

HID - SAFETY REPORT ASSESSMENT GUIDE:

Whisky Maturation Warehouses

14 August 2001

Contents List

1 Introduction

- 1.1 Fundamental Considerations**
- 1.2 Role of the Assessor**
- 1.3 Consistency and Proportionality**
- 1.4 Proportionality and Depth of Risk Assessment**
- 1.5 Input to the decision on whether the Risks ALARP?**
- 1.6 How the Predictive Criteria Should be Used**

Criterion 3.1

Criterion 3.1.1

Criterion 3.1.2

Criterion 3.2

Criterion 3.3

Criterion 3.3.1

Criterion 3.3.2

Criterion 3.4

Criterion 3.4.1

Criterion 3.4.2

Criterion 3.4.3

Criterion 3.4.4

Criterion 3.4.5

Criterion 3.5

Criterion 3.5.1

Criterion 3.5.2

Criterion 3.5.3

Criterion 3.5.4

Criterion 3.5.5

Criterion 3.5.6

Criterion 3.6

List of Tables

<u>Table 1</u>	Source of data for Off-site Accident Initiators
<u>Table 2</u>	Whisky Maturation Warehouse Major Accident Scenarios
<u>Table 3</u>	Accident Initiators Requiring Consideration in a Safety Report
<u>Table 4</u>	Typical Failure Frequencies
<u>Table 5</u>	Effect of Input Parameters on Predicted Accident Consequences
<u>Table 6</u>	Typical Uncertainties in Consequence Modelling

1. Introduction

The purpose of this document is to describe how the Competent Authority's Assessors test whether COMAH safety reports meet the criteria that apply to the predictive aspects of COMAH. It provides background information on hazards from whisky maturation warehouses, and an interpretation of the criteria based on useful examples. The information supplements rather than supplants that in the safety report assessment manual.

It is assumed that the Assessor is fully familiar with:-

- HSC/E's enforcement policy, the application of the ALARP principle and associated publications (eg HSE, 1999; HSE 1992; Treasury, 1998).
- The COMAH Training Manual.
- The contents of the HID Safety Report Assessment Manual (SRAM), particularly the guiding principles, and the procedures for handling and assessing safety reports.

The sections below provide important background information, particularly on ALARP decisions and the application of the proportionality principle to the assessment of safety reports. Section 1.2 provides guidance to supplement the explanatory text for the predictive criteria in Part 2, Chapter 3 of the SRAM and should be applied for each safety report assessment.

1.1 Fundamental Considerations

Before assessing a safety report an Assessor needs to be clear about:-

- His/her role in the assessment process and what the safety report Assessment Manager (AM) is expecting from the assessment.
- The degree of proportionality that applies, this determines what can justifiably be expected from the Operator's risk assessment (RA) - ie the depth of the arguments supporting the various demonstrations.
- HSE's approach to the application of the ALARP principle to **on-site** (ie HSW Act Section 2), and **off-site** (ie Section 3) risks for new and existing establishments.
- How the assessment criteria should be applied and factors which influence the depth of the assessment process; an important consideration is the type of report being assessed eg first submission, or an update report.

These issues are outlined in the remainder of this Introduction and are revisited as appropriate in later sections of the guidance.

1.2 Role of the Assessor

The predictive assessment is pivotal to the demonstrations required under Section 4, Part 1, paragraph 2 of the COMAH Regulations; particularly the need to demonstrate that:-

- all major accident hazards (MAHs) have been identified;

- that all necessary measures to prevent and limit the consequences of these MAHs are identified and implemented.

The Assessor's role relates solely to the risks to people both on-site and off-site. Risks to the environment are for the Environment Agencies and are not addressed here.

When the assessment of the predictive aspects of a safety report is complete, the Assessor should return the completed assessment form to the Assessment Manager giving conclusions about whether:-

- the process of the hazard identification and risk analysis is fit for purpose;
- all MAHs have been identified; any gaps must be recorded on the AF;
- the consequence assessment is adequate for the purposes of COMAH ie the extent **and** severity of representative MAs must be quantified (Schedule 4, Part 2, Paragraph 4).

The assessment form allows Assessors to comment against each criterion and subcriterion. This guidance is designed to help provide consistent comments and conclusions and is structured in terms of questions which relate to the criteria and help to identify any weaknesses in the safety report. These should help Assessors to write succinct 'deficiency' statements and make clear what is required eg further information or analysis or both.

