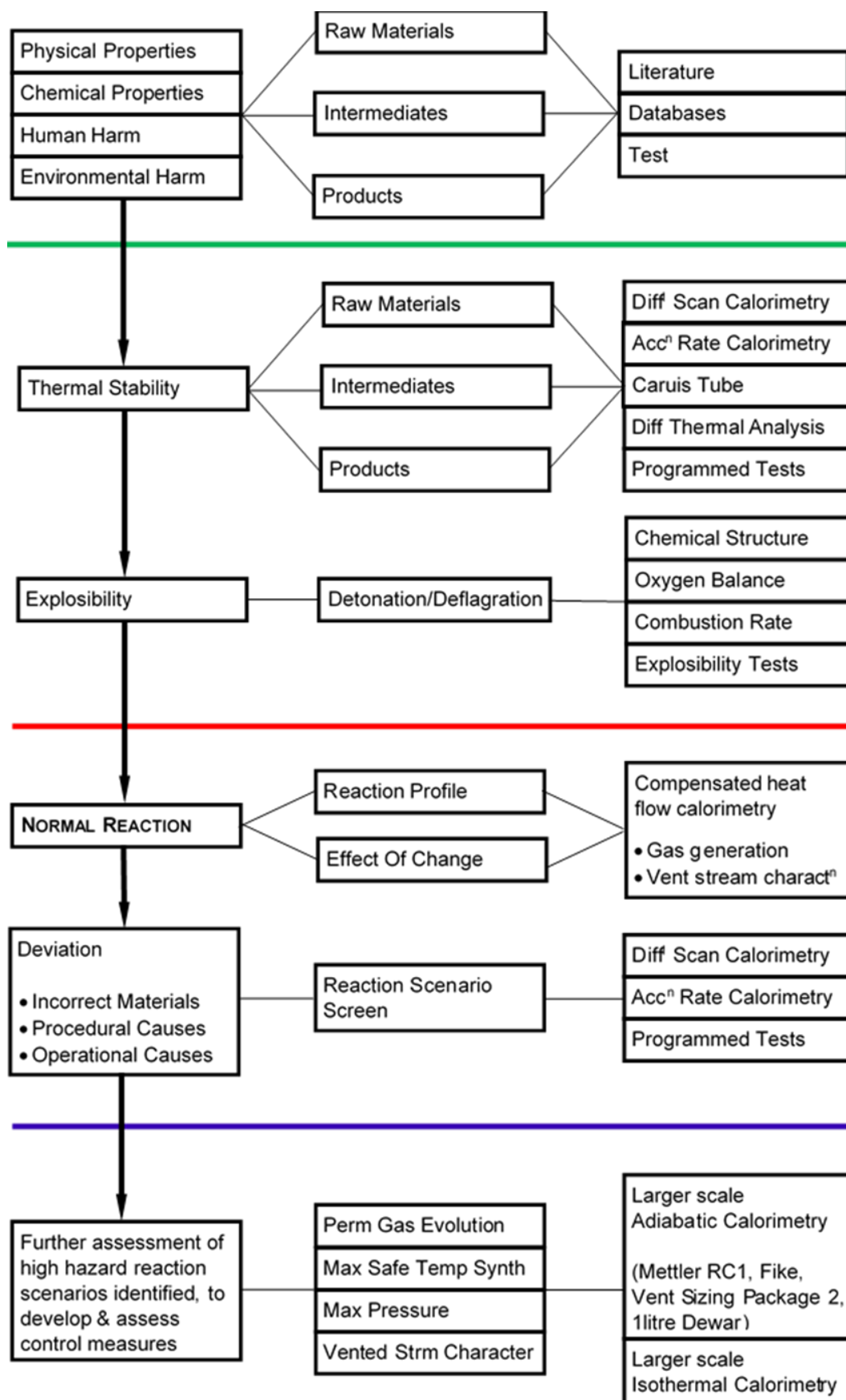


Figure A3-13 - Relationship of aspects that define chemical behaviour and the tests/information used to determine relationships and interactions.

When the chemical behaviours and interaction studies carried out indicate the potential to give rise to a MAHS, the Operator of a COMAH establishment should complete the potential-MAHS screening protocol to identify MAHS. This will involve undertaking the process outlined in **Figure A3-13** and the supporting accompanying text in this annex. Further studies will not be necessary when the chemical behaviours and interaction studies carried out indicate no potential to give rise to a MAHS.

Laboratory scale process

Hazard potential will also determine the scale at which studies between the red line and the blue line should be completed. As a general guide, it is strongly suggested that at above the 25 litre ('semi-tech') scale this should trigger the studies between the red line and blue line regardless of hazard potential.

It should be noted that evidence of apparent endothermic behaviour from normal laboratory equipment for processes operating above ambient temperature is often misleading as the rate of heat loss from such equipment may exceed the rate of heat produced by reaction. Therefore, an exothermic reaction may require heating in the laboratory to overcome the effects of heat loss.

Hazard potential will determine at what scale work beyond the blue line will be required.

Relationship between scale and thermal hazard

It should be noted that sensitivity to thermal hazards increases with plant scale, and therefore requires data/test-work giving proportionately greater resolution as the phi factor of the system (often described as thermal inertia) decreases. The phi factor (Φ) describes the ratio of mass and specific heat capacity of a sample, or sample mixture; compared to that of the test vessel or sample container. The closer the phi factor is to 1, the lower the influence of the vessel/container and the more representative the result is of the sample itself^{[17][18]}.

$$\Phi = \frac{\Delta T_{ad}}{\Delta T_{obs}} = 1 + \frac{m_V \cdot C_{p,V}}{m_S \cdot C_{p,S}}$$

2. Chemical, physical and hazard properties

The minimum requirements are that a material safety data sheet (MSDS) and safety data sheet (SDS) must have been obtained and reviewed for each raw material present (either pure component or mixture). Resulting process streams also require an MSDS and SDS, which must be made available if the material is exported from site:

- raw material,
- intermediates,
- final products,
- bi-products, and
- waste streams.

Data should have been obtained from sources which are established as being reliable. Where this is not possible, the data should be corroborated or gathered by suitable testing. It should be observed that established sources may have limits of application and will also require corroboration where used outside those limits of application.

Sources of data may include SDS/MSDS; the European Chemicals Agency (ECHA), and its associated database; 'standard texts' such as Lewis (Sax)¹⁹, Bretherick²⁰, Kirk-Othmer²¹ and commercially available software databases used within their limits of applicability.

Synthesised data

Synthesised or predicted data must be fit for purpose. Models should be suitably validated, and accuracy commensurate with the hazard potential and scale of operation. This applies to data for pure component, preparations and mixtures. The potential impact of departure from ideal behaviours should be assessed where synthesised/predicted data is used.

The use of analogues and ideal behaviour should only be selected if it is known to be conservative. It should be demonstrated that 'predictive techniques' are appropriate and make predictions within validated limits.

Necessary information about the substances, preparations, or mixtures

Basic attributes include:

- hazard classification (including ECHA entry if available),
- Chemical Abstracts Service (CAS) registry number if available,
- composition,
- physical properties.

¹⁹ Lewis, R. (2021) 'Sax's Dangerous Properties of Industrial Materials', 12th edition, Volumes 1-5. Wiley.

²⁰ Bretherick, L. (2017) 'Bretherick's Handbook of Reactive Chemical Hazards', 8th edition. Elsevier Ltd.

²¹ 'Kirk-Othmer Encyclopedia of Chemical Technology (2007)', 5th edition, Index and Volumes 1-26. Wiley.

2.1 Hazardous properties of the substances present

The basic hazardous properties of the raw materials, intermediates and final products must be determined. These include:

- Health hazards;
 - toxicity,
 - general,
 - mutagenicity,
 - carcinogenicity.
- Physical hazards:
 - flammability,
 - explosibility,
 - self-reactivity,
 - pyrophoricity,
 - oxidising potential.
- Environmental harm:
 - hazardous to the aquatic environment.

2.1.1 Toxic to human health

The principal risk to human health from toxic materials in this context comes from materials which are toxic by inhalation.

The COMAH regulations define a major accident hazard as leading to serious danger to human health [or the environment] (whether immediate or delayed) inside or outside the establishment and involving one or more dangerous substances. The guidance to the regulation, L111^[14] paragraph 36, defines serious danger to human health as 'the risk of death, physical injury or harm to health; (a) a substantial number requiring medical attention; (b) some people seriously injured, requiring prolonged treatment'.

Any incident resulting in serious danger will have the potential to cause death, but it will not necessarily do so. The effect may be immediate or delayed. For example, respiratory distress may follow some hours after exposure to a toxic gas. There may be other circumstances when the harm occurs even further in the future.

A small number of carcinogens are listed in COMAH Schedule 1, Part 2. This list is not exhaustive and the effects of exposure in a major accident could manifest themselves much later. The important point is that the harm arose from a single acute exposure, release or event.

Many Operators choose to use 'risk of death' as a measure in order to establish tolerability. When carrying out risk assessment, the Operator could theoretically use an interpretation that is of a higher resolution, but in practice this is unlikely to be experienced. The legislation is clear in that it defines serious danger to human health, not death, as the criteria. It should be noted that calculations that determine death cannot be meaningfully integrated to give the numbers of serious injuries. This is why the use of dangerous dose is encouraged, noting that Probit equations are based on risk of death (ROD).

A dangerous dose causes death in a third of the normal (off-site) population; for a skewed population of solely those that are fit and well and of working age it will only cause a few percent of deaths. For sensitive populations such as the young and old, a dangerous dose will lead to approximately 100% of deaths. Everybody who is exposed to a dangerous dose is in serious danger. It is expected that the duty holders assess MAHS both on the basis of death and serious injuries.

It is therefore strongly suggested when screening, that the dangerous toxic load, for both death and dangerous dose, are considered. It is entirely possible that a toxic release could seriously injure tens of people but cause no deaths.

Dangerous dose is calculated by using the 'specified level of toxicity, dangerous toxic load' (SLOT DTL). Risk of death can be estimated by using 'significant likelihood of death, dangerous toxic load' (SLOD DTL). This is of the form:

$$\text{DTL} = \text{concentration}^n \times \text{time}$$

Where the concentration is raised to the power of the constant 'n'

The values for 'n' and the DTL values for specified level of toxicity (SLOT) and significant likelihood of death (SLOD) can be found on the HSE Website and may be periodically revised. There are other relationships that can be used, but specialist advice on using these should be obtained.

2.1.2 Explosibility

If a substance or mixture has an oxygen balance score of more than -200 (minus two hundred), or if a component contains a known unstable chemical group (for example, nitro, and azide groups), it should be tested for explosibility. A combustion energy of >500kJ/kg is a further indication of the possibility of fast deflagration that could lead to detonation. Lists of the reactive groups are given in references [18][19].

Unless a substance or mixture is known to be inert, or proven to be stable and of low reactivity: it would be expected that all raw materials, intermediates, and products; would have been subjected to a suitable ramped temperature test, to screen out explosibility and establish their thermal stability. This basic test establishes base line stability, but the phi factor of the test means that it can only give a broad screen. The other methods of determining stability grow progressively more sensitive, their selection is commensurate with the phi factor of the system in which they are placed.

Various methods are available for predicting the explosive yield of liquid and solid phase explosible substances or mixtures. The most often used is TNT equivalence, which can be used in the TNT equivalence model. The TNT equivalence can be calculated by bond energy, though this method is subjective. For materials categorised as 'explosive' other dynamic tests such as the Ballistic Mortar are used.

Strong oxidising and strong reducing agents should also be considered in terms of possible contamination and incompatibility with other reactants leading to explosion.

2.1.3 Flammability

Flammability is a basic set of properties that are needed to determine if a substance or mixture poses a flammable hazard. For a flammable liquid the principal hazard is of radiant heat from a pool fire. For a vapour the 'fuel reactivity/flame speed' and the degree of congestion and confinement can give rise to 'fast deflagration'/flash fire' through to vapour cloud explosion (VCE). Ignition of flammable mixtures in closed vessels may lead to flame propagation, overpressure and the creation of missiles. Basic flammable properties of the liquids present

should be determined to ascertain if flammable hazards are present. These properties include:

- flash point,
- upper and lower flammable limits,
- ignition energy,
- autoignition temperature.

Flash point and ignition tests should be conducted to recognised international standards. It is normal practice to carry out both open and closed cup tests for liquids. Low levels of flammable contaminants can have a disproportionate effect on flammable properties.

Further properties may need to be considered if the vapour generated at the temperatures experienced is capable of forming explosive mixtures under the conditions proposed. These properties include:

- maximum overpressure generated from closed stoichiometric combustion;
- laminar flame speed;
- fuel reactivity (Baker, Strehlow, Tang);
- ratio of stoichiometric fuel volume to combusted gas volume;
- combustion energy;
- oxygen balance.

2.1.4 Self-reactivity, pyrophoricity, oxidising power

Materials may be self-reactive, pyrophoric, or have high oxidising power such that their storage conditions are critical. Storage may be under water, at low temperature, in inert atmospheres, or segregated from other materials. For example, there are some materials that have a limited 'shelf-life' that must be returned to the manufacturer or their stability will be reduced such that they may be liable to detonate under certain conditions. Most of these material properties have known 'active groups' and/or can be identified from their classification. For complex organic materials, there may be no information available, and any screening regime must be capable of identifying them.

2.1.5 Hazardous to the environment

As a minimum, the toxicity to the aquatic environment should be established. Further requirements are outlined in the industry acknowledged CDOIF Guideline Environmental Risk Tolerability for COMAH Establishments.

2.2 Required pure substance physical properties

The following properties are considered to be the basic relationships, where appropriate, that should have been established by the duty holder:

- freezing point,
- boiling point,
- vapour pressure/temperature relationship,

- critical pressure,
- critical temperature,
- specific heat capacity,
- enthalpy of vaporisation,
- density.

Which properties are required may depend on the physical phases which may be present during normal operation and during the development of potential-MAHS.

Physical properties may vary significantly with both temperature and pressure. Conservative values of properties should be used. Where databases offer temperature correlations for databases, the correlations should only be considered reliable within the temperature range to which the data has been fitted.

2.3 Required non-reaction mixture physical properties

Some mixtures exhibit non-ideal behaviour, so it is important to establish the vapour liquid equilibrium (VLE) relationship for the mixture. This can impact on the potential for loss of containment as it can result in higher than expected pressures. For example, a particular potential issue may be created by the presence of azeotropes. All systems with two liquid phases have azeotropes and will exhibit higher pressures than would be expected for an ideal mixture.

3. Contaminants

Many process materials have contaminants which may have come from the raw materials, materials of construction, side reactions; or part reaction. Contamination in raw materials, intermediates, recycle streams, products, by-products and wastes must be considered. Contaminants may be benign, or have the potential to introduce instability; or lead to the build-up of flammable atmospheres as they are concentrated in vessel headspaces.

Where contaminants can catalyse reactions, or induce decomposition; changes in sourcing may be significant even where the purchase specification is identical. Consideration of contaminants should continue throughout the assessment of the potential reaction hazards. The testing of raw materials from new suppliers may need to be integrated into change control.

It is expected that a composition contamination profile will be assembled for raw materials, intermediates and products. The required resolution is dependent upon the nature and scale of materials. It is expected that a composition contamination profile will be assembled for raw materials, intermediates and products. An appropriate initial starting point could be considered to be 0.1%. However, screening is often an iterative process, the degree of iteration depending largely on what is known. For example, some substances give rise to catalysis at much lower levels, which is why it is important to also carry out appropriate screening tests and calorimetry. The final resolution required is dependent upon the nature and scale of materials and the processes involved, with the results of tests indicating whether further investigation is required.

3.1 Materials of construction

Many reactions are catalysed by transition metals or their ions. This includes common construction materials such as iron in steel. Often test equipment may have cells made from glass or other corrosion resistant materials such as Inconel, as these provide a neutral

environment and it is therefore useful to differentiate between them when conducting a screening process. If the materials of construction and their corrosion products are not present during the test, the findings may be misleading. Consideration should be given to ensuring that thermal stability and reaction rate have considered the material of construction of the vessels and pipework. This test should include the incorporation of construction materials and their corrosion products, it should be noted that such materials may accelerate or inhibit the reaction, so testing may be required both with and without such materials.