When filling in the assessment form the paragraph number and page number in the report should be shown for cross referencing purposes. For example:-

Criterion	Safety Report Refs	Comments	Issue* Category
3.3 The safety report should identify all potential major accidents and define a representative and sufficient set for risk analysis	pxx para yy	The safety report does not identify catastrophic vessel failure leading to total loss of contents as a potential MA. The report fails to meet criterion 3.3; the Operator has to provide more information.	Decided by team at final meeting

* The Issue Category relates to the inspection plan only.

The assessor must also provide input to the assessment team conclusions on whether the prevention and mitigation measures make risks ALARP.

1.3 Consistency and Proportionality

The assessment approach needs to be proportionate and consistent (HSC 1995; HSE 1999), therefore Assessors should come to a view on proportionality before starting to assess a report against the predictive criteria.

Consistency does not mean uniformity. It means taking a similar approach in similar circumstances to achieve similar ends. For some, professional judgement may need to be exercised in order to come to a decision on whether the demonstrations in the report are fit for purpose when assessed against the predictive criteria. The criteria and the associated

guidance are designed to help Assessors exercise this judgement in a consistent way. Occasionally they may need to discuss some issues with HID colleagues who are familiar with the site, the land use planning situation, or the Operator's approach to discharging his Section 3 responsibilities, before reaching a decision.

The assessment team have a key role to play in achieving consistency in the overall assessment of safety reports and in the drawing of the Competent Authorities (CAs) conclusions. Other ways of achieving consistency include;

- exemplar reports
- Lead unit system
- Sharing experiences through knowledge management systems.

Proportionality is a fundamental consideration when exercising judgement on whether assessment criteria are met or not. HSE guidance (HSE 1999b) on the COMAH Regulations (paragraph 74) states that 'there must be some proportionality between the risk and the measures taken to control the risk. The phrase "all measures necessary" will be interpreted to include this principle'.

Proportionality is essentially determined by the severity of the worst possible consequences, ie those resulting from the worst case scenario, and the levels of risk (individual and societal), that remain after taking account of the prevention and mitigation measures the Operator has put in place. The following factors (see also paragraph 292 of HSG 190), are therefore important:-

- (a) the scale (inventory, vessel sizes, etc) and nature (hazardous properties, toxicity, flammability, etc) of the hazards;
- (b) the location of the site in relation to off-site populations;
- (c) the density and types of off-site population (eg dwellings, hospitals, schools, etc);
- (d) the number of people on site;

- (e) the variation of residual individual risks with distance¹.

Proportionality should influence the aspects on which Assessors focus the most attention ie the issues where the occupier is expected to provide convincing arguments to support the demonstrations. Information in the safety report should enable Assessors to fully understand site specific circumstances (on-site and off-site), so that a view on proportionality can be reached. The report should therefore describe the processes, the hazardous substances involved and their effects on people, the distribution of people off-site, and the numbers of people on-site and their distribution in relation to the various installations.

To reach a view on proportionality the Assessor needs to know the potential maximum injury toll. Schedule 4, Part 2, Paragraph 4(b) requires the Operator to determine the extent and severity of the consequences of identified major accidents. Schedule 7 defines injury severity that constitutes a major accident. The threshold is a single death, six persons on the establishment hospitalised for at least 24 hours; or 1 person off-site hospitalised for at least 24 hrs. Severity therefore includes fatal and serious injury (ie hospitalisations) as a minimum. Operators must include the severity of the consequences for the worst case event in terms of expected numbers of fatalities and serious injuries in their accident consequence analysis. Less severe injuries should also be considered eg minor injuries.

1.4 Proportionality and Depth of Risk Assessment

Proportionality will influence the type and level of analysis detail that Assessors might expect to underpin the various demonstrations in the safety report (see paragraph 292 of HSG 190). HSG 190 gives the following RA definitions:-

- (a) **Qualitative risk assessment** is the comprehensive identification and description of hazards from a specified activity, to people or the environment. The assessment is informed by a representative selection of specific examples for comparison with standards and relevant good practice.
- (b) **Semi-quantitative risk assessment** is the systematic identification and analysis of hazards from a specified activity, and their representation by means of qualitative and quantitative descriptions of the frequency and extent of the consequences, to people or the environment. The range of possible events may be represented by broad categories, with classification of the likelihood and consequences for comparison and the identification of priorities.
- (c) **Quantitative risk assessment** is the application of methodology to produce a numerical representation of the frequency and extent of a specified level of exposure or harm, to specified people or the environment, from a specified activity . There is also a comparison of the results with specified risk criteria.

It is implicit in para 292 of HSG 190 that as proportionality increases from a low level to the highest level, the form of risk assessment is likely to change from qualitative, through semi-quantitative to quantitative risk assessment. It is important for Assessors to realise that QRA does not mean that a detailed and full numerical analysis resulting in iso-risk contours and F/N societal risk curves is needed. Rather the extent of the quantification and

1. Societal risks considerations are implicit in b) and d) above. Although the risks may be ALARP , they could be towards the top end of the band. Such a site would require more evidence and arguments to support the various demonstrations and deserve more inspection/assessment resource than a similar plant where the risks to people were towards the bottom end of the ALARP band.

the form it takes will depend on the site specific circumstances determining the level of proportionality that applies.

1.5 Input to the decision on whether the risks ALARP?

Criterion 3.6 addresses the “all necessary measures” demonstration, which is essentially an ALARP demonstration. In general, decisions on whether risks are ALARP for major hazard installations are based on the generalised Tolerability of Risk (TOR) Framework (HSE 1992, HSE 1999 - the latter being referred to as R2P2 below). For nuclear hazards there is considerable experience in making such ALARP decisions, but the mechanisms for other hazards are still evolving (see HSE 1999). Nevertheless some companies have adapted the TOR framework to devise their own major hazard risk criteria. Whatever approach is used, professional judgement is usually needed; the team approach to assessment should help achieve consistency in such decisions for top-tier COMAH sites.

The Operator’s ALARP demonstration should be founded on the degree to which good practice, engineering standards, recognised codes, guidance and standards, etc have been adopted. The control measures introduced by this process will be usually satisfactory for low hazard sites. In terms of the TOR framework this amounts to using **technology-based** criteria for making ALARP decisions, ie qualitative risk assessment. Such criteria will usually be sufficient when inherently safe design principles have been adopted because then the scale of the hazard should have been drastically reduced. As the level of proportionality increases, a decision has to be made as to whether further risk reduction measures are reasonably practicable as required by the HSW Act. Basically, two questions have to be answered:-

- what additional risk reduction measures are possible?
- which of these are reasonably practicable to implement, ie to make the risks to people (on-site and off-site), ALARP?

If no further measures can be identified, the Operator must have all necessary controls in place; it is then a matter to verify by inspection that this is the case and that the measures are sufficiently reliable. To answer the second question some quantification and CBA is usually required. The degree and rigour of this quantification will depend on the level of proportionality and the site specific circumstances. Such ALARP decisions usually involve the application of the generalised TOR framework as outlined in R2P2. The ALARP band is defined by levels of individual fatality risk. For members of the public the corresponding fatality risk levels are 10^{-4} (upper limit of tolerability) to 10^{-6} (broadly acceptable level) per year.

Societal risks should meet the criterion in R2P2 ie the likelihood of a single major industrial activity producing 50 or more fatalities should be less than 1 in 5000 per year ie less than 2×10^{-4} per year. This is essentially an **equity-based** criterion for societal risk. If the criterion is met for a single plant it is still necessary to judge whether the risks are ALARP for the site, which may have several plants.

To assess whether the societal risks are ALARP **utility-based** criteria are usually applied. These are based on the individual risk levels and a cost benefit analysis to estimate what further risk reduction is costing for each life saved by the introduction of an additional measure. By comparing this ‘value of preventing a fatality’ to the value society puts on each life (eg £1M) an indication of the level of disproportion is obtained. Judgement on whether this is gross will depend on the site specific circumstances, in particular the nature of the hazard and the likely value of the number of fatalities from the worst case scenario (WCF).

In the case of societal risks, deciding whether the risks are ALARP can be quite onerous, particularly for complex sites. One of the earliest examples, which underlines the complexity of making ALARP decisions, is the Canvey Island Studies, which are documented in two Reports (HSE 1978; HSE 1981). The Canvey studies considered the risks to members of the public from a number of major hazard sites operated by different companies and a proposed new refinery.

Individual risk (aggregated for all sites), was predicted at a number of locations together with the Societal risk arising from all operations. The first assessment showed that the risks were unacceptable and Industry accepted that risk reduction measures were needed, despite the fact that no agreement had been reached on risk criteria that were appropriate for major hazards. A second study (about two years later), which took account of the proposed measures and advances in risk assessment methods showed that the risks were lower by about a factor of 20. The highest individual risk of fatality was about 3.5×10^{-5} ie close to the limit of tolerability. However, HSE decided that no further risk reduction was necessary. HSE's decision attracted criticism, which is encapsulated in this extract from the report:- **“We have been criticised for seeming to adopt too high a level of acceptable risk in our conclusions. We concede that others may legitimately question our view of acceptable risk, but we would emphasise that in our opinion decisions about acceptable risks have to be made in the light of the facts of risk, consequences and costs in each individual case. We are not tied to a particular numerical level of acceptable risk, and inferences about what we have judged to be an acceptable risk in particular cases in the Canvey area should not automatically be applied elsewhere.”**