Some containment systems rely on the presence of a layer of passivation, again consideration should be given to the fact that this layer may become depleted or eroded, allowing the process materials to become exposed to the materials of construction.

4. Chemical interaction

Chemical interactions are examined:

- Within the intended reaction system.
- Outside the intended reaction system (also applies to plant with no intended reactions).

It is expected that production material will be used for tests and analysis unless it can be shown not to be reasonably practicable. Where tests have not been carried out using production materials, unless it can be shown otherwise, it may be considered that the analysis does not constitute a suitable and sufficient risk assessment.

4.1 Within the intended reaction system (batch or continuous reaction)

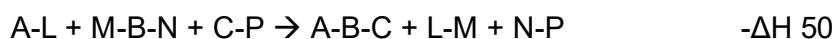
The Operator must:

- describe the intended reaction route and the hazards associated with it;
- screen for possible reactions between substances normally present and those potentially present;
- determine reaction hazards associated with incorrect procedure and raw materials used in the defined reaction route (order of addition, substitution, multiple addition);
- determine reaction hazards associated with operational causes; and
- determine reaction hazards associated with the addition of materials present but not normally associated with the process.

4.1.1 Description of the intended reaction route and the hazards associated with it

The overall route and pathways need to be discussed for each reaction step, for example if:

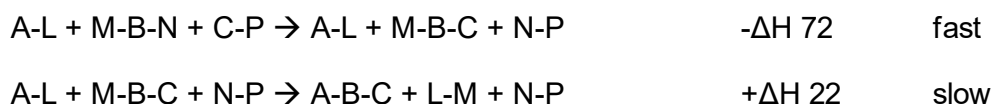
Overall reaction route



Possible pathway 1 (predominates below 50°C)



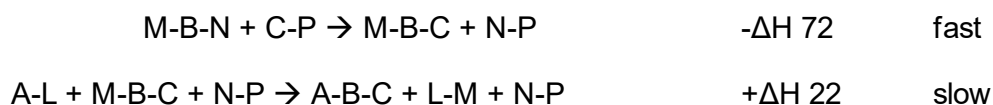
Possible pathway 2 (predominates above 50°C)



Order of addition 1



Order of addition 2



All the isolatable intermediates along each of the pathways between the starting materials and product need to be included.

Normally the heat of reaction would be expected to be present for each part of the pathway. However, where this is not possible, the reasons should be given together with the available information.

4.2 Exothermic reactions

For exothermic reactions, where the enthalpy of the reactants exceeds those of the products, the total potential energy present and the rate of heat generation must be considered. This may lead to the temperature exceeding the boiling point of the reactants and the pressure of the system increasing with vapour pressure. In some cases, the temperature may rise above the level of thermal stability and the materials present may decompose, leading to further heat generation, and/or gas generation and an increase in pressure. Heat losses from typical laboratory equipment mean that it cannot be assumed that reactions which require heating in the laboratory are not exothermic.

4.3 Gas generating reactions

Reactions with the potential to generate permanent gas also require further study. This includes reactions where: the pathway intentionally generates a permanent gas; reactions which may induce instability which in turn generates gas; and reactions which include a substance with the specific purpose of absorbing the gas which would otherwise be released.

4.4 Polymerisation

Some monomers used as raw materials, may require stabilisation or other controls to prevent uncontrolled exothermic polymerisation. Process intermediates or finished products may also contain materials which can polymerise. It is important that potential unintended polymerisation is screened for as a potential hazard.

4.5 Catalytic behaviour

Some materials (raw materials, intermediates, and final products) may exhibit catalytic, or auto catalytic behaviour. This may be due to the nature of the reaction system, the presence of contaminants, materials of construction, or the temperature to which they are subjected. This behaviour should be looked for during literature searches and the screening process.

Catalytic behaviour may only be expressed under certain conditions. Where practicable, tests should be carried out using typical plant materials. Consideration should be given to performing parallel tests, with and without particles of the materials of construction present; as these are more representative of the plant conditions at which such behaviours may become apparent.

5. Mapping reaction routes to process steps

In order to make a transparent demonstration, the process route(s) can be mapped to the process stages, where this is not adequately addressed by the process description.

For a batch reactor, the stages may take place in the same vessel; for continuous reaction, they may take place in a single vessel, or across many vessels. It must be possible to determine what reaction is taking place in which vessel(s).

A process consists of a sequence of steps such as heating, cooling, addition, distillation, reflux; over a single vessel, or over specific unit operations. The intended locations for each process operation should be identified. In the case of batch processes, it may be necessary to specify both location/vessel and the sequence relative to other operations carried out.

It is suggested that a table can be used to relate process steps to reaction stages, for example:

Step no.	Process step	Corresponding reaction stage
1.1	M1 Mixing of reactants A & B	I (II)
1.2	R6 Feed into first continuous reactor	II (III)
1.3	T1 Crude Product Storage	-
1.4	C2 Distillation	III
1.5	R8 Feed into Second Reactor Addition of reactant C	IV
1.6	R10 Oxidation Vessel	V
1.7	R10 Crystallisation	-

5.1.1 Determination of hazards associated with the intended chemical reaction route

As a minimum, the potential for the following should be evaluated:

- Exothermic reactions.
- Thermal instability of reactant mixtures and products.

-
- Catalytic behaviour.
 - Permanent gas evolution.
 - Polymerisation.
 - Effect of materials of construction.

5.2 Exothermic reactions

In exothermic reactions, the enthalpy of the reaction products is less than the reactants; the resulting energy output heating the reaction mixture and the reactor. The reaction rate increases exponentially with temperature, only limited by the availability of the reactants and mass transfer coefficients. With continuous addition, if the reaction rate is sufficiently high, then the heat output will be 'feed rate limited'. If not, the unreacted material can accumulate, then 'runaway' if the heat output can overcome the heat transfer capability of the reaction system. Note that in a feed rate limited system, there will be accumulation until the concentration in the equipment results in a reaction rate which matches the feed rate. This accumulation can result in 'runaway' in the event of process disturbances, for example loss of cooling.

The increase in reaction system temperature typically causes an increase in vapour pressure. When the vapour pressure exceeds the atmospheric pressure in the reaction vessel, the mixture will boil with the rate of vapour evolution equivalent to the reaction rate. If the vapour rate exceeds the vent capacity, the pressure will increase and the temperature will increase in accordance with the vapour liquid equilibrium of the system. The resulting temperature and pressure must not exceed the design conditions or loss of containment may result. While the peak temperature will occur at the end of the reaction, the peak pressure may occur earlier; for example, where the reactant(s) are more volatile than the product(s). It should be noted that the release of vapour via the vent as a result of runaway may be a potential-MAHS even where the design pressure is not exceeded.

In systems where both reactants are added, then heated to a point where the reaction energy is greater than that lost from the system, the temperature will increase until either equilibrium is reached with heat removal, or until the capacity of the heat removal systems is overcome.

Exothermic reaction can be generated from either the desired reaction or from unintended reaction between incompatible materials, or where contaminants change the reaction route, or catalyse it.

If the temperature can rise to the point where the components dissociate/decompose, then an uncontrollable pressure increase can occur, which if the system is not designed to accommodate it, may lead to loss of containment.

The information on identified process routes and pathways must be representative of the operation and the particular materials used. Trace amounts of impurities, contaminants, and materials of construction; can grossly affect reaction speed and pathway.

To address the impact of impurities, contaminants and material of construction, unless it can be demonstrated that it is not reasonably practicable, testing should be carried out on the actual plant substances in the presence of the actual material of construction.

It would be expected that the process routes and pathways identified are screened for significant exothermic potential.

5.2.1 Requirement for calorimetry

If there is no directly applicable literature on the chemical behaviours and interactions identified; it would be expected that calorimetry would be used to characterise the heat input/output of the intended process route for each reaction stage. It should be noted that if the heat generation of the process is close to that which could lead to exothermic runaway, greater emphasis should be placed on test data. Note that because of the potential impact of impurities and materials of construction, there may not be sufficient information in the available literature to demonstrate applicability.

Calorimetry should be conducted in a calorimeter whose phi factor is below that of the process; if not, reasons should be given to justify why the low resolution of the data obtained is adequate.

It should be noted that normally small-scale screening equipment such as: accelerating rate calorimetry, differential screening calorimetry, Carius tube, thermal screening units; are generally unsuitable for plant scale studies. Calorimetry is an expert field, and the Operator is encouraged to seek further advice if they do not have extensive experience. If required, references [17][18] and [22] will give the Operator sufficient knowledge to have an informed conversation.

5.2.2 Characterisation of the vented stream

When an uncontrolled chemical reaction occurs there is potential for complex two-phase relief venting. If this behaviour has not been considered it cannot be ensured that any relief venting will be effective. As part of the vent sizing process, the vent stream behaviour must be characterised (gassy, foaming, gel forming, single phase, two-phase etc). It will be necessary to characterise the behaviour by testing unless there is evidence or tests already performed (if the Operator considers that a relief characterisation test is not required, the rationale for this decision should be given). It should be noted that the release pressure and temperature will affect the nature of the vented relief stream, particularly for vapour pressure systems and tempered 'hybrid' systems exhibiting two-phase flow. In addition, the reaction products can affect vent stream behaviour; for example, the viscosity and tendency for gel formation may increase as the reaction progresses.

This guidance only considers the behaviour and interactions that may give rise to a scenario that leads to uncontrolled reactions and their relief. For further guidance on the design of relief systems see HSE's workbook for chemical reactor relief system sizing.²²

5.2.3 Computer models

Computer models may only be used when they have been suitably validated for the assessment of chemical reaction hazards. This means that the data used to create the model must cover a wider range of conditions than has been predicted by the model.

5.2.4 Thermal instability of reactant mixtures and products

Raw materials, isolatable intermediates, and final products must be subject to tests (or have applicable literature data for that particular composition and impurity profile) to determine their thermal stability. Materials are heated to determine the point at which they decompose, or begin to exhibit autocatalytic decomposition, exothermically or leading to permanent gas evolution. This should be carried out in such a way that considers appropriate heat/search and/or heat/search/wait protocols. Results need to be interpreted, taking into account the characteristics of the test equipment. Many types of equipment for such tests are non-

²² Etchells, J. and Wilday, J., HSE (1998) 'The workbook for chemical reactor relief sizing'. HMSO.

adiabatic and the observed onset conditions require correction to indicate the plant onset conditions.

Where reasonably practicable, the reaction system should be operated such that it cannot reach conditions at which the raw materials, intermediates or products become unstable and decompose exothermically and/or with gas evolution. Where this is not reasonably practicable, the system must be designed either for containment or to safely vent the system.

Commonly used approaches such as maximum safe temperature of synthesis and maximum temperature of synthesis reaction can be useful, but can be misleading in some cases.

Maximum Safe Temperature of Synthesis (MSTS) is the temperature above which either the raw materials, intermediates, or products become unstable and decompose exothermically or with permanent gas evolution.

Maximum Temperature of Synthesis Reaction (MTSR) is normally determined by adding the adiabatic temperature of the intended reaction to the maximum start temperature of the system^[18]. Some duty holders have used this to estimate end pressure and for comparison with the thermal stability data of the product.

For some systems, this will be a non-conservative approach, for example where one or more of the following applies:

- peak pressure occurs at intermediate point;
- decomposition of an intermediate;
- a reaction other than the intended reaction becomes significant.

5.2.5 Permanent gas evolution

This aspect must be assessed as part of thermal stability, but also as part of reaction and calorimetry studies as this can lead to potential overpressure of the system.

Where tests identify higher quantities of heat and/or gas generation than would be expected from the intended reaction, it is important that the potential causes of the excess heat and/or gas are investigated. Understanding the causes is essential to the application of the hierarchy of control with a view to preventing the hazard scenario.

6. Screening of possible reactions between substances normally present

6.1 Determination of incompatibility between substances present

All substances should be listed and the interaction between the pairs examined. In considering the pairs, the potential for process conditions to activate or enhance the reaction must also be examined. This is often conducted in the form of a table, with the material listed both on the vertical and horizontal axis; interactions investigated and noted if hazardous. In some cases it may be necessary to consider if further permutations of materials may promote a reaction.

The emphasis should be on the materials associated with the reactions and stages performed that are readily available to the reaction system or made be fed forward from other stages.

Services, fixed or selective, such as cooling water, heating/cooling-oil, steam, refrigerants, or air, may enter the reactor/process if coils/jackets fail, and as such should be included in any study of compatibility.

For multi-use plant where other reactions or variants are performed, this should also include:

- materials that may be connected to the reactor system/module;
- materials that may be present in the location (bulk bags, charge cans).

This screening should include consideration of substances which could be added as a result of failures in systems, but would not normally be added to the process, or at that location (in the case of batch processes, this may be time dependent as intermediates created as part of the process, are only present at certain times).

Sources include, but may not be limited to:

- lines or charge systems directly connected (solid, liquid, gas);
- services and utilities;
- containers present in the building which can be connected into that process at some point; and
- charges prepared and imported from a common location which could be present in the building in error.

6.2 Determine reaction hazards associated with incorrect procedure and raw materials used in the defined reaction route

Deviations from the intended operating procedure must be assessed. The possible errors when charging materials can be categorised into five main types.

No addition: the material charge is omitted, and the process moves onto the next addition or step.

Under addition: reduced quantity than specified is added during the step.

Over addition: greater quantity than specified is added during the step.

Multiple-addition: the correct charge step is completed, then it is repeated.

Substitution: substitution of the material to be charged, with another material supplied to the process/reactor module.

The process steps may be more than just additions of chemicals, but involve further operations; such as distillation, filtration, layer separation and so on. In a batch reactor it is possible that the process step may be omitted, or carried out in the wrong order, leading to an unexpected composition. The cause of this type of error may be due to failures in the control system, human error, or both. Re-starting a batch part-way through the process following a breakdown (due to power failure, equipment failure or other); could lead to the process being re-started at the wrong process step.

Process step omitted: the process step/operation is omitted and continues to next step.

Process step carried out in the wrong order another process step is carried out other than the one intended.

Permutation: combination of errors.

Note that the hazards associated with such deviations may occur in a location or at a time remote from the deviation. For example, failure to add a reactant may allow the unreacted

components to travel to a later part of the process, where it may encounter conditions which result in a different reaction (including decomposition).

7. Determination of reaction hazards associated with operational causes

Reaction hazards are dependent not just on the chemical reaction route but the mode of operation. Reactions may be operated as a batch (all-in), fed/semi-batch, or continuous processes. While aspects of the assessment are common to all modes, each mode may exhibit different hazard scenarios.

This section is intended to give an overview of determination of reaction hazards associated with operational cause. This is normally carried out to outline behaviour as part of the iterative design process; then again, in detail when the design is fixed. Without these studies when conducting hazard and operability studies (HAZOP), and other guideword driven methodologies, there is insufficient knowledge as the effect of the deviation is unknown.

The Basis of Safety, and Safe Operating Envelope, will also evolve and may change throughout the process lifecycle.

The depth of analysis required is proportionate to the degree of the MAHS associated with the unit operation being considered (**see section 2.3**). Very simple processes such as storage may just require some simple test work to gauge stability, while very complex processes may require multi-variate analysis. The Operator is expected to have sufficient knowledge and competency to ensure adequate analysis has been performed. The remainder of this section is to indicate the degree of resolution that may be required.

7.1 Establishing Basis of Safety

HSE's HSG 143 'Designing and operating safe chemical reaction processes'²³ outlines the requirement for a declared Basis of Safety.

Without a stated basis of safety and defined safe operating envelope, it is difficult to show that the systems of control and safety are adequate, such that it can be demonstrated that all measures necessary have been taken, and therefore the risks from the process are ALARP.

7.1.1 Common Basis of Safety

Non-specific examples of basis of safety are:

- containment;
- control and relief;
- control and high integrity protection systems;
- control, quench and relief.