This extract from the second Canvey report underlines the site specific nature of ALARP decisions - a vital consistency consideration. An important point stemming from the Canvey studies and the 1992 TOR document is that when several sites contribute to the risk born by an off-site individual, the aggregated fatality risk must be ALARP and less than 10^{-4} per year. This has implications for multi-installation sites and multi-occupier sites, and for the assessment of safety reports at such sites. This issue is not addressed in R2P2. **Should this type of situation arise in the assessment of COMAH safety reports the team should consult HID OPGG on the way forward.**

In the case of new plant, precedents have been set to apply more stringent ALARP criteria (HSE 1992). This precedent recognises that most risk reduction opportunities exist at the design stage, eg through the application of inherent safety principles and the application of new technology.

1.6 How the Predictive Criteria Should be Used

The purpose of HSE's assessment of a safety report against the criteria in the SRAM, is to come to a conclusion on whether the requirements and demonstrations in Schedule 4, Part 1 have been met. The extent of the information required for each demonstration to be made will depend on the level of proportionality considerations and the type of safety report required by COMAH Regs 7 or 8. The different report types include: the initial report for existing establishments, pre-construction (PCSR), pre-operation (POSR), modification and updated reports.

Operators will write the safety report in a structure that suits them. Whatever structure is adopted, the Operator should ensure that the information is linked to the required demonstrations in a transparent way. The Assessor should bear in mind that the same control measures and arguments may apply to more than one demonstration. This means

that information to support a demonstration is likely to be found in different parts of a safety report.

The predictive criteria are designed to help you make consistent professional judgements about whether the demonstrations in a safety report are adequate. Such demonstrations need to be based on a suitable and sufficient risk assessment (EU 1998). The criteria are necessarily quite general, but sufficiently broad in nature to cover the various types of installation, the range of hazards to be encountered, and the types of risk assessment that might be employed. Therefore, not all the predictive criteria may need to be considered in the same detail by the Assessor, but **all the top level criteria need to be applied**. The issues identified in the assessment plan for close examination should help identify the predictive criteria that are key for a particular assessment. The extent to which the sub-criteria are applied should be proportionate. At the lowest level of proportionality a qualitative risk assessment based on recognised codes or guidance will suffice; no quantification of event probabilities may be needed so that the associated criteria need not be tested rigorously.

The criteria are provided as a guiding framework with in which professional judgements are made: *they are not provided as a tick list*. The assessment form should make clear that the Assessor has tested all the predictive criteria. **The effort put into the assessment should be proportionate and sufficient to enable valid conclusions to be drawn; the reasons behind these conclusions need to be transparent ie recorded for auditing purposes.**

Assessors should bear in mind that Operators may rely on published guidance or standards in seeking to demonstrate compliance. However, Operators who demonstrate compliance using company, or other non-published standards will have to show that they are fit for purpose, ie they need to be based on a risk assessment. They must also show that they have properly identified all foreseeable hazards and that they have implemented all necessary measures to prevent major accidents. **This means that the Operator has to demonstrate that HSW Act Section 2 (on-site) and Section 3 (off-site) risks are ALARP.** The report will therefore have to address any risks that remain after compliance with standards or guidance in order to demonstrate that all the necessary measures have been taken. For example, standards may only address risks to workers, in which case the Operator may (depending on the level of proportionality), need to justify their relevance to making off-site risks ALARP. It is then a matter of judgement whether the risks to people on and off site are ALARP. {Note that the Enforcement Policy Statement (HSE 1995), emphasises that neither codes or guidance material are in terms which necessarily fit every case}.

The SRAM provides guidance on how to assess the various types of safety report. As a general guide, the Assessor should take a quick overview to gain insight into the sites activities, environs, the scale and nature of the hazards, the range of MAs, the controls in place, and the maximum casualty potential (WCF). This will enable a view to be taken on proportionality and the most important issues. Then the assessment criteria can be used in detail to draw conclusions on the report.

The following points are central to the assessment process:-

- (a) Above all, an Assessor should ensure that he/she is clear about how the proportionality principle applies. The type of report will be an influence eg if it is an update report, or a modification report, the primary focus should be on the new material and how this affects the risk assessment.