It is typical to start with the premise that the basis of safety will be control and relief. The safe operating envelope is then established for one degree of freedom. For each process carried out in the reactor, the maximum tolerable deviation for each process condition in order to operate the system in a safe stable state. The basis of safety will evolve with plant design.

²³ HSE, (2000 rep 2008) 'Designing and operating safe chemical reaction processes'. HSE Books.

7.2 Safe Operating Envelope

The safe operating envelope is defined by a number of operational criteria which if met ensure that the system operates in a safe stable state. Once the basis of safe operation has been established, the safe operating envelope can then be determined. Safe operation is assured as long as the required criteria are met, for example, for a typical batch reactor operating with a catalysed feed rate limited reaction:

(a) addition is carried out in the correct order and mass/rate:

- i) specified initial material charged,
- ii) specified charge mass,
- iii) specified reactant charge rate,
- iv) specified material charge ratio (or charge ratio which gives lower reaction rate),
- v) specified catalyst/inhibitor at the correct concentration/pH,
- vi) specified catalyst/inhibitor present before addition takes place.

(b) reaction is, started and maintained, between defined temperature limits:

- i) addition started above specified minimum reactor temperature,
- ii) no external heat input during peak rate of reaction,
- iii) only one reactor module of paired reactor set at high thermal load,
- iv) specified time between additions where split addition is used,
- v) adequate cooling capacity,
- vi) adequate cooling water flow,
- vii) adequate cooling water temperature.

(c) amount of accumulated reactants is below that which would cause the relief/quench system capacity to be exceeded (maximum back pressure should be stated):

- i) sufficient agitation,
- ii) limited amount of accumulated reactants.

(Note: If unable to establish the degree of deviation that would cause the process to operate outside the defined operating envelope, the conservative assumption is that any deviation will cause the system to operate outside the defined operating envelope).

Where the basis of safety is dependent upon the availability of other system(s), this should be highlighted. For example, if sufficient reactant accumulation could occur to overcome the cooling system.

7.3 Establish each system's thermal capacity

The method of heat removal must be stated (for example, cooling and/or vent/reflux condenser). Then the maximum cooling capacity for each reactor must be determined, with the water-cooling system at the greatest expected level of stress during normal operation. For example:

- cooling water flow just above the trip/interlock set point;
- cooling water temperature just below any trip/interlock set point;
- maximum summertime temperature and humidity (obtained from cooling water tower design standard);
- greatest degree of fouling process side and tube side;
- lowest expected cooling water inventory (with no emergency cooling);
- with other reactor in the pair (or other plant) at the greatest expected load.

7.4 Establish range of predicted exothermic events and quantify

Most scale reaction calorimetry is carried out in devices that mimic batch stirred tank reactors. Where the plant is something other than a batch stirred tank reactor, this may require alternative calorimetric approaches or particular attention to the planning of the calorimetric tests and the interpretation of the results.

Tests are performed to predict:

- maximum accumulation of reactants;
- maximum self-heat rate dT/dt ;
- maximum rate of pressure generation dP/dt ;
- maximum overpressure;
- total heat released.

This could be achieved by initial tests being performed adiabatically with batch charges at normal process temperature and no inhibitor present. Tests should be performed using equipment with a comparable ϕ factor, or less than that of the plant.

Calculation can be used provided the necessary assumptions can be substantiated or the worst case has been adopted.

Calorimetry/calculation should demonstrate that the reactor system can either: contain; can be quenched; or has sufficient relief capacity to contain process excursions caused by the deviation outside the defined condition(s)/parameter(s).

Isothermal calorimetry will usually be required where the basis of safety involves operating a feed rate limited regime. It is necessary to establish the level of accumulation which will occur in the reactor, and assess whether it results in a potential hazard in the event of deviations; for example, loss of cooling.

This may be related to degraded performance; for example, if two cooling water pumps are normally in service, the relief system could be adequate for the failure of a single pump but not both.

8. Determination of reaction hazards associated with materials not normally associated with the process

Materials that may enter the process in error, or through equipment failure, should be considered. (See also section 6.1 of this annex, 'Determination of incompatibility between substances present'):

- materials used to clean vessels or prepare for maintenance;
- materials used to pacify or prevent corrosion;
- steam;
- boiler feedwater treatment chemicals in directly injected steam;
- cooling water;
- cooling water corrosion inhibitors;
- ammonia gas refrigerant.

9. Operations outside the intended reaction system (also applies to plant with unintended reactions)

Very often supporting operations such as storage and solvent recovery, and recycle streams are overlooked. These too must be screened for hazardous reactions.

9.1.1 Delivery of incompatible materials in error

The measures to control delivery of materials to the establishment need to be described. This is to prevent receipt of materials not used on site, and outline the measures to segregate those materials which may not be compatible.

Where raw materials are sourced externally, there is the possibility of materials being supplied that may give rise to a reaction hazard, either in the storage vessel or in the process itself. The sensitivity to contaminants usually associated with that raw material must be considered and appropriate measures must be in place.

9.1.2 Stabilised raw materials

Stabilised raw materials (often self-reactive, pyrophoric and strong oxidising materials such as monomers, peroxides, formaldehyde, acrylonitrile) have associated hazards in storage and ancillary equipment. Inhibitors, scavengers or any system that prevents the hazardous substance forming or undergoing a transition with hazard potential must be described. (see also section 2.14 on self-reactivity, pyrophoricity, oxidising power).

9.1.3 Recycle streams

In some cases when materials are recycled in a process, contaminant(s) are concentrated, and stabilisers/inhibitors become depleted. Therefore, recycled materials may exhibit very different hazardous behaviours from the initial stream/raw material. This may not be readily apparent from analysis as trace quantities may promote or inhibit instability. Such changes in stability may only become apparent after several cycles, so it is important that test work adequately considers this.

9.1.4 Waste streams - residue decomposition

Distillation to recover products and/or solvents from waste streams concentrate less volatile substances, some of which may be unstable. The impact of their instability may become progressively greater as they are concentrated; some residues may also become less stable with age. These potential reaction hazards must be fully assessed, residue stability testing may require extended duration.

Annex 4 - Collated accidents and incidents summary table – for illustrative purposes

Page	Date	Site	Incident	Issues Revealed	Company Response and/or Key arrangements already in place
4	23/03/05	BP Texas City Refinery, Texas, USA	Blowdown stack over-filled, major VCE. 15 fatalities, 180 people injured, major destruction & damage	- Poor safety culture - Inadequate maintenance/ tolerance of failed safeguards - Inadequate manning & handover - Reliance on undersized atmospheric relief - Inappropriate location of temporary accommodation	- Eliminated atmospheric blowdown stacks - Initiated review of all atmospheric relief systems - New Standards for portable buildings, personnel access during start-up, shift handover, safe operating limits, fatigue management, & operator training
8	11/05/05	Hertfordshire Oil Storage Limited Oil Terminal, Buncefield, UK	Overfill of gasoline tank, large vapour cloud generated in still conditions, VCE. 43 people received minor injuries, no fatalities, but major destruction & damage, environmental impact	- Inadequate maintenance/ tolerance of failed safeguards - Inadequate filling procedure - Inadequate bund integrity - Inadequate emergency response arrangements	- Overfill risk assessment & implementation of SIL-rated protection per PSLG - Bund capacity & integrity improvements - Improved tank level and transfer management arrangements (control system, alarm arrangements, procedures)
11	18/02/15	ExxonMobil Torrance Refinery, California, USA	ESP explosion during maintenance due to flammable mixture reaching live ESP, 4 injuries, no fatalities, major damage	- Passing spent catalyst slide valve (SCSV) could not hold catalyst seal - Inadequate instrumented safeguards - ESP not de-energised despite reactor system shutdown - Failure to recognise need to move from standby to full shutdown	- Need to monitor & maintain minimum reactor-to-fractionator delta pressure clarified 2018 PHA identified desirability of new pressure measurement location – accepted action - Robust layers of protection for SCSV delta P & catalyst level - ESP always shuts-down with reactor (inter-locked) - Safety culture would have ensured full shutdown

Annex 5 - Open source chemical incident databases

This annex provides a selection of open sources of investigation reports and analyses of chemical accidents and incidents. It is recommended that Operators maintain their own sources of information, some of which will provide alerts of specific incidents. Industry groups may also collate incident records for their members.

ARIA (France) <http://www.aria.developpement-durable.gouv.fr/>

A database operated by the French Ministry of Ecology, Energy, Sustainable Development listing the accidental events which have, or could have, damaged health or public safety, agriculture, nature or the environment. Chemical accidents are reported that meet established criteria.

Number of events: >10 000 **Time span:** > 1970

Geographic coverage: France and some major disasters in other countries.

Purpose: Lessons learned.

Format: Free text only.

Description of content: Concise, and sometimes, comprehensive technical summaries of serious accidents from all hazard sources. Reports are verified by technical experts. Impacts are reported in free text. All accidents associated with sources classified as high hazards and meeting a certain impact criteria are recorded in this database in accordance with French legislation.

Data on impacts: Each incident is classified according to the EU Gravity Scale based on human health, environment, community and economic impacts.

CSB Chemical Safety and Hazard Investigation Board (United States)

<https://www.csb.gov/investigations/completed-investigations/>

The CSB conducts root cause investigations of chemical accidents at fixed industrial facilities. Video recreations and written texts.

Number of events: >170 **Time span:** > 1984

Geographic coverage: United States of America.

Purpose: To share lessons learned and causal analysis.

Data on impacts: Information on human health impacts.

CSC (Korea) Chemistry Safety Clearinghouse <https://icis.me.go.kr>

Chemical accident and near miss data notified to authorities according to Korean law.

Number of events: > 400 **Time span:** >2014

Geographic coverage: Korea.

Purpose: Lessons learned and causal and impact statistics.

Format: Classified by technical cause.

Description of content: Short summaries of chemical accidents on fixed sites and in transportation, reported in accordance with Korean legislation. For each accident there are statistics on human health impacts, and a mix of qualitative and quantitative information on other impacts.

Data on impacts: Quantitative data on human health impacts. Inconsistent data in all other categories. Economic impacts not collected.

eMARS <https://emars.jrc.ec.europa.eu>

Accidents reported to the European Commission in compliance with Seveso Directive Annex VI criteria.

Number of events: >1000 **Time span:** > 1984

Geographic coverage: EU/OECD countries.

Purpose: Lessons learned and causal and impact statistics.

Format: Free text and classification of events by various filters (substance, industry type, impact).

Description of content: Completeness and precision of descriptions varies considerably. For each accident there is a free text description of the incident, statistics on human health impacts, and a mix of qualitative and quantitative information on other impacts. All EU accidents on high-hazard (Seveso) fixed sites meeting certain impact criteria are recorded in this database in accordance with the EU Seveso Directive.

Data on impacts: Quantitative data on human health impacts. Inconsistent data in all other categories. Economic impacts not collected.

Energy Institute Toolbox <https://toolbox.energyinst.org/home>

Number of events: > 500 (process safety events) **Time span:** > 2000

Geographic coverage: Global.

Purpose: To share lessons learned and causal analysis.

Description of content: Database of accidents in upstream and downstream petroleum sectors. Provides analysis of sequence of events, response, causes and lessons learned.

Data on impacts: Information on human health impacts.

Failure Knowledge Database www.sozogaku.com/fkd/en/

Number of events: > 200 (process safety events) **Time span:** > 1970

Geographic coverage: Japan.

Purpose: To share lessons learned and causal analysis.

Description of content: Database of accidents in several industries, including chemical and petroleum sectors. Provides detailed structured analysis of sequence of events, response, causes and lessons learned. The contributor factors are also mapped in a scenarios diagram.

Data on impacts: Information on human health impacts, physical damage and costs incurred.

High Pressure Gas Safety Institute <https://www.khk.or.jp>

Number of events: >20,000 **Time span:** >1965

Geographic coverage: Japan.

Purpose: Preventing chemical incidents. **Format:** Excel file

Description of content: The accident case database consists of chemical incidents, including location, substance, industry and descriptive information about the incident (in Japanese).

Data on impacts: Provided as part of the accident summary.

ICHEME Safety Centre & Safety and Loss Prevention SIG www.icheme.org

Number of events: 100 - 200 **Time span:** >1960

Geographic coverage: Global.

Purpose: Lessons learned from historical chemical disasters.

Format: Classified by industry type.

Description of content: Summaries of well-known chemical accidents on fixed sites. For each incident, there is a description, incident analysis and lessons learned.

Data on impacts: Quantitative data on human health impacts and property damage.

(see also Loss Prevention Bulletin available to LPB subscribers and IChemE members)

IOGP Safety Performance Indicators and Process Safety Events (International Association of Oil and Gas Producers - IOGP) www.iogp.org

Accident data reported by IOGP participating member companies.

Number of events: >6000

Time span: > 2015

Geographic coverage: Participating members worldwide.

Purpose: Lessons learned and causal and impact statistics.

Format: Classified by technical and underlying causes.

Description of content: IOGP is one of the first industry organisations to report disaggregated data on safety events occurring in member company operations. Database of activities that can be sorted by type of activity and impact. Many of the incidents are occupational. It also publishes a book of process safety case studies on an annual basis.

Date on impacts: Each incident is classified as Tier 1 or Tier 2 severity based on human health, environment, community and economic impacts.

Process Safety Forum <https://processsafetyintegrity.com/org/psf/>

Process safety incidents, historic and reported incidents.

Number of events: >1000

Time span: > 1900

Geographic coverage: World.

Purpose: To pool process safety incident experience.

Description of content: Good search interface. Concise summaries of serious chemical accidents.

Data on impacts: Specific numbers provided on deaths and injuries. Limited detail on other types of impacts.

ProcessNet (German industry)

https://processnet.org/en/incident_db.html [en],

<https://processnet.org/ereignisdb.html> [de]

Hazardous incidents in process engineering facilities managed jointly by DECHEMA and VCI.

Number of events: ~100

Time span: > 2000

Geographic coverage: Not available.

Purpose: Lessons learned and causal information.

Format: Free text.

Description of content: Concise technical summaries of chemical accidents.

Data on impacts: Very limited, if available at all.

RISCAD (Japan) Relational Information System for Chemical Accidents Database

<https://riscad.aist-riss.jp/>

Operated by the Japanese National Institute of Advanced Industrial Science and Technology.

Number of events: >7 500

Time span: > 1949

Geographic coverage: Japan.

Purpose: Lessons learned and causal and impact statistics.

Format: Technical causes by keyword.

Description of content: Summarises accidents reported by various firefighting, response and safety organisations. For each accident, there is a free text description of the incident, statistics on human health impacts, and free text descriptions of other impacts.

Data on impacts: Quantitative data on human health impacts.

UEMS (Unplanned Explosions at Munitions Sites) database

<http://www.smallarmssurvey.org>

Unplanned explosions occurring at munitions sites, including production and storage, since 1979.

Number of events: >500

Time span: >1979

Geographic coverage: Global.

Purpose: Motivate improved reduction of risk associated with munitions sites.

Format: Classified by technical and underlying causes.

Description of content: The Small Arms Survey defines UEMS as the accidental explosion of stockpiles of ammunition and explosives at storage sites, whether the stockpiles are properly stored or are abandoned, damaged or improperly stored. Its work is intended to highlight a global problem with poor risk management at many these sites.

Data on impacts: Statistics on fatalities and injuries.

Work Accident Map (China) China Labour Bulletin

<http://maps.clb.org.hk/accidents/en#201801/201807/1821>

Work accidents collected from the media and other sources by the China Labour Bulletin.

Number of events: >1 700

Time span: >2014

Geographic coverage: China.

Purpose: Lessons learned and impact statistics.

Format: Mapped by location, location links to short summary with reference to a news report.

Description of content: Database and map of workplace accidents, including chemical accidents. Short summaries plus a link to a newspaper description are included. Statistics on human health impacts only.

Date on impacts: Quantitative data on human health impacts (on-site only).

ZEMA (Germany)

<http://www.infosis.uba.de/index.php/de/site/12981/zema/index.html>

Database managed by the German Federal Environment Agency of hazardous incidents and incidents in process engineering facilities.

Number of events: >750

Time span: > 1980

Geographic coverage: Germany.

Purpose: Lessons learned and causal and impact statistics. **Format:** Free text.

Description of content: Concise technical summaries of chemical accidents. All accidents associated with sources classified as high hazards and meeting a certain impact criteria are recorded in this database in accordance with German legislation.

Data on impacts: Quantitative data on human health impacts. Inconsistent data in all other categories. Economic impacts not collected.

Journals reporting chemical incidents and accidents

- i) Journal of Loss Prevention in the Process Industries, Elsevier.
- ii) Loss Prevention Bulletin, IChemE.

Annex 6 - Typical screening table for illustrative purposes, showing different approaches

Equip Number	Equipment Name	Equipment Type/funcn	Dangerous Substs(s)	Quantity tonnes	Operating Temp/press	Scenario/Sub-Scenario	Scenario/Sub-Scenario Number	Outcome	Consequence	Likelihood	Potential MAHS	MAHS? Y/N	Rep Set? Y/N (set ref if not)
Tank Farm 3													
T145	Crude Oil Storage Tank	External Floating Roof Tank	Crude Oil	95 000	50/amb	Floating Roof Failure	S7/7.1	Pool fire	Major	High	Y	Y	Y
						Corrosion							
						Mechanical Failure							
						Overfill • Ship • Inter-tank	S7/7.2	Pool fire	Major	Medium	Y	Y	
						External fire • Boil-over	S7/7.3	Pool fire	Major	Low	Y	Y	
						Internal Explosion	S7/7.4	Explosion	Minor	Low	Y	Y	
T146	Crude Oil Storage Tank	External Floating Roof Tank	Crude Oil	60 000	50/amb	As above	As above					Y	N (S7 - T145)
T147	Crude Oil Storage Tank	External Floating Roof Tank	Crude Oil	70 000	50/amb	As above	As above					Y	(S7 – T145)

Equip Number	Equipment Name	Equipment Type/funcn	Dangerous Substs(s)	Quantity tonnes	Operating Temp/press	Scenario/Sub-Scenario	Scenario/Sub-Scenario Number	Outcome	Consequence	Likelihood	Potential MAHS	MAHS? Y/N	Rep Set? Y/N (set ref if not)
T148 T149 T150 T151	Crude Oil Storage Tank	External Floating Roof Tank	Crude Oil	95 000	50/amb	As above	As above					Y	N (S7 - T145)
T152	Pentane	Double Skinned Fixed Roof Tank	Pentane	30	Amb/amb	Overfill	S10/10.1	Pool fire Flash fire	Minor	Low	Y	Y	Y
						Internal Explosion	S10/10.2	Explosion	Minor	Low	Y	N	-
T153	Solvent Flush Tank	Small Fixed Tank	Methanol	1.4	Amb/amb	LOC All modes	S8	Pool Fire Tox Exposure	Minor	Low	Y	N	-
Process Area: DHT2													
V203	Hydro-cracker reaction Circuit	Packed catalyst bed	Hydrogen Vacuum Gas Oil Naphtha Kerosene LPG	20	133/9	Pressure breakthrough from high pressure to low pressure	S2/2.1	VCE Flash Fire	Major	Medium	Y	Y	Y
C310	Hydro cracker primary fractionator	Dist column	Naphtha Kerosene LPG	10	3/120	Column overpressure -flooding - reboiler system failure -reflux system failure	S3/ 3.1 3.2 3.3 3.4	VCE Flash Fire	Major	Medium	Y	Y	N (S25 -C309)

Equip Number	Equipment Name	Equipment Type/funcn	Dangerous Substs(s)	Quantity tonnes	Operating Temp/press	Scenario/Sub-Scenario	Scenario/Sub-Scenario Number	Outcome	Consequence	Likelihood	Potential MAHS	MAHS? Y/N	Rep Set? Y/N (set ref if not)
Process Area: HFA													
R102	HFA Reactor	Reactor and settler/exchanger	Isobutane alkene (C3-C4) HF Acid Iso octane	30	36/12	Over pressure due to cw failure	S4/4.1	Pool Fire VCE Flash Fire Tox Exposure	Major	Medium	Y	N	-
						corrosion due to high alkyl acids	S4/4.2			Medium	Y	Y	Y
						Cold cat failure	S4/4.3			Low	Y	Y	

Annex 7 - Consideration of batch processes

Identify Basis of Safety

Examples of the basis of safety are:

- containment;
- control and relief;
- control and high integrity protection systems;
- control, quench and relief.

Determine the safe operating envelope for one degree of freedom

For each process carried out in the reactor, establish the maximum tolerable deviation for each process condition in order to operate the system in a safe stable state.

For example:

Operation assumes that the following are performed to ensure the particular reaction system operates within a defined operating envelope.

(a) Addition is carried out in the correct order and mass/rate:

- i) specified initial material charged,
- ii) specified charge mass,
- iii) specified reactant charge rate,
- iv) specified material charge ratio (or charge ratio which gives lower reaction rate),
- v) specified catalyst/inhibitor at the correct concentration/pH,
- vi) specified catalyst/inhibitor present before addition takes place.

(b) Reaction is, started and maintained, between defined temperature limits:

- i) addition started above specified minimum reactor temperature,
- ii) no external heat input during peak rate of reaction,
- iii) only one reactor module of paired reactor set at high thermal load,
- iv) specified time between additions where split addition is used,
- v) adequate cooling capacity,
- vi) adequate cooling water flow,
- vii) adequate cooling water temperature.

(c) Amount of accumulated reactants is below that which would cause the relief/quench system capacity to be exceeded (**maximum back pressure should be stated**):

-
- i) sufficient agitation,
 - ii) limited amount of accumulated reactants.

(Note: If unable to establish the degree of deviation that would cause the process to operate outside the defined operating envelope, use the conservative assumption that **any** deviation will cause the system to operate outside the defined operating envelope).

Where inherent safety is dependent upon the availability of other system(s), this should be highlighted; such as if sufficient reactant accumulation could not occur to overcome the cooling system.

Establish each system's thermal capacity

The method of heat removal should be stated, such as cooling jacket, or vent/reflux condenser. The maximum cooling capacity for each reactor should be determined, with the water cooling system at the greatest expected level of thermal stress during normal operation:

- cooling water flow just above the trip/interlock set point;
- cooling water temperature just below any trip/interlock set point;
- maximum summertime temperature and humidity (obtained from cooling water tower design standard);
- greatest degree of fouling process side and tube side;
- lowest expected cooling water inventory (with no emergency cooling);
- with other reactor in the pair (or other plant) at the greatest expected load.

Establish range of predicted exothermic events and quantify

This should include:

- maximum accumulation of reactants;
- maximum self-heat rate dT/dt ;
- maximum rate of pressure generation dP/dt ;
- maximum overpressure;
- total heat released.

This could be achieved by initial tests being performed adiabatically with batch charges at ambient temperature and no inhibitor present. Test volumes should be proportionate to reactor volume and maximum batch size. Tests should be performed using equipment with a comparable phi factor, or greater than that of the plant.

Calculation can be used provided the necessary assumptions can be substantiated.

Calorimetry/calculation should demonstrate that the reactor system can either: contain; be quenched; or has sufficient relief capacity to contain process excursions caused by the deviation outside the defined condition(s)/parameter(s).

This should include a blow-down/flow test to characterise the relief stream at the set pressure, of each reactor, that the particular process can be performed in, and a possible range of compositions.

The requirement for isothermal calorimetry should be considered where the basis of safety involves operating a feed rate limited regime. This can be used to assess degraded performance, for example: if two cooling water pumps are normally in service, the relief system could be adequate for the failure of a single pump but not both. Similarly, the relief vent could only have sufficient capacity for the level of an accumulated reactant, but only at up to 23% of the feed rate set-point.

Possible sub-scenarios for batch processes

For feed rate limited batch reactions, a fault tree may be required to reach the required degree of resolution. The fault tree may include:

- (i) Temperature control failure**
- (ii) Cooling system failure:**
 - tower (or other system) failure;
 - fan failure,
 - packing collapse,
 - low cooling water level (LOC),
 - valve closed in error,
 - strainer blocked,
 - demand exceeds tower capacity.
- (iii) Quench addition failure:**
 - quench head tank level low;
 - operator error;
 - exotherm exceeds quench addition rate/charge;
 - trip failure.
- (iv) Relief system failure:**
 - high level in reactor.
- (v) Inhibitor not charged:**
 - concentration too low,
 - insufficient quantity charged,
 - charged too late/early.
- (vi) High reactant addition rate:**
 - maximum rate of addition on system failure (for example, return line blocked);
 - high concentration.

(vii) Under addition of other materials

(viii) External heating

Annex 8 - Suggested criteria to determine harm to the person from thermal radiation

Basis of the suggested criteria

The criteria for thermal effects to the person generally assume that they are subjected to just thermal radiation, are clothed, and are in the open. The type of clothing may modify the effects of thermal radiation by providing a shield if it doesn't ignite. However, there is no consistent data available to adjust the stated criteria to account for this. Separate criteria are provided to determine when the interior of a building could be considered to be engulfed in flames.

For longer duration fires, persons may gain some benefit by running away from the fire. In addition to being able to run away, persons inside a building will be protected to a degree against thermal radiation if the building itself does not ignite. The criteria of spontaneous and piloted ignition are used to define the onset of building ignition.

Thermal dose criteria are for people not engulfed by the flames and hot gas. Where people are engulfed by the flames, such as if they were inside a flash fire cloud, or a fire occurs in an oxygen enriched atmosphere, it is assumed that the persons will be killed by a combination of some, or all, of the following: a dose of radiation, direct skin damage caused by their clothes catching fire, shock and asphyxiation caused by inhaling hot gas/smoke/unburned gas or vapour.

Criteria associated with thermal effects on the person

Thermal hazard	Significant likelihood of death (SLOD)		Equivalent 'dangerous dose'	
	Normal population	Vulnerable population	Normal population	Vulnerable population
Fireball (without escape)*	$1800 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$500 \text{ s. (kW/m}^2)^{4/3}$
Jet fire	$1800 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$500 \text{ s. (kW/m}^2)^{4/3}$
Pool fire	$1800 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$1000 \text{ s. (kW/m}^2)^{4/3}$	$500 \text{ s. (kW/m}^2)^{4/3}$
Flash fire	A person within the LFL envelope is assumed to be a fatality; between LFL to $\frac{1}{2}$ LFL they are considered to have received a dangerous dose.			
Fire due to oxygen enrichment	A person in a fire within the 35% oxygen concentration envelope is assumed to be a fatality.			

Criteria associated with thermal radiation effects on buildings

Thermal hazard	Threshold	
	Spontaneous ignition	Piloted ignition
Fireball	$167.6 \text{ kJ/m}^2\text{s}^{1/5}$	-
Jet fire - constant flux, building exterior	25.6 kW/m^2	14.7 kW/m^2
Jet fire - constant flux, building interior	40.0 kW/m^2	-
Jet fire - variable flux	$167.6 \text{ kJ/m}^2\text{s}^{1/5}$	$118.4 \text{ kJ/m}^2\text{s}^{1/5}$
Pool fire	25.6 kW/m^2	14.7 kW/m^2

Consideration of escape on-site

It is normally assumed that a healthy person can escape at a velocity of 2.5ms^{-1} . The area where the person of interest is located should be examined to determine a reasonable escape distance; a default of 50 m could be used.

When a person reaches a flux of 6.3 kW/m^2 , it is generally assumed that they are at the point where they will no longer accumulate further significant amounts of thermal radiation.

A fireball produces a burst of thermal radiation that is of relatively short duration (~ 3 to 30 seconds burn duration). It is normally assumed that an exposed person has no time to escape, and therefore receives a constant level of thermal radiation for the duration of the fireball.

Consideration of escape off-site

It is assumed that a healthy person from the normal population will usually be able to escape from the fire and seek shelter, travelling at a velocity of 2.5 ms^{-1} , and a person from a vulnerable population (for example, old people's home) escapes at a velocity of 1 ms^{-1} . If a person is immobile or of very limited mobility (for example, hospital patients), it is assumed that the person is static, and accumulates thermal radiation for the duration of the event or a stated time.

A person escaping from a major hazard fire will need to travel a certain distance before shelter in the form of a building, or shade behind a wall, is reached. For off-site populations, assumed distances of 50 m and 75 m are normally assumed for escape in suburban and rural areas respectively. As with escape speeds, these distances may need to be modified for individual cases.

The number of thermal dose units received by a person escaping from a long duration fire is integrated over the time taken to travel from the starting point to a place of shelter. Compared to standing still, a person gains two benefits by travelling away from the fire. Firstly, the incident thermal flux reduces as they move away from the fire, and secondly the duration of their exposure to thermal radiation is limited. Suitable models take account of both of these effects. Hazards associated with jet fires can be highly directional and are assessed with allowance for escape relative to the hazard direction. No allowance for escape is normally made for escape from fireball hazards because the burn durations are short.

It should be noted that where there are expected to be very large populations present, who are corralled and/or their egress is controlled/limited (such as large sporting venues or music festivals), the escape velocity and distance should be tailored to the particular circumstance.

Criteria for the thermal radiation effects on buildings

Buildings will catch fire if the combustible parts of the building exterior ignite. This may occur by either of two mechanisms: spontaneous ignition due to high heat flux; or piloted ignition. In the former case, the thermal radiation flux is sufficiently high to ignite the combustible material on its own, whereas in the latter case a source of ignition also needs to be present.

Criteria for spontaneous and piloted ignition of buildings

The ignition of wood is used as the basis for establishing the criteria of a higher flux level at which a building is assumed to offer limited protection (5 to 15 minutes) before spontaneously igniting; and a lower flux level at which a building is unlikely to suffer piloted ignition, and would therefore afford protection for an unlimited duration. The presence of plastic elements such as doors, window frames, soffits and fascia boards; are likely to reduce the flux level at which ignition may occur.

In addition to ignition of the building exterior, it is recognised that at very high thermal flux levels it is possible for the materials within a building to spontaneously ignite. At 40 kW/m^2 , glass normally shatters under thermal shock; if it doesn't shatter, transmission of thermal radiation through window glass will still normally be sufficient to spontaneously ignite curtains, carpets, and furniture. Therefore, at a thermal flux level of 40 kW/m^2 , it is assumed that buildings will offer no protection, and escape will be required. It should be noted that persons continually exposed to 40 kW/m^2 , escaping at normal

speeds, will always exceed 1000 tdu. The criteria for ignition of the building exterior, given above, assume that the thermal flux level on the building remains constant.

Consideration of fire engulfment

In some cases, the potential for direct fire engulfment may be important. In the case of: a fireball, a horizontal jet fire, flash fire, or a windblown pool fire; there is a potential for people in the vicinity of the release point to be engulfed by the fire. The hazard range for engulfment is normally defined by: the radius of the fireball, the length of the jet fire, or the length of the 'pool fire blowing' (a fluttering tilted cylinder of flame rising from the bund, distorted, cleaved, and spread by the wind).

Whilst fireballs and jet fires have the potential to engulf persons within the vicinity of the release point; flash fires have a similar potential, but often to some distance remote from the release point. The minimum distance considered as being in the cloud is set by the lower flammable limit. As the cloud tapers and dispersion is increasingly affected by terrain and topography, the distance to half the lower flammable limit ($\frac{1}{2}$ LFL) is an indication of the maximum range within which persons would be liable to be engulfed by a flash fire. It is therefore suggested that within the distance to LFL, a person would be fatally injured; between LFL and $\frac{1}{2}$ LFL, people exposed would be considered to have received a dangerous dose of thermal radiation.

Criteria associated with thermal hazards due to oxygen enrichment

There are a number of installations in the UK that store and handle liquid oxygen. Oxygen possesses major hazard potential due to its ability to increase the potential for, and the severity of, fires involving combustible materials within the oxygen-enriched atmosphere.