- (b) The Assessor needs to take a view about whether the Operator's approach to risk assessment is proportional to the risks presented by the site. This should be done at an early stage in the whole assessment process because it is key to deciding whether a report contains grossly insufficient information eg when some quantification (eg of event likelihood), is needed and only qualitative arguments are used.
- (c) For existing CIMAH sites there may be outstanding risk assessment issues already raised with the occupier that are fundamental to the COMAH requirements. Assessors are advised to check whether there are outstanding issues and whether they have been addressed.
- (d) All the criteria must be applied in a proportionate and consistent way. For qualitative risk assessments the main focus is on the top level criteria.
- (e) All safety reports need to demonstrate that the risks to occupied buildings have been assessed, for example, in line with the CIA guidelines.
- (f) When the assessment has been completed the HID form should be filled in and the conclusions summarised for the Assessment Manager.

Criterion 3.1 “The safety report should clearly describe how the Operator uses risk assessment to help make decisions about the measures necessary to prevent major accidents and to mitigate their consequences.”

The purpose of this criterion is to help the Assessor determine if the Operator's approach to risk assessment is suitable and sufficient ie.(proportionate and systematic). Since this can only be properly assessed after the safety report has been read, it is probable that Assessors will need to return to this criterion at the end of the assessment process. To this end the following questions and answers may prove useful:-

Q: Has the Operator a policy on risk assessment?

This is an important point because the Operator must demonstrate a risk-based approach to his activities and to the production of the safety report. Failure to provide adequate evidence on this point may be viewed as a failure to comply with both the Management and the COMAH Regulations. The section of the safety report dealing with the major accident prevention policy (MAPP) will inform the Assessor on this issue.

Companies that manage their business with the aid of risk assessment might refer to the use of risk assessment in areas of safety management such as COSHH, commissioning (HAZOP) and cost benefit analysis. In these cases there may be reference to one or more formalised methods of determining risks such as event tree, fault tree and FMEA, and the use of risk assessment will probably not be confined to major accident analysis, but be detectable throughout the report. Assessors should not forget that risk does not necessarily involve quantification and that qualitative risk assessment has its place in the demonstration of safe operation.

Examples of non-quantified approaches that are acceptable include:-

- Hazard studies.
- Job safety analysis.

- Reference to industry standards.
- Safety reviews.
- Human error identification.

Q: Does the safety report summarise the methods of risk assessment or quantified risk assessment that are used in the report?

Since the regulations call for a risk assessment, the safety report should describe the approach adopted. If a QRA has been undertaken, the information that should be presented includes:-

- The extent of the analysis (plants/processes addressed).
- The method of identifying major accident event sequences (HAZOP).
- The analytical approach (event tree, fault tree, FMEA).
- The source of the base failure rate.

If a non-quantified approach is adopted because the risks are low, the basis for demonstrating that the residual risks are both tolerable and ALARP should be given. One or more of the following is acceptable if supported by well reasoned argument:-

- Industry standard good practise.
- Regulatory guidance.
- Industry association guidance.
- Historical data.

Q: Does the safety report summarise the criteria for use with the risk assessments or quantified risk assessments that are used in the report?

Operators should summarise the criteria used to judge when risks are tolerable. Ideally this should appear near the beginning of the report so that the Assessor can make the following judgements:-

- Are the criteria appropriate?
- Does the safety report demonstrate compliance with its own criteria?

Q: Does the safety report state the basis for judging whether all necessary measures have been taken to prevent major accidents and to limit their consequences?

The way Operators demonstrate that all necessary measures have been implemented is likely to depend on their approach to risk assessment. Most will not base their report on QRA and will be able to satisfy the requirements of the regulations by demonstrating compliance with good practice and adherence to standards and regulatory guidance. If a significant number of off-site casualties are predicted as a consequence of the worst accidents, other more quantitative approaches may be required.

For example:-

(a) Demonstrating that the risks are negligible (risk of death of an individual $< 10^{-6}$ /year).

or

(b) Demonstrating that risks are tolerable (risk of death of an individual $< 10^{-4}$ /year).

or

(c) Societal risks are shown to be tolerable or broadly acceptable.

Assessors should not expect to see detailed cost benefit calculations in a COMAH safety report, but Operators should list possible practical improvements and justify why they are not implemented.

Q: Has the Operator demonstrated a routine and general application of risk assessment in different aspects of operations, or has a limited amount of quantified analysis been carried out for the sole purpose of the safety report.

The safety report should convince the Assessor that the Operator understands risk assessment and routinely uses it to reduce risks at all levels and in all aspects of site operations. The complexity of such uses and level of detail given in the safety report should be proportionate to the risks involved.

The tone of the safety report and the way it is written will be a reliable indicator of the Operator's use and understanding of risk assessment. Assessors should look to the MAPP for evidence of a risk assessment culture rather than the accident analysis that may have been carried out by a consultant.