As the oxygen concentration in air is increased, the ease of ignition, burning rate, and fire spread; exhibit a non-linear rate of increase. In general, these effects are slight at 25% oxygen, significant at 40% and near to their maximum at about 50%. Beyond 50%, the increase in effect due to further enrichment is barely detectable. Where bulk oxygen can be released into an area where hydrocarbons and/or flammable solvents are processed, it is generally assumed that above a concentration of 35% v/v oxygen, a fire will give rise to a dangerous dose of thermal radiation.

Annex 9 -Suggested criteria to determine harm to the person from exposure to toxic gases and vapours

Suggested criteria to determine harm to the person from exposure to toxic gases and vapours can be found on the following pages on the HSE website. These are updated, so should be referred to when required:

Toxicity levels of chemicals - Death and Dangerous Dose 'Assessment of the Dangerous Toxic Load (DTL) for Specified Level of Toxicity (SLOT) and Significant Likelihood of Death (SLOD)'

<https://www.hse.gov.uk/chemicals/haztox.htm>

Annex 10 - Suggested criteria to determine harm to the person from overpressure (and impulse)

The focus of an explosion assessment is usually the overpressure produced, often expressed as 'peak side-on overpressure' (P_{so}). This is the maximum pressure experienced by the face of an object as the pressure wave reaches it; as if the object and the source of the explosion were suspended facing each other far from the ground. In normal circumstances there is also a reflected pressure wave from the ground and other surrounding surfaces. These reflections both combine and rarefy, increasing the pressure objects experience. The blast actually experienced is the peak side-on overpressure and reflected overpressure, the total of which may be up to six times the peak-side on overpressure. Therefore, where a value is found to be just below a threshold of harm from overpressure, it should be taken to that threshold in order to be sufficiently conservative.

People in the open

People in the open are subject to the primary secondary and tertiary effects of blast.

Primary effects: Caused by the body being subject to direct pressure and include lung damage and ear drum rupture. Very close to the blast, other internal organs could be damaged.

Secondary effects: Missiles created by fragmentation of anything containing/surrounding the explosion, such as vessel fragments or building materials. Fixtures and fittings may become detached then entrained, when subject to dynamic pressure or air flow. The velocity and size distribution of objects is highly dependent on the specific circumstances in which the explosion occurs. Harm may come from penetration by sharp objects or blunt trauma by large objects. Glass fragments appear to be given undue importance in determining harm. Where the blast is from an internal vessel explosion, it will be necessary to assume a vessel fragment distribution, and in turn the harm caused. There are a number of models given in the literature, the model used being dependent upon circumstance.

Tertiary effects: These are caused by dynamic pressure pushing a person to the ground or into fixed objects, directly resulting in injury. This can include head injury and blunt trauma to the torso. Transitional effects may also be included, this occurs when a person is given momentum by the air flow, the limbs being damaged or torn-off as the body impacts with objects as it moves through space. A TNT explosion giving rise to a peak overpressure of 10psi, will give rise to airflows of up to 294mph (132ms^{-1}); this creates a dynamic pressure of 152mbar.

In reality, multiple injuries resulting from primary, secondary, and tertiary effects, are expected when a person is subject to significant blast. Considered separately each of these injuries may be survivable, together they could result in 'polytrauma', which is very difficult to diagnose and treat. It is possible that when individual harm criteria are assessed in isolation, this substantially underestimates the risk of death or serious injury. As a rule of thumb, 250mbarg could be considered to be the threshold to serious injury for a person in the open exposed to blast.

It is important that the assessor considers the surroundings of the person subject to blast, and selects values that are reasonably conservative for both death and serious injury. It is not possible to specify this value given the wide variety of circumstances. A table of selected values is given in order to assist the assessor.

<i>Damage details:</i>	<i>Incident equivalent peak overpressure (mbar)</i>
<i>Effects on people</i>	
Threshold for temporary hearing loss	6.9 to 13.8
Threshold for eardrum rupture	138
Minimum for penetration injury by small glass fragments	55.2
Threshold of skin laceration by missiles	69 to 138
Persons knocked down or thrown to the ground	103 to 200
Possible death of persons by being projected against obstacles	138
50% probability of eardrum rupture	345 to 483
90% probability of eardrum rupture	689 to 1034
Threshold of internal blast injuries	483
50% fatality from serious missile wounds	276 to 345
Near 100% fatality from serious missile wounds	483 to 689
Threshold of lung haemorrhage	827 to 1034
50% fatality from lung haemorrhage	1379 to 1724
Near 100% fatality from lung haemorrhage	2068 to 2413
Immediate blast fatalities	4826 to 13790
General effects on buildings	
5% of exposed glass panes broken	1.24 to 2.9
50% of exposed glass panes broken	5.52 to 13.1
Near 100% of exposed glass panes broken	46.2 to 110.3
Limited minor structural damage	20.7 to 27.6
Doors and window frames may be blown in	53.1 to 89.6
Partial demolition of houses - rendered uninhabitable	68.95
Lower limit of serious structural damage	137.9

Partial collapse of walls and roofs of houses	137.9
Nearly complete destruction of houses	344.7 to 482.6
Probable total destruction of houses	689
Effects on UK brick-built houses	
Category A damage - completely demolished	689.5 to 1827
Category B damage - badly damaged and beyond repair	244.7 to 586.1
Category Cb damage - uninhabitable without extensive repairs	137.9 to 241.3
Category Ca damage - uninhabitable but repairable	68.9 to 124.1
Category D damage - inhabitable but repairs required	17.2 to 51.7
50% destruction of brickwork	275.8 to 482.6
Effects on industrial buildings	
Steel frame clad building slightly distorts	~ 90
Cladding of light industrial building ruptured	~ 276
Effects on plant	
Reinforced structures distort and unpressurised storage tanks fail	210 to 340
Wagons and plant items overturned	340 to 480
Extensive damage	above 480
Failure of a pressurised storage sphere	above 700

Harm to a person inside a building

Unlike thermal radiation, a person is often more susceptible to harm from blast overpressure inside a building rather than outside it, due to its susceptibility to damage and consequent collapse. Buildings are also affected by 'impulse', this is the wave of positive pressure followed by negative pressure which occurs when an explosive is detonated, or a fast deflagration occurs. Impulse creates a 'push and pull' effect, which is very much greater for vapour cloud explosions than for conventional explosives; and therefore very much more damaging for the same peak side on overpressure. The limit of partial building collapse occurs at approximately 140mbarg, with the limit of total collapse of traditionally built housing occurring at approximately 700mbarg. Industrial buildings are generally of differing construction to housing so are specifically addressed below.

On-site occupied buildings

Site-occupied buildings subject to vapour cloud explosion should be screened for their resistance to overpressure and impulse as part of an occupied buildings survey. Rudimentary guidance is given in

the CIA 'Guidance for the location and design of occupied buildings on chemical manufacturing sites' 4th edition 2020. This suggests a vulnerability relationship for four building types: hardened structural buildings; office blocks with concrete frames and roofs, brick block wall panels; typical domestic dwelling timber floors; portable, or semi-portable, or fixed timber construction (often generically referred to as 'Portakabins'). The CIA guidance is only indicative as the position of a building and its surroundings can dramatically affect the level of overpressure it's exposed to. The building age and type of construction can also dramatically affect a building's ability to withstand overpressure. It is strongly recommended that where a process can give rise to a significant vapour cloud explosion (>150mbarg), or accumulates a significant amount of materials categorised as explosive, then an occupied building survey should be carried out by a qualified specialist in blast resistance assessment. It should be noted that where an on-site occupied building cannot withstand the peak side-on overpressure and also impulse, a case would need to be made why the occupants cannot be moved, or the building strengthened or replaced.

Off-site occupied buildings

Since WWII there have been numerous advances in civil engineering which means there are now a wide variety of buildings with a wide variety of construction techniques in use.

- Traditional brick dwellings:
 - single-storey brick,
 - two-storey brick,
 - terraced,
 - triple-storey brick (town house).
- Multi-storey cellular dwellings:
 - multi-storey reinforced concrete decks with glass and/or concrete curtain walls,
 - multi-storey steel framed with brick/concrete panels.
- Retail/workplace/public buildings:
 - coated-steel clad steel portal frame buildings,
 - reinforced concrete curtain walled buildings,
 - glass curtain walled buildings,
 - open deck car parking.
- Variants that may need to be considered:
 - long span – supermarkets/sports hall,
 - high rise – very tall multiple deck structures.

Some use frames, others use long spans with geodetic curtain walls, others are multiple modular systems. Those that flex may cope well with the long impulse generated by VCE, those which depend on a high strength curtain wall may totally collapse once this is compromised.

For buildings that may be exposed to blast overpressure of more than 140mbarg, other than brick-built domestic dwellings, it would be expected that the Operator would obtain advice from a qualified specialist in blast resistance assessment.

Traditional brick-built domestic dwellings

Most of the work on the blast resistance of housing comes from WWII bomb damage. This is problematical for two reasons. Firstly, brick houses are now usually built with a structural inner wall which carries most of the load, the brick curtain wall has little structural function; they have a non-structural dampcourse, few if any inner supporting walls, so have little connection to the foundation;

often have heavy concrete tile roofs. Whilst this makes for a dry stable house, these factors may substantially lower blast resistance.

Secondly, high explosives have a very short impulse duration, whilst VCE have a long duration impulse which is much more damaging to structures. Together, this would suggest that criteria generated from WWII bomb damage is not very conservative. This is important when evaluating blocks of housing which may be just outside the threshold criteria.

It is suggested that the following threshold criteria for brick-built domestic housing are used:

<i>Threshold</i>	<i>Overpressure</i>	<i>Harm to people</i>
Extent of window glass breakage	2.5mbarg	Limit of injury to people in buildings
Beginning of partial collapse	140mbarg	Assumed occupants receive an equivalent dangerous dose
Probable building collapse	700mbarg	Assumed occupants are fatally injured

Between 2.5mbar and 140mbar buildings may suffer glazing damage, with windows and doors being blown in toward the higher end of that range. Consideration should be given to the likely number of serious injuries. Unless there is a vulnerable or sensitive population present it would be expected that fatalities would only be a few percent as injuries would be caused by flying glass and fragments of frames. It would be possible but unlikely that a person struck by a door or window frame would be a fatality. However, if there were a large number of homes, say 50 or more, located in the 2.5mbar to 140mbar zone, then it would be reasonably conservative to expect that this would result in a fatality.

From 140mbarg upwards, it is expected that partial collapse of some brick-built houses would occur, with some suffering total collapse at 700 mbar. As discussed earlier, the degree of conservatism is justified given reflected overpressure and modern construction.

Other off-site building types

For most sites, only a very large VCE would give rise to overpressures above 150mbar outside the site boundary.

Where a process can give rise to a significant vapour cloud explosion, or accumulates a significant amount of materials categorised as explosive; such that it can give rise to an off-site side-on overpressure that exceeds 150mbarg; then either:

- (i) the Operator should establish which off-site buildings on the population location list are within the 150mbar side-on overpressure isopleth, and an off-site building survey should be carried out by qualified specialist in blast resistance assessment (which also considers impulse);

OR

- (ii) it should be assumed that between 150mbarg and 700mbarg the off-site population in a building would experience the equivalent of a dangerous dose; and a person in a building exposed to over 700mbarg would experience the equivalent of SLOD.

Annex 11 - Example simple scenario frequency summary table

Note: this is a **summary** table. Where there are many sub-scenarios with many different protective systems, summary tables are useful to show the different initiating events and layers of protection that are present. Caution should be used when using a summary table to calculate a final frequency as it may not consider common cause failures (CCF), and common mode failures (CMF), and can overestimate the true reliability of the protective systems.

Category 4 event frequency		
Initiating events:	Frequency/ probability	Justification
Tank level indication failure, system LI xxx/x.	0.1 per year	Typical level instrument failure on a clean duty (Appendix x – Table X).
Operator error, for example, fail to swap over tanks.	0.16 per year	Single operation per week, error of an act embedded in a procedure Appendix y – Table Y . (The frequency assumptions assume batch wise operation which is the worst case in terms of likelihood of a tank overfill event.)
Pump failure.	0.01 per year	Pump failure on a clean duty (Appendix x – Table X). Credit is taken for the independent response from the receiving plant digital flow gauge at North Site. Warning from FD unit flow loss would be rapid, within minutes, therefore apply an order of magnitude risk reduction for this mitigation.
Layers of protection:		
Operator response to high level alarm to Central Control LAH xxx/x set at 8.67 metres.	0.1	At the normal filling rate of 60 tonnes/hour, the time from the high-level alarm to the extra high level alarm is 30 minutes. To tank overfill, the time is in excess of 20 hours. Probability of inadequate operator response 0.1 (Appendix y – Table Y). Non-independent from initiating cause of LI xxx/x failure.
Operator response to extra high-level alarm to Central Control LAHH xxx/x set at 10.71 metres.	0.3	Less credit taken for the second alarm because of common cause failure with LAH5283/4. Alarm is routed to the same control room, although it is permanently manned. For LI yyy/y failure no credit is taken for LAH xxx/x, but a 0.1 probability of failure on demand is taken for LAHH zzz/z.
Routine operator check of tank level via tank-side gauge LG zzz/z.	1.0	Tank levels are routinely documented from control room instruments and therefore no credit is taken for monitoring of local tank-side gauges.

Weather conditions.	0.1	F2 weather conditions that support a large hazard range for a drifting vapour cloud occur for 10% of the time at this location (see section x.x.x.x).
Emergency intervention by operations to isolate the feed to the tank.	1.0	Gas detection (tanker loading area) alarms to central control and the tank side ROSOV are remotely operable from Central Control. However, no credit taken because this represents a further alarm to the same operator (in addition to the tank level alarms), detection effectiveness is wind direction dependent, the location of the gas detectors is remote from the leak source and their operation may be too late, in that a flammable cloud has already drifted as far as the road tanker loading bay and the fire hazard may be realised before effective response is made.
Probability of delayed ignition.	0.5	The HSE vapour cloud model (site SR Reference 7) predicts a vapour release rate of 7 kg/second. Probability of delayed ignition for a vapour release of 7kg/second 0.02. However, for a large drifting vapour cloud, this would seem overly optimistic. For this reason, an average probability of delayed ignition of 0.5 is applied.
Probability operator/ tanker driver present and injured.	0.14	Road tanker loading bay is in the prevailing wind direction (directional probability 0.7) and the occupancy of the road tanker bay is taken as 0.2 based on operating experience. All other areas covered by routine operator patrols occupancy less than 0.1 (Appendix zz – Table Z).
Two tank operation.	0.5	The above analysis applies to T01 and T02 therefore to consider each tank individually requires a 0.5 factor.
Event frequency:	5.2 x 10 ⁻⁵ per tank per year	

Annex 12 - Example of a layer of protection summary table

Initiating event table:									
Scenario S5. Distillation Column Loss of Containment due to Overpressure									
Ref	Sub-scenario/(initiating event) (broken down into initiating events where appropriate)	Initiating event frequency (.yr ⁻¹)	Notes/basis						
A	REBOILER HIGH VAPOR RATE	0.17							
a(i)	Temperature Control Loop TIC674 failure (Temperature sensor TT/TE 674, control valve TCV674, PLC-XIC 9)	0.1	Failure of DCS type control loop as per BSEN 61511 (Would require full justification and breakdown for high proportionality scenario)						
a(ii)	E409 Tube Failure	0.06	Site developed shell and tube failure rates, see report J609.						
a(iii)	Control TCV 674 by-pass open	0.01	Operator error (see study ref 2.33.506)						
B	CONDENSER FAILED	0.024							
b(i)	Cooling water failure	0.02	Includes low/no flow, high temp, isolation in error (see section xx).						
b(ii)	Fouling	-	High purity process materials and cooling water quality. Considered further in general measures - see section yy.						
b(iii)	Mechanical failure	0.004	Site developed shell and tube failure rates, see RR358.						
C	REFLUX SYSTEM FAILURE (events would be expanded below)	0.05							
D	BLOCKED/ISOLATED VENT (events would be expanded below)	0.01							
E	COLUMN FLOODED/BLOCKED (events would be expanded below)	0.02							
Sub-scenario Reference	Initiating Event Frequency Yr ⁻¹	Pre-alarms to Trip	ESD High Pressure Trip –(XPE0256) - Column Feed Isolation closes valve XCVE02 - Reboiler E409 Steam Flow Trip - closes Steam isolation valve XCVE04 and opens condensate blow-down valve XCVE05	Control system HIHI Pressure Trip PAHH PT569 - Closes feed valve FCV129 - Closes steam valve TCV12	Control System HI Temperature Trip - Closes TCV12	Control system Column Feed Hi Flow Trip - Closes FCV129	Control System Cooling water failure Trip FS125 - Trips closed feed valve FCV129 and steam valve TCV12	Column Relief Valve PRV002 lifts - discharge to flare (see study 36.258.54 Flare availability)	Sub-Scenario Frequency Yr ⁻¹
A	0.17	1	0.05	-	0.1	-	-	0.04	3.4 x 10 ⁻⁵
B	0.024	1	0.05	-	-	-	0.1	0.00	4.8 x 10 ⁻⁶
C	0.05	1	0.05	0.1	-	-	-	0.04	1.0 x 10 ⁻⁵
D	0.01	1	0.05	0.1	-	-	-	0.04	2.0 x 10 ⁻⁶
E	0.02	1	0.05	0.1	-	-	-	0.04	4.0 x 10 ⁻⁶
Scenario Frequency Loss of Containment									5.4 x 10⁻⁵

Annex 13 - Failure rate data sources

The following provides a non-exhaustive list of industry accepted data sources; noting that many of the sources are associated with other sectors such as nuclear, defence and telecoms. Nevertheless, the sources often contain data relevant to the operations of CDOIF members. Unless specified otherwise in the source, failure rates are given for a clean process fluid and stress-free environment. It is for the Operator to ascertain the suitability of any data used. **The colloquial name is given in bold.**

Smith, D.J. (2021) 'Reliability, Maintainability and Risk', 10th edition. Butterworth Heinemann. Standard text covering topics including reliability assessment techniques and a selection of methods used in quantitative risk assessment. The book also contains extracts from the FARADIP.FOUR reliability database.

Technis; **FARADIP.FOUR** Database. Comprehensive component level database from a range of industry sources, including data on failure rates and failure modes.

Reliability Dynamics; Process Equipment Reliability Database (PERD). Reliability database originally run as a standalone project by the Center for Chemical Process Safety, now offered as an add-in for the SAP platform.

Quanterion Systems Inc:

Nonelectronic Parts Reliability Data (**NPRD-2023**),

Electronic Parts Reliability Data (**EPRD-2014**),

Failure Mode/Mechanism Distributions (**FMD-2016**).

Reliability Prediction Standard (**MIL-HDBK-217**) (also contains failure rate estimates for the various part types used in electronic systems)

Extensive collection of failure rate and failure mode data from across the US Department of Defence, now offered as a cloud-based service.

FIDES; Reliability Methodology for Electronic Systems, Edition A (July 2023). Detailed methodology, based on physics of failure, for predicting failure rates of electronic systems.

OREDA; Offshore and Onshore Reliability Data. Extensive collection of failure rate and failure mode data, primarily topside and subsea process equipment from Norwegian North Sea oil and gas platforms, now offered as a cloud-based service. Can be considered as complementary to the PDS Handbook.

SINTEF; PDS Data Handbook 2021, Reliability Data for Safety Equipment. Developed to support reliability assessments of safety instrumented systems that should comply with IEC 61508 & 61511. Extensive collection of failure rate and failure mode data, primarily topside and subsea safety-related equipment from Norwegian North Sea oil and gas platforms, can be considered as complementary to OREDA.

United States Naval Surface Warfare Center; Handbook of Reliability Prediction Procedures for Mechanical Equipment (January 2010). Detailed methodology for calculating reliability and maintainability of mechanical equipment, also available as a freeware software application, **MechRel**.

Exida; Component Reliability Database Handbook (CRD), 6th Edition. Handbook in three volumes covering reliability data for an extensive range of plant and equipment: Volume 1, Electrical Components; Volume 2, Mechanical Components; Volume 3, Electrical Sensor Components. Can be considered as complementary to SERH.

Exida; Safety Equipment Reliability Handbook (SERH) Database, 4th Edition. Handbook in three volumes covering reliability data for safety instrumented systems: Volume 1, Sensors; Volume 2, Logic Solvers; Volume 3 Final elements. Can be considered as complementary to CRD.

IEEE; Std. 500-1984, IEEE Guide to the collection and presentation of electrical, electronic, sensing component, and mechanical equipment reliability data for nuclear-power generating stations. Includes an appendix of reliability data intended for the use of nuclear systems reliability analysts and design engineers which may be applicable to other sectors.

Netherlands Institute for Public Health and the Environment; '**Guideline for Quantitative Risk Assessment**', known as the '**TNO Purple Book**' **CPR 18E, 2005.** QRA handbook for major hazards Operators in the Netherlands. Includes base failure rates for vessels and other process equipment containing dangerous substances, plus a method for estimating release rates from pipework.

International Association of Oil & Gas Producers; **IOGP 434-03**, August 2022, Storage Incident Frequencies. Part of an extensive directory of release frequencies and other data relevant to QRA in the oil and gas sector. NB: Not suitable for scenarios which are configuration specific, involve random failures in control systems or human factors, see 4.7.6 Parts Count.

Failure Rate and Event Data for use within Risk Assessments ('**FRED**'), 6 November 2017, HSE. Failure rate failure frequencies for Hazardous Substance Consent. Context specific, and may not be applicable. Where mechanical failures that may lead to MAHS are driven by predictable service-induced degradation (for example the perforation of pipelines and vessels by corrosion), and the failure rate is largely determined by the quality and rigour of the management system; then the use of FRED values may be appropriate, see 4.8.9. The values given could also in this case serve as a starting point in the absence of site-specific data. If Operators use this data, it should be stated why the use of FRED is appropriate, or if it has been used simply as a comparator. However, where MAHS or sub-scenarios involve loss of process control, these frequencies should be calculated from the principles outlined in **section 4.9**.

Note – See Annex 18 for human error identification/probability references.

Annex 14 - Deriving failure rates from site data

Purpose

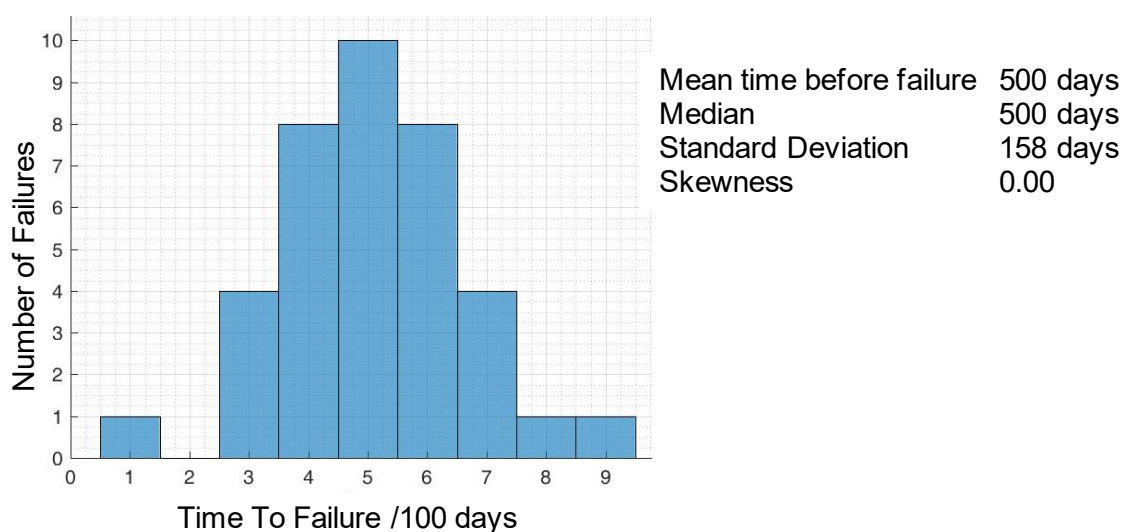
Site data can be used very effectively to determine failure rates for the specific equipment model used on site; or corroborate generic failure rates at component, sub-assembly and simple equipment level (pump model, agitator model, filter model). Operators are encouraged to derive their own failure rates where possible, if only to corroborate any generic values used. This annex is not intended to be a comprehensive guide to deriving failure rates from site data; but to provide an overview of the assumptions, process and treatments used.

Data collection

The practicality of this may be determined by how data is currently collected. In many cases, it may need to be compiled from various sources such as: break-down reports, proof-test logs, and routine maintenance reports. It is strongly recommended that if site generated failure rates are to be incorporated into the safety management system, an integrated system of data collection is put into place; so that there is no additional burden, and all failures are reported. It should be possible to determine the type, size, and manufacturer of the particular component/device from any report. The failure mode should be recorded, and if necessary resolved later, as to whether it is a failure to danger; alternatively, it could be conservatively assumed that all failures are to danger. To limit the amount of data required, the process can be simplified if there are common assemblies used on site. For example, a common ESD valve package: with a specific ball valve manufacturer, a common actuator package, common position feedback indicator, standardised air solenoid: in this case failures could be recorded against the standardised unit.

Sample size and distribution

One of the most significant issues of site data collection is the sample size. In most cases, a few data points will not be sufficient to generate a meaningful failure rate. Simply using the arithmetic mean for the failure rate, without any supporting analysis, may give misleading results in some cases; a larger sample size may be needed to achieve the desired level of confidence. A common rule of thumb is to accept a sample of 30, or greater, as being statistically significant; in some cases a smaller sample may suffice, in others larger sample is required.



Calculating the standard deviation and variation gives some insight into the data. High variability in the population requires a larger sample size, as variability within the population causes the margin of error to increase. A low variation would justify a smaller sample size. The use of less than ten data points may not be considered sufficiently robust unless the variation is very low, however this could be used in conjunction with generic data to show that the failure rate used is appropriate.

Excel includes an optional 'Data Analysis' add-in under the 'Data' tab that quickly calculates the mean, median, standard deviation and skewness for a data set. There are also statistical software packages available.

Counting failures

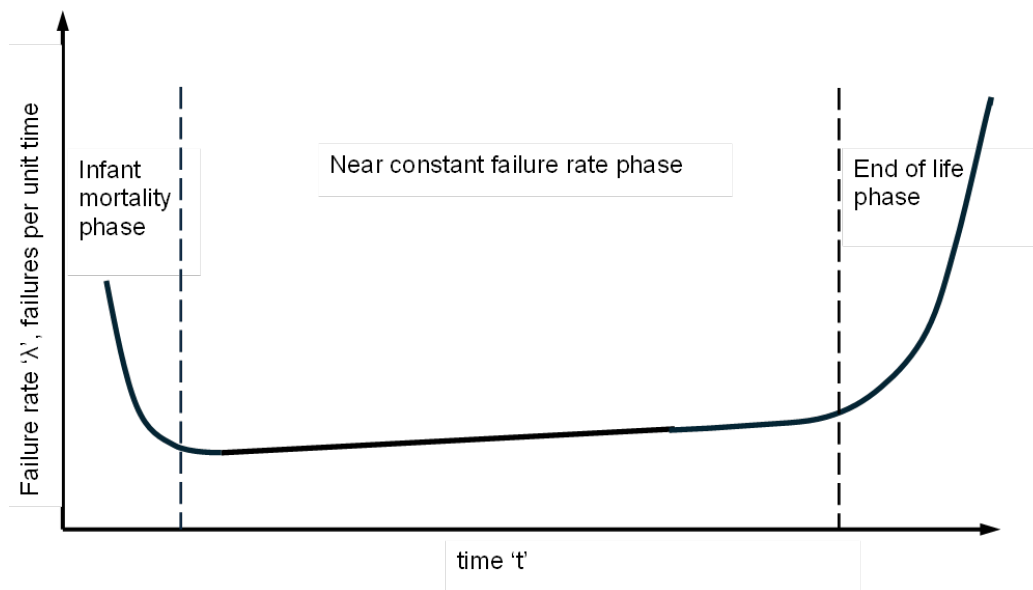
If a population of devices has not exhibited any failures over many years, this does not mean that the failure rate is so low that it does not need to be considered. It could be that the failure rate is very low, so the number of devices and cumulative time at risk is insufficient for a failure in the population to have occurred. It is possible that a component is about to fail and would have failed a few hours after the data was collected, or the test completed. It is normal practice to add a single failure to the data before determining the failure rate. This treatment is not problematical when examining a large population but may need further thought where the population is small.

Pre-conditions to allow the statistical treatments to be meaningfully applied

For any statistical analysis to be meaningful the component/device must:

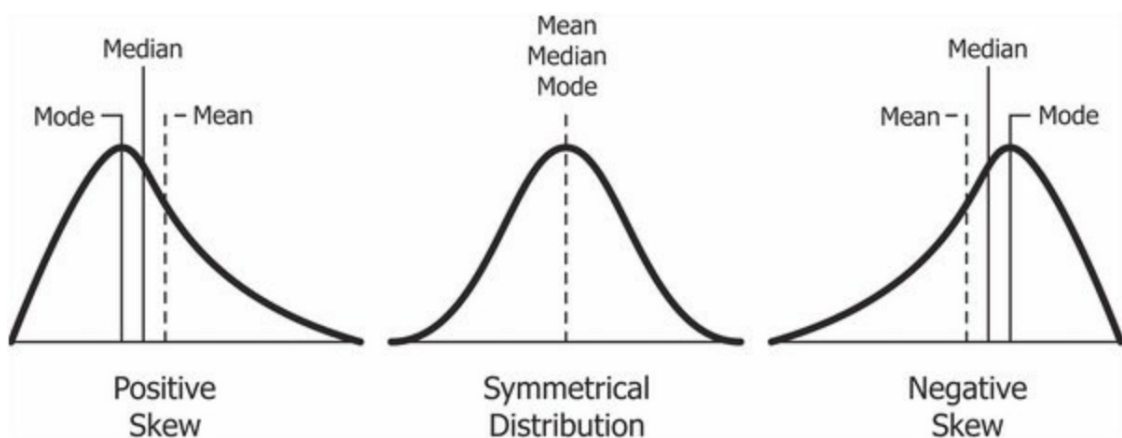
- have been only subject to random failure;
- be in its near 'constant failure rate' phase;
- not subject to external influence;
- maintained appropriately.

For example, in cases where corrosion is the main mode of failure, then failure is not random, but is determined by the operating and maintenance regimes. Failure rates tend to be constant for the greater part of the component/devices effective life, however they may be very much higher when equipment is first installed, and when nearing the end of their life, this gives rise to the well-known Weibull Plot or 'bathtub curve'.



Whilst it is possible to use Weibull approximations in the regions where the failure rate is not constant, this would require a very large data set with a long history, so it is seldom practical. The standard statistical treatments are based on the flat, near constant failure rate, part of the curve. This is borne out by everyday experience where very old equipment often suffers from high failure rates with unpredicted failure mechanisms. For critical applications manufacturers may subject new components/devices to an extended test in order to approach the constant failure rate period when installed.

Skewed data



If the component/device is subject to external influence or the failures are not entirely random, this can be detected in the distribution of the data. If the data plotted as a frequency distribution gives the classic bell-shaped curve, the distribution is said to be 'normal' and failure random.; and allows key relationships to be meaningfully derived. For a normal distribution the mean, median, and mode, are all on the central inflexion point of the curve. However, it is normal for the data to show some 'skew'; this is where the median is offset to the right or the left of the mean. Further information on skew can be found in most statistical textbooks or software packages such as Minitab. The degree of skew can be assessed simply using 'Pearson's Median Skewness Test', or the 'Fisher - Pearson Equation' used in many statistical software analysis packages. It should be readily apparent if the failures are not at all random; it is not practical to give advice here on when the data is so skewed it cannot be

used to calculate a meaningful failure rate, as this is dependent on both the sample size and the variance.