Criterion 3.1.1 "It should be clear that human factors have been taken into account in the risk analysis."

When making a judgement about compliance of the safety report with this criterion, Assessors should pose the following questions:-

Q: Has the Operator demonstrated that the risk assessment he has carried out to aid decision-making on the measures necessary to prevent major accidents and to mitigate their consequences includes allowance for human factors?

Risk assessment should not focus exclusively on random failures of hardware, but should also consider all types of operator error that can result in a major accident or a dangerous situation. The Operator should describe the role, operatives play in controlling hazard and show that their potential errors are identified. He should also describe measures that have been taken to reduce their probability and how they are accounted for in the major accident analysis. The safety report should demonstrate that his systems and procedures are fit for purpose and incorporate adequate attention to human factors. This may be described in the management section dealing with staff training, competence assessment, and the way incidents and near misses are dealt with.

Accounting for human error in risk assessment is not straightforward because some human reliability literature data are not universally applicable. Assessors should primarily be

concerned with checking that human reliability is included in the analysis rather than with the accuracy of the data used.

Q: Does the safety report consider an adequate range of human failings?

Inclusion of human factors in risk assessment does not necessarily mean simply accounting for process plant Operators opening the “wrong” valve or failing to control the process properly. Events such as, corner cutting, unauthorised absence, and even sabotage may warrant consideration. Errors at the design and construction stage of vessels used for storing distilled spirits should not be overlooked.

Examples of the types of event which may warrant consideration are:-

- Failure to successfully carry out an operation that is part of normal duties.
- Bulk tank filling and discharging errors made by the tanker driver.
- Erroneously carrying out an operation that is not part of normal duties.
- Failure to respond correctly to an alarm situation (failure to control or making a situation worse).
- Deliberate or inadvertent degradation of the safety of a plant (eg switch an alarm off, or bypass a safety system),
- Deliberate rule flouting (eg smoking in a non-smoking area).
- Failure to detect failed components during testing.
- Introduction of failures by damaging equipment or leaving equipment mis-aligned during testing or maintenance.

In practice many safety reports will not address human factors as thoroughly or with as much rigour as engineering issues. This can be understood in the light of traditional approaches to safety and safety reports, but cannot be justified where human reliability plays a critical role.

The following are examples of common omissions in safety reports:-

The potential for an Operator to override designed safety features has not been covered.

There should be some mention of ‘violations’ or ‘breaking the rules’ as well as ‘human error’.

The hazard analysis process failed to identify anything more than errors of omission (the Operator failing to act).

Most safety reports need to consider errors of commission (an Operator making an action but the wrong one), or decision making errors.

The role of people other than as front-line Operators (eg maintainers, supervisors) is not considered.

Many human failures are the result of actions, omissions and decisions taken by other people including designers and managers. For example, the potential for a maintenance error on a safety related system may not be addressed in the RA process.

There was no consideration of the possibility of a hardware failure with a simultaneous human error.

Some appreciation that when the hardware of a protective system fails the Operator may also not respond in the intended manner.

The Operator is being asked to do a critical task that would probably be more reliably done automatically.

There appears to be undue reliance on an Operator to identify and respond rapidly to an alarm condition.

If so, we would need some justification of the human error probability included. This should be justified in relation to the specific design of the system interface they have on site rather than a generic value taken from a table.

There is reliance on 'heroic' acts by Operatives to recover situations eg going back to the control room when suffering from effects of toxic gas.

Q: Does the safety report show how human factors are included in the risk assessment?

Data tells us that human failures contribute up to 80% of industrial accidents. Even in oil refineries, which are highly capitalised and automated, the figure is 50%. The implications of this run throughout the safety report and through many of the assessment criteria, so they will need to be considered by several members or all of the assessment team.

The safety report should consider in a rigorous and proportionate way how Operators may contribute to the initiation of a major accident (see Criterion 3.4.4). It should also describe the part Operators play in controlling hazards and risks. If an Operative is required to take certain actions following an alarm, the risk analysis will need to make assumptions about the likelihood that the correct action is taken. For example, if the economic consequences of emergency shutdown are great, the Operator may very well hesitate or fail completely to press the button.

If a task is critical to the prevention of a major hazard and an unrealistically high level of human reliability has to be assumed to make the risks ALARP, this may not be acceptable as it places an undue burden on the Operator. Instead automatic control and protection systems can be used to reduce the reliance on the Operator to intervene correctly. To achieve the required reliability it may be necessary to build redundancy and diversity into the control systems.