Basic relationships

In most cases when a component or device fails it is replaced so the plant can continue to function. This is called a replacement model and the mean time between failures (MTBF) is determined. There are also repair models which derive the mean time to repair (MTTR), usually in the context of determining reliability; but consideration of MTBF alone is sufficient in most cases. If the criteria given in the section above on pre-conditions to allow the statistical treatments to be meaningfully applied are met, then it can be assumed that:

$$\frac{1}{\text{Failure rate } '\lambda'} = \text{Mean Time Between Failure 'MTBF'}$$

Where:

$$MTBF = \frac{\text{total cumulative operating time for N devices}}{\text{number of failures from N devices}}$$

Of course, this is an approximation as the site population is only a sample of the total population of that type of component/device. It is assumed that given the appropriate degree of confidence and an appropriate minimum sample size that this relationship is true.

Linking sample size to confidence for the calculated failure rate

The simple Chi-square test is used to determine if the mean time between failures has a confidence interval of 90% or greater. This does require the assumption that the data follows the Chi-square distribution, but if the criteria given in **section 1.4** of this annex hold, then this is considered reasonable. Only a 'one-sided test' is required to determine that the value of 'MTBF or better' would be observed 90% of the time. If unfamiliar with statistics and the application of the Chi-square test when determining failure frequencies, this is discussed in more detail in the reference Smith, D.J. (2021) 'Reliability, Maintainability and Risk' (Tenth Edition) also mentioned in **Annex 13** – Failure rate data sources. This reference also includes an appended table giving the 'Percentage Points of the Chi-square Distribution', though this can be found in most sets of statistical tables.

All populations may not be equivalent

Often the population of that component/device has not all been installed at the same time, but numbers increase as new unit operations are added or replaced. It is reasonable to combine data sets, as long as the failure rate is not selectively derived from a new plant, or a plant with a much less arduous duty, then used for a plant which is long established and whose equipment may no longer exhibit a near constant failure rate.

Deriving probability of failure to danger from failure rates

It should be noted that the failure rates derived from site data, or other sources, cannot be used directly as the probability of failure on demand. The correct mathematical treatment is given at the beginning of **section 4.9** 'Scenario failure frequency data'.

Annex 15 - Standard discount factor table

Year	Discount Rate	Discount Factor						
0	n/a	1	42	3.00%	0.2499	84	2.50%	0.0754
1	3.50%	0.9662	43	3.00%	0.2426	85	2.50%	0.0736
2	3.50%	0.9335	44	3.00%	0.2355	86	2.50%	0.0718
3	3.50%	0.9019	45	3.00%	0.2287	87	2.50%	0.0701
4	3.50%	0.8714	46	3.00%	0.222	88	2.50%	0.0683
5	3.50%	0.842	47	3.00%	0.2156	89	2.50%	0.0667
6	3.50%	0.8135	48	3.00%	0.2093	90	2.50%	0.0651
7	3.50%	0.786	49	3.00%	0.2032	91	2.50%	0.0635
8	3.50%	0.7594	50	3.00%	0.1973	92	2.50%	0.0619
9	3.50%	0.7337	51	3.00%	0.1915	93	2.50%	0.0604
10	3.50%	0.7089	52	3.00%	0.1859	94	2.50%	0.0589
11	3.50%	0.6849	53	3.00%	0.1805	95	2.50%	0.0575
12	3.50%	0.6618	54	3.00%	0.1753	96	2.50%	0.0561
13	3.50%	0.6394	55	3.00%	0.1702	97	2.50%	0.0547
14	3.50%	0.6178	56	3.00%	0.1652	98	2.50%	0.0534
15	3.50%	0.5969	57	3.00%	0.1604	99	2.50%	0.0521
16	3.50%	0.5767	58	3.00%	0.1557	100	2.50%	0.0508
17	3.50%	0.5572	59	3.00%	0.1512	101	2.50%	0.0496
18	3.50%	0.5384	60	3.00%	0.1468	102	2.50%	0.0484
19	3.50%	0.5202	61	3.00%	0.1425	103	2.50%	0.0472
20	3.50%	0.5026	62	3.00%	0.1384	104	2.50%	0.046
21	3.50%	0.4856	63	3.00%	0.1343	105	2.50%	0.0449
22	3.50%	0.4692	64	3.00%	0.1304	106	2.50%	0.0438
23	3.50%	0.4533	65	3.00%	0.1266	107	2.50%	0.0428
24	3.50%	0.438	66	3.00%	0.1229	108	2.50%	0.0417
25	3.50%	0.4231	67	3.00%	0.1193	109	2.50%	0.0407
26	3.50%	0.4088	68	3.00%	0.1159	110	2.50%	0.0397
27	3.50%	0.395	69	3.00%	0.1125	111	2.50%	0.0387
28	3.50%	0.3817	70	3.00%	0.1092	112	2.50%	0.0378
29	3.50%	0.3687	71	3.00%	0.106	113	2.50%	0.0369
30	3.50%	0.3563	72	3.00%	0.1029	114	2.50%	0.036
31	3.00%	0.3459	73	3.00%	0.1	115	2.50%	0.0351
32	3.00%	0.3358	74	3.00%	0.097	116	2.50%	0.0342
33	3.00%	0.326	75	3.00%	0.0942	117	2.50%	0.0334
34	3.00%	0.3165	76	2.50%	0.0919	118	2.50%	0.0326
35	3.00%	0.3073	77	2.50%	0.0897	119	2.50%	0.0318
36	3.00%	0.2984	78	2.50%	0.0875	120	2.50%	0.031
37	3.00%	0.2897	79	2.50%	0.0854	121	2.50%	0.0303
38	3.00%	0.2812	80	2.50%	0.0833	122	2.50%	0.0295
39	3.00%	0.2731	81	2.50%	0.0812	123	2.50%	0.0288
40	3.00%	0.2651	82	2.50%	0.0793	124	2.50%	0.0281
41	3.00%	0.2574	83	2.50%	0.0773	125	2.50%	0.0274

Annex 16 - Discount factors to value human health

Year	Discount Rate	Discount Factor						
0	n/a	1	42	1.29%	0.5488	84	1.07%	0.3271
1	1.50%	0.9852	43	1.29%	0.5419	85	1.07%	0.3236
2	1.50%	0.9707	44	1.29%	0.535	86	1.07%	0.3202
3	1.50%	0.9563	45	1.29%	0.5282	87	1.07%	0.3168
4	1.50%	0.9422	46	1.29%	0.5215	88	1.07%	0.3135
5	1.50%	0.9283	47	1.29%	0.5149	89	1.07%	0.3101
6	1.50%	0.9145	48	1.29%	0.5083	90	1.07%	0.3068
7	1.50%	0.901	49	1.29%	0.5019	91	1.07%	0.3036
8	1.50%	0.8877	50	1.29%	0.4955	92	1.07%	0.3004
9	1.50%	0.8746	51	1.29%	0.4892	93	1.07%	0.2972
10	1.50%	0.8617	52	1.29%	0.483	94	1.07%	0.294
11	1.50%	0.8489	53	1.29%	0.4769	95	1.07%	0.2909
12	1.50%	0.8364	54	1.29%	0.4708	96	1.07%	0.2878
13	1.50%	0.824	55	1.29%	0.4649	97	1.07%	0.2848
14	1.50%	0.8118	56	1.29%	0.459	98	1.07%	0.2818
15	1.50%	0.7999	57	1.29%	0.4531	99	1.07%	0.2788
16	1.50%	0.788	58	1.29%	0.4474	100	1.07%	0.2758
17	1.50%	0.7764	59	1.29%	0.4417	101	1.07%	0.2729
18	1.50%	0.7649	60	1.29%	0.4361	102	1.07%	0.27
19	1.50%	0.7536	61	1.29%	0.4306	103	1.07%	0.2671
20	1.50%	0.7425	62	1.29%	0.4251	104	1.07%	0.2643
21	1.50%	0.7315	63	1.29%	0.4197	105	1.07%	0.2615
22	1.50%	0.7207	64	1.29%	0.4144	106	1.07%	0.2587
23	1.50%	0.71	65	1.29%	0.4091	107	1.07%	0.256
24	1.50%	0.6995	66	1.29%	0.4039	108	1.07%	0.2533
25	1.50%	0.6892	67	1.29%	0.3988	109	1.07%	0.2506
26	1.50%	0.679	68	1.29%	0.3937	110	1.07%	0.2479
27	1.50%	0.669	69	1.29%	0.3887	111	1.07%	0.2453
28	1.50%	0.6591	70	1.29%	0.3838	112	1.07%	0.2427
29	1.50%	0.6494	71	1.29%	0.3789	113	1.07%	0.2401
30	1.50%	0.6398	72	1.29%	0.3741	114	1.07%	0.2376
31	1.29%	0.6316	73	1.29%	0.3694	115	1.07%	0.2351
32	1.29%	0.6236	74	1.29%	0.3647	116	1.07%	0.2326
33	1.29%	0.6157	75	1.29%	0.36	117	1.07%	0.2301
34	1.29%	0.6079	76	1.07%	0.3562	118	1.07%	0.2277
35	1.29%	0.6002	77	1.07%	0.3524	119	1.07%	0.2253
36	1.29%	0.5926	78	1.07%	0.3487	120	1.07%	0.2229
37	1.29%	0.585	79	1.07%	0.345	121	1.07%	0.2205
38	1.29%	0.5776	80	1.07%	0.3414	122	1.07%	0.2182
39	1.29%	0.5703	81	1.07%	0.3377	123	1.07%	0.2159
40	1.29%	0.563	82	1.07%	0.3342	124	1.07%	0.2136
41	1.29%	0.5559	83	1.07%	0.3306	125	1.07%	0.2113

Annex 17 - Example population map and population tables

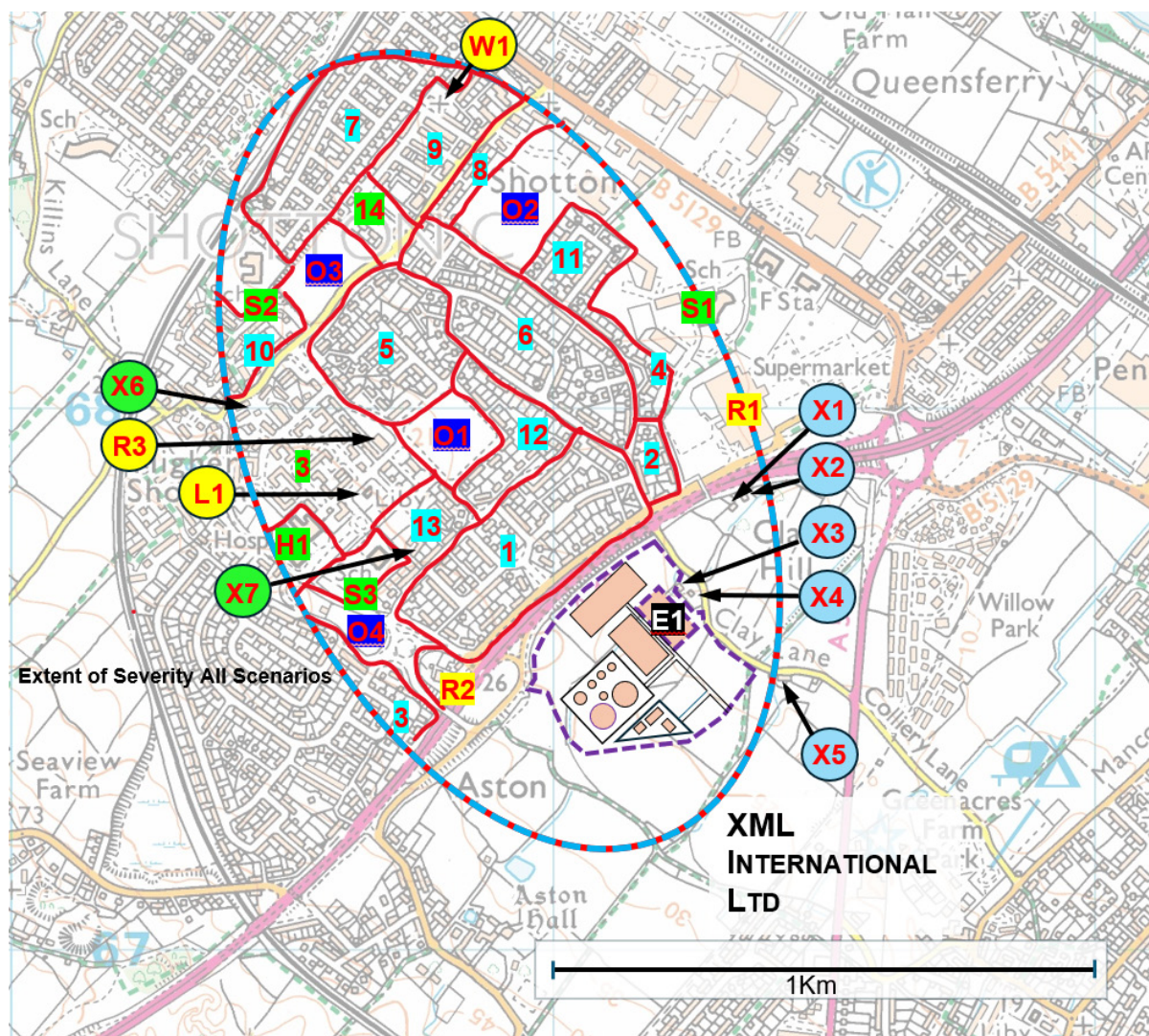


Figure A17 - 1: Example population map (XML International Ltd).

Example population map and tables

The population map example given in Figure A17-1 and the accompanying tables given in Figures A17- 2 to 4, illustrates the suggested level of resolution when determining off-site cumulative individual risk, and also off-site societal cumulative risk. It is based on an imaginary site 'XML International' but in the context of an actual population present in 2024. Like many established sites it has an 'enclave', this is where a portion of the land inside the site boundary is controlled by another company. As the population in an enclave is not under control of the site, its population are viewed as members of the public.

The limit of the area of interest should be based on an envelope which contains the hazard ranges of the MAHS identified. It is normally apparent which MAHS will set the limits, using a slightly larger circle or simple ellipse is useful if the hazard range is found to increase after the initial analysis.

The example has most of the development types that will be encountered in the UK. There are no high-rise multi-storey buildings present, as these are seldom encountered within the hazard range of COMAH sites, as their development largely occurred after Land Use Planning legislation was

introduced. Where high-rise buildings are encountered, simple fixed reference point dispersion models for toxic materials, or simple blast models, may not be sufficient to assess severity. Long established development can appear confused and complex, but this is the situation around many long-established sites; with land use developing over many years, and Hazardous Substance Consent being deemed later.

In the above diagram the blocks of housing, numbers (1) to (13), are phases of development, or intuitive areas containing similar housing types. These will typically be: detached, semi-detached, terraced; single storey or two storey. In some cases, the types of occupancy encountered suggests the intuitive area, such as the development of sheltered housing (3), where it is known the population will be sensitive or vulnerable. The table should give the assumptions regarding the population per dwelling. For individual dwellings, an assumption of 2.5 people per household can be made, it is assumed that these represent the normal population distribution, and they are present 24 hours a day (other basic assumptions could be used as long as they are properly justified). The housing density should be determined for each area of housing. Normally, this is a straightforward process using Google Earth or similar, perhaps corroborated by a walk-around. The resulting map and developed tables should allow the population within the particular MAHS hazard isopleth to be calculated at a later stage.

For other types of discrete development such as schools, retail, and care homes; the occupancy pattern should be obtained directly from the Operators if possible, from publicly available records, or from other data sources such as the commercially available National Population Database tool (NPD). Many of the commercially available tools will identify a wide range of development types and give the actual population, or number of dwellings. Where the population changes with time, particularly for a dual-use building, direct contact or public records will still be required.