Not all safety reports will need to quantify human reliability. The focus should be on demonstrating the quality of the training and supervision. If a human reliability figure is used in a fault tree, the Assessor should check that the top event is not sensitive to the value adopted.

At whisky maturation sites, Operator error may occur during the following operations:-

- Road tanker loading/unloading

- Maintenance of bulk storage facilities
- Warehousing
- Blending
- Cask filling

Q: Does the safety report describe how the probability of Operator error is reduced?

In the context of Operator error and how the company ensures that it is minimised, the safety report should:-

- Describe how Operator errors are identified.
- What measures have been taken to reduce their probability.
- How they are accounted for in the major accident analysis.
- Demonstrate that the systems and procedures for selection, training and supervision of Operators are fit for purpose.

Criterion 3.1.2 “Any criteria for eliminating possible hazardous events from further consideration should be clearly justified.”

This criterion deals with the Operator’s limitation of accident analysis in the safety report and can be judged by reference to the following:-

Q: Have any major accidents been discounted on probability grounds?

Operators are obliged to demonstrate that low frequency events with severe consequences are adequately controlled - that all necessary measures have been taken to prevent their occurrence. However, most safety reports are unlikely to determine the consequences and frequency of very improbable accident initiators such as a meteor strike, simultaneous multiple failures of reliable systems, and terrorist activity. It is essential that the risk dominating accidents be dealt with comprehensively and that accidents such as cold catastrophic failure of storage vessels with bund over topping, guillotine rupture of large diameter pipe work should not be discounted.

Assessors should recognise that the COMAH regulations do not call for QRA. Frequency evaluation for highly improbable accidents does not need to be as detailed as that for risk dominating sequences and can be based on historical data, industry standards and regulatory guidance, etc.

Q: Does the safety report unjustifiably eliminate ‘small scale’ releases?

It is reasonable for the Operator to reduce the number of release cases by defining a scale of event that will not lead to a MA. For example, the consequence assessment may show that any failure resulting in a release smaller than that equivalent to a 10 mm diameter hole does not produce a hazard to on-site or off-site populations. This provides a basis for defining major accident hazards. However, Operators may need to take account of smaller flammable releases into confined spaces, which might ignite and explode and trigger a more severe accident. The Operator should also consider any known or foreseeable changes to the sensitivity of the surrounding environment, eg future dwellings which may be built nearer

to the site boundary as these can affect the appropriate degree of proportionality. Such changes should be also considered whenever the risk assessment is reviewed.

In situations where this 'protection' based approach is not sufficiently limiting, ie the hazard ranges from very small releases extend into population, a risk based approach may be needed. This requires the contribution to the residual risk of releases of different sizes to be considered so that a justifiable 'cut-off' can be decided. All contributions to release likelihood need to be taken into account otherwise, the 'cut-off' may be overly optimistic.

Q: Has the Operator grouped the consequences of several accidents together?

It is reasonable for Operators to describe in detail the consequences of only a relatively small number of representative accident sequences, provided all significant accidents are identified and ranked according to the risk they pose. If, for example, six different accidents resulted in a similar rate of release of a large quantity of whisky spirit, and gave rise to similar evaporating pools or pool fires of similar types, the consequences of only one of them need be described in the safety report. The relative likelihood of the others should be evaluated in order to demonstrate that the risks are ALARP. Operators have discretion on the way this is done and Assessors should not insist on a particular approach, but the arguments presented must be robust.

Q: Is adequate justification provided for dismissing major accidents on the grounds of low probability?

A safety report may describe the consequences of a representative set of accidents, provided account is taken of all major accidents. In particular it should describe the risk from all accidents that the Company has taken measures to prevent occurring. The frequency determinations do not necessarily have to involve the application of formalised methods such as fault tree analysis. Reference to appropriate source material/documents, industry standards etc. is likely to be the norm.

The safety report should also demonstrate that risks from accidents, for which no preventative measures are taken are tolerable. In general these will be low probability events initiated by an off-site event such as aircraft impact or an earthquake.

Incredible accidents are not clearly defined in this context, and Assessors are expected to use common sense and professional judgement about events that can be neglected. Examples include meteor strike, terrorist activity and simultaneous failure of several diverse and redundant safety systems.

Q: Has the Operator determined or ranked the frequency of all major accidents?

Assessors should recognise that the COMAH regulations do not call for a full QRA. Frequency evaluation for highly improbable accidents does not need to be as detailed as that for risk dominating sequences and can be based on historical data, industry standards and regulatory guidance, etc. However, the statement - 'the probability of this accident is judged to be less than 10^{-6} ' is not acceptable if they are not backed with supporting evidence. A poorly documented or sparsely detailed frequency analysis that appears somewhat optimistic may be judged as failing to comply with the assessment criteria.

Operators are obliged to demonstrate that low frequency events with severe consequences are adequately controlled, ie that all measures necessary have been taken to prevent their occurrence. If precautions have been taken to reduce the probability of an accident, then

the consequences of the event must be assessed so that they can be balanced against the precautions.

If the Operator has not attempted to quantify accident frequencies, but builds a case based on terms such as high, medium and low probability, he should rank the accidents according to their perceived severity. Without any quantification it is difficult to determine if an accident that kills a few people with “medium likelihood” is worse than one that kills many people with “very low likelihood”. In such cases, the Operator should determine that both risks are tolerable.

Criterion 3.2 “The safety report should demonstrate that the Operator has used information and data that are suitable and sufficient for risk analysis”.

A key requirement of the regulations is that information provided about the site and its hazardous substances is **suitable** and **sufficient** for a risk assessment. Table 1 provides some examples of where such information may be found. When considering this part of the safety report the assessor should ask if it provides answers to the following questions:-

Q: What is the maximum distilled spirit inventory and how and under what conditions is it stored?

The site description must describe the location and type of each storage system and provide information on the maximum inventories of all distilled spirit and the conditions (temperature and pressure) under which it is stored. It is important that the report adequately addresses the requirements of Schedule 1 of COMAH and considers all substances qualifying under the aggregation rules. The hazard from each qualifying substance must be assessed.

Q: Does the safety report give a description and explanation of site operations sufficient to enable all potential major accident scenarios to be identified?

The safety report should describe plant and plant operations so that failures and errors having severe consequences can be identified. The detail provided needs to be sufficient to enable Assessors to determine if the accident analysis is thorough and complete. In addition to a full description of the storage facility and any associated control and shutdown systems, the safety report should describe the associated equipment subject to the requirements of COMAH. This may include import and export lines, pressurising systems for vessels, failure modes of equipment such as transfer pumps, flow control valves, level control devices and venting systems.

Q: Are there sufficient maps and plans to allow the location of hazard sources and vulnerable populations/habitats to be identified?

The standard of maps and plans is likely to vary from one report to another, but all the information needed to determine risk should be present. Maps and plans should clearly show the location of all significant distilled spirit inventories and populated areas at risk from the installation. Particular attention should be given to elevated structures such as railway viaducts and high rise buildings that may be at risk from buoyant releases such as the smoke plume from a pool fires, or even the flames themselves when tilted by a strong wind.

Some accidents at the maturation warehouses have the potential to affect the natural environment, and in particular aquatic systems, SSSI's or SBI's that may lie some considerable distance from the site but are connected to it by a water course.

In addition to assessing the consequences of fire, the safety report should describe the potential effects of contaminated fire fighting water run-off. In this context the location of bulk storage tanks with respect to watercourses is particularly important.

Vapour cloud explosion hazards should not be discounted, particularly if the vapour from a spill can be confined by the nearby structures and plant. In addition to unexpected releases, inadequate purging prior to hot work which can result in an explosion with major accident consequences or the potential to initiate a major accident, may need to be addressed.

Q: Can the source terms for all accidents be determined from the information provided?

The information in a safety report must be sufficient to enable the Assessor to deduce the approximate source term for each major accident. In other words, sufficient information should be given to allow the Assessor to determine 'how much, for how long and from where?' Assessors should take the view that any containment system or item of plant can fail and release its contents, therefore the safety report should provide:-

- Information on the pressure and volume of vessels and other plant. This includes the diameter and length of pipe work between isolation valves, when the potential volume of liquid that can be released is capable of producing a major accident.
- A list of equipment such as pumps, import and export systems (including road tanker loading facilities), level devices, flow control systems, pressurising systems, containment sumps, bunds (including dimensions), together with the operating pressures and temperatures.
- Flow rates and inventory levels associated with the storage and import/export facilities.
- A description of the containment systems and shutdown systems to control material loss in the event of an unexpected release. Claims for such mitigatory systems should be carefully scrutinised and excessive optimism that results in a significant under prediction of major accident source terms should be considered as a serious omission when measured against the assessment criteria.

A safety report that fails to supply all of this information, is unlikely to comply with the assessment criteria.

Q: Are the assumptions used in the accident analysis adequately justified and clearly stated?

The assumptions referred to here do not relate to mathematical modelling of an accident, but are connected with the operation of a site. For example, if the Operator assumes that an alarm will be seen immediately, or that a hardware failure will be detected immediately, the control room must be permanently manned and the instruments that would detect the failure in question should have a status indicator. Even then, the possibility of a delay