The building type can be determined by visual inspection of images from Google Earth; this is particularly important when a building is on the cusp of a hazard criteria threshold. Taking the example of a building just outside the overpressure limit of total collapse; if it was a brick terraced house it may be deemed to collapse, but if it was a portal steel frame building with block infill it could be deemed to sustain damage but not collapse. The degree of resolution should be in proportion to the severity of the MAHS (see **Annex 2, Consideration of MAHS proportionality**).

It may be useful to add data columns for general information that will be used in the MAHS assessment later, such as the air changes per hour (ACPH) for toxic gas assessments. This makes it clear what values have been used where. Values are available in the literature and could be derived from standards such as 'BS5925 Code of Practice for Ventilation Principles and Designing for Natural Ventilation'.

The tables given in **Figures A17- 2 to 4** below, show the output from the population map.

Development Category and block ref no	Area	Number people per dwelling/ housing density	Population Group	Occupancy	Building Type	Assessment Specific	
						Toxic air changes per hour	Blast limit of partial collapse/ limit oif total collapse
Housing							
1	Terrig St Aston Rd (Clwyd St)	2.5 pe/dwelling 5.0 dwellings/ha	Normal	24hours	Mix of brick built Semi-detached, and four in a block, two storey houses		
2	Dee View (Chevrans Rd)	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
3	(Holly Grove) Coutland Dr	2.5 2.3 dwellings/ha	Sensitive & Vulnerable	24hours	Single storey brick blocks of two and 4 dwellings		
4	North Street	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
5	Grosvenor Rd Farmfield Cl Tudor Cl	2.5 2.2 dwellings/ha	Normal	24hours	Detached brick built single storey bungalows		
6	Green Lane (North St)	2.5 5.1 dwellings/ha	Normal	24hours	Mix of brick built Semi-detached, and four in a block, two storey houses		
7	Chester Cl Caenarvon Cl	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
8	Shotton Ln	2.5 5.6 dwellings/ha	Normal	24hours	Terraced, and semi- detached two storey brick built dwellings		
9	Strickland St Wellington St (Shotton Ln)	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
10	Greenbank Rd	2.5 3.1 dwellings/ha	Normal	24hours	Detached two storey brick buit dwellings		
11	Westminster Cres	2.5 5.0 dwellings/ha	Normal	24hours	Mix of brick built Semi-detached, and four in a block, two storey houses		
12	Cornwall Rd	2.5 5.3 dwellings/ha	Normal	24hours	Mix of brick built Semi-detached, and four in a block , two storey houses		
13	Clwyd St	2.5 3.1 dwellings/ha	Normal	24hours	Brick built two storey Semi-detached		
14	Hafan Glyd	2.5 4.4dwellings/ha	Sensitive & Vulnerable	24hours	Single storey brick blocks of two and 4 dwellings		

Figure A17-2: Example population table (XML International Ltd) – Part 1.

Development Category and block ref no	Area	Number people per dwelling/ housing density	Population Group	Occupancy	Building Type	Assessment Specific	
						Toxic air changes per hour	Blast limit of partial collapse/ limit oif total collapse
Discreate Housing							
X1	Daisey Bank Farm	2.5	Normal	24hours	Brick built detached dwelling		
X2	1 Clay Hill lane	2.5	Normal	24hours	Brick built detached dwelling		
X3	2 Clay Hill Lane	2.5	Normal	24hours	Brick built detached dwelling		
X4	3 Clay Hill Lane	2.5	Normal	24hours	Brick built detached dwelling		
X5	4 Clay Hill Lane	2.5	Normal	24hours	Brick built detached dwelling		
X6	Hollybank Residential Care Home	17	Sensitive & Vulnerable	24hours	Brick built two storey with added wings		
X7	Green Croft Care Home	28	Sensitive & vulnerable	24hours	Three storey brick		
Hospital							
H1	Deeside Community Hospital	150day 50 night	Sensitive & vulnerable	day 08:00 to 17:00 night 17:00 to 08:00	Brick/steel Frame		
Leisure (indoor)							
L1	Library	34	Normal	day 08:00 to 16:30	Steel frame, block infill		

Figure A17-3: Example population table (XML International Ltd) – Part 2.

Development Category and block ref no	Area	Number people per dwelling/ housing density	Population Group	Occupancy	Building Type	Assessment Specific	
						Toxic air changes per hour	Blast limit of partial collapse/ limit oif total collapse
Outdoor Leisure							
O1	Higher Shotton Sports Field	20 (50)	Normal	08:00 to 21:00	Open field		
O2	Higher Shotton Sports & Community Centre	25 day	Normal	08:00 to 21:00	Open field		
O3	Higher Shotton 33 Club Recreation Ground	30 day	Normal	08:00 to 21:00	Open field		
O4	Aston Bowls Club	20 day	Normal	12:00 to 22:00	Open field		
School							
S1	Queensferry CP School	149 pupils day 10 staff	Sensitive	08:00 to 16:30	Steel frame concrete		
S2	Venerable Edward Morgan Catholic School	229 pupils day 17 staff	Sensitive	08:00 to 16:30	Brick single storey		
S3	St Ethelwolds Church Primary School	120 pupils day 12 staff (23 wed evenings)	Sensitive	08:00 to 16:30 Used for adult literacy wed 19:00 to 22:00	Prefabricated concrete pannels		
Retail							
R1	Asda Superstore	150 staff and shoppers	Normal	06:00 to 22:00	Aluzinc clad portal steel framed building, glass fronted		
R2	Plough Inn	80	Normal	11:00 to 23:00	Two storey brick		
R3	Melrose Inn	75	Normal	11:00 to 24:00	Two storey brick		
Place of Worship							
W1	Biserica Creștină Penticostala Râul Vieții	50	Normal	see further detail	Traditional brick		
Site Enclave							
E1	COB Industrial Gases Ltd	5 staff	Working age	07:00 to 16:30 Tue - Sat	Portakabin single storey		

Figure A17-4: Example population table (XML International Ltd) – Part 3.

Annex 18 - Human error identification/probability references

Human error is very specific to the particular task being performed, how that task is performed, and the experience of the person it is being performed by. The identification of safety critical tasks and human error usually comes from bottom-up assessment, such as Hazard and Operability Study. However, where a plant has a high hazard potential (identified from top-down analysis) and has a high degree of manual operation, using Hierarchical Task Analysis to identify safety critical operations is strongly suggested.

There are many tools to determine Human Error Probability (HEP); most of these have been derived from THERP and HEART. THERP was the earlier technique primarily developed from the expansion of the nuclear industry in the 1980s, the seminal work being NUREG/CR-1278 by A.D Swain. HEART, developed by JC Williams is more general. B. Kirwan follows on and develops these techniques further, noting his involvement in the analysis of the 'Three Mile Island' near nuclear meltdown at a nuclear reactor in Pennsylvania; which was largely caused by human error and a fault intolerant design. Given the different circumstances in which human error occurs, it is not possible to point to one single guide. Here, a range of references are given, which should allow the Operator to determine if they have the necessary knowledge to derive their own HEP, or allow them to be an informed customer.

Human Task Analysis (HTA)

B. Kirwan and L.K. Ainsworth.(1992)(1993) 'A Guide to [Human] Task Analysis'; Taylor and Francis.

Human Reliability Assessment

B. Kirwan. (1994) 'A Guide to Practical Human Reliability Assessment'; Taylor and Francis.

Technique for Human Error-rate Prediction (THERP)

Swain, A.D., & Guttman, H.E. (1983). 'Handbook of human reliability analysis with emphasis on nuclear power plant applications'. Final report. NUREG/CR-1278. Washington, DC: US Nuclear Regulatory Commission [Sandia National Labs., Albuquerque, NM (USA)].

The Human Error Assessment and Reduction Technique (HEART)

Williams, J.C. (1985) 'HEART- A proposed method for achieving high reliability in process operation by means of human factors engineering technology'. In Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society (Vol. 16), pp.5/1-5/15.

Also recommended

B. Kirwan; (1996) 'The validation of three human reliability quantification techniques – THERP, HEART, JHEDI: part I -technique descriptions and validation issues', Appl. Ergon

B. Kirwan; (1997) 'The validation of three human reliability quantification techniques – THERP, HEART, JHEDI: part II-Results of validation exercise'.

Further reading

HSE (2009) 'Review of human reliability assessment methods', RR679, HSL, HSE Books.

Abbreviations Used

Abbreviation	Description
AIChE	American Institute of Chemical Engineers
ACOP	Approved code of practice
ACPH	Air changes per hour
ALARP	As low as reasonably practicable
API	American Petroleum Institute
ASO	Acid soluble oils
BPCS	Basic Process Control System
BOS	Basis of Safety
BLEVE	Boiling liquid expanding vapour explosion
BS	British Standard
CA	Competent Authority
CAS	Chemical Abstracts Service
CBA	Cost-benefit analysis
CCF	Common cause failures
CCPS	Centre for Chemical Process Safety
CCR	Continuous Catalytic Reformer
CDOIF	Chemical and Downstream Oil Industries Forum
CIA	Chemical Industries Association
CM	Conditional modifiers
CMF	Common mode failures
COMAH	Control of Major Accident Hazards Regulations 2015
DCS	Distributed Control System
DTL	Dangerous toxic load
EA	Environment Agency
ECHA	European Chemical Agency
EN	European Standard
EFD	Engineering flow diagram
ESD	Emergency shutdown system
EV	Expectation value
FMECA	Failure mode, effects and criticality analysis
HAZID	Hazard identification
HAZOP	Hazard and Operability Study
HEART	Human Error Assessment and Reduction Technique
HEP	Human error probabilities

Abbreviation	Description
HF	Hydrogen fluoride
HIPS	High integrity protection system
HSE	Health and Safety Executive
HSWA	Health and Safety at Work etc Act 1974
HTHP	High temperature high pressure
HTHA	High temperature hydrogen attack
HTA	Human Task Analysis
IChemE	Institution of Chemical Engineers
IPL	Independent protection layers
IROD	Individual Risk of Death
LFL	Lower flammable limit
LNG	Liquefied natural gas
LOC	Loss of Containment
LOPA	Layer Of Protection Analysis
MAHS	Major accident hazard scenario (or scenarios)
MAPP	Major accident prevention policy
MATTE	Major accidents to the environment
MAWP	Maximum allowable working pressure
MHHHRA	Major Hazard Human Harm Risk Assessment
MHSWR	The Management of Health and Safety at Work Regulations 1999
MSTR	Maximum safe temperature of reaction
MTSR	Maximum temperature of synthesis reaction
MTBF	Mean time between failure
MTTR	Mean time to repair
NaTech	Natural hazards triggering technological events
NFPA	National Fire Protection Association
NPV	Net present value
NRW	Natural Resources Wales
ONR	Office for Nuclear Regulation
ONS	Office for National Statistics
OPP	Off-shore production platform
P&ID	Piping and Instrumentation Diagram
PFD	Process Flow Diagram
PFD	Probability of failure on demand
PHA	Process Hazard Analysis
PHR	Process Hazard Review

Abbreviation	Description
PLC	Programmable logic controller
PLL	Potential loss of life
QHRA	Quantitative Human Reliability Assessment
QRA	Quantitative Risk Assessment
RGP	Relevant good practice
RAM	Risk assessment matrices
ROD	Risk of death
ROSOV	Remotely operated shut-off valves
R2P2	Reducing risks, protecting people (HSE publication now withdrawn, see references list)
RTC	Risk tolerance criteria
SA	Sensitivity analysis
SOE	Safe Operating Envelope
SEPA	Scottish Environment Protection Agency
SIL	Safety Integrity Level
SFAIRP	So Far As Is Reasonably Practicable
SLOD	Significant likelihood of death
SLOT	Specified level of toxicity
SMS	Safety management system
SRAM	Safety report assessment manual
TDU	Thermal dose unit
THERP	Technique for Human Error-Rate Prediction
TOR	Tolerability of risk
UEL	Upper Explosive Limit
VCE	Vapour cloud explosion
VLE	Vapour liquid equilibrium

Reference List

1. Chemical and Downstream Industries Forum (CDOIF), (2016) 'Environmental Risk Tolerability for COMAH Establishments – Guideline', V2.0. CDOIF.
2. CDOIF, (2024) 'Guideline – Adapting to climate change', V1.0. CDOIF.
3. Liquid Gas UK, 'LPG Industry Codes of Practice'. Liquid Gas UK.
4. COMAH, (2015) 'The Control of Major Accident Hazards Regulations 2015, Guidance on Regulations L111', 3rd edition. HSE Books.
5. HSE, (2015) 'Safety Report Assessment Manual (SRAM)'. HSE.
6. CIA, (2020) 'Guidance for the location and design of occupied buildings on chemical manufacturing and similar major hazard sites', 4th edition. Chemical Industries Association (CIA).
7. HSE, (2013) 'SPC/Tech/OSD/30 - Indicative human vulnerability to the hazardous agents present offshore for application in risk assessment of major accidents'. HSE.
8. HSE, (2013) 'Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment'. HSE.
9. IOGP, (2022) 'Risk Assessment Data Directory - Storage incident frequencies, International Association of Oil & Gas Producers (IOGP) Report 434-03'. IOGP
10. HSE, 'Failure Rate and Event Data for use within Risk Assessments'. HSE
11. HSE, (2001) 'Reducing risks, protecting people'. HSE. (Withdrawn by HSE 2025) available at <https://webarchive.nationalarchives.gov.uk/ukgwa/20230703113731/https://www.hse.gov.uk/enforce/expert/r2p2.htm>
12. HSE (1989), 'Risk criteria for land use planning in the vicinity of major industrial hazards'. HSE.
13. COMAH competent authority (CA), 'All measures necessary - Environmental aspects guidance'. COMAH competent authority (CA).
14. HSE, 'Costs to Britain of workplace fatalities and self-reported injuries and ill health 2023 to 2024'. HSE.
15. HM Treasury, (2026). 'The Green Book'. HM Treasury.
16. HSE, (2013) 'Managing for health and safety (HSG 65)'. HSE.
17. Barton, J. and Rodgers, R. (2004) 'Chemical Reaction Hazards – A Guide', 2nd edition. IChemE.
18. Steinbach, J. (1999) 'Safety Assessment for Chemical Processes'. Wiley-VCH.
19. Lewis, R. (2021) 'Sax's Dangerous Properties of Industrial Materials', 12th edition, Volumes 1-5. Wiley.
20. Bretherick, L. (2017) 'Bretherick's Handbook of Reactive Chemical Hazards', 8th edition. Elsevier Ltd.
21. 'Kirk-Othmer Encyclopedia of Chemical Technology' (2007), 5th edition, Index and Volumes 1-26. Wiley.
22. Etchells, J. and Wilday, J., HSE (1998) 'The workbook for chemical reactor relief sizing'. HMSO.
23. HSE, (2000 rep 2008) 'Designing and operating safe chemical reaction processes'. HSE Books.
24. 'API RP 571: Damage Mechanisms Affecting Fixed Equipment in the Refining Industry', 3rd edition, American Petroleum Institute (2020).

-
25. API Recommended Practice 941 (2016), 'Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants'; 8th edition, American Petroleum Institute.
 26. HSE, (1988) 'The tolerability of risk from nuclear power stations'. HMSO

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industries Forum Process Safety work stream.

CDOIF wishes to record its appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Helen Conlin	IChemE
Edmund Cowpe	Health and Safety Executive
Peter Davidson (Chair)	Tank Storage Association
Kris Ellenthorpe	Process Safety Consulting
Richard Heaton	Health and Safety Executive
Richard Hodges	SABIC
Julian Hought	Chemical Industries Association
Leighanne Moir	Scottish Environment Protection Agency
Jim Neilson	Health and Safety Executive
Carolyn Nicholls	RAS
Andrew Nixon	Environment Agency
Carl Owen	AstraZeneca

CDOIF would also like to extend a special thanks to all those who are not named above but contributed to the writing and development of this guide.

Revision History

Issue /rev	Section	Description	Date	Changed by /Issued by
1.0	All	Final Document First Issue	28 th Sept 26	Issued PD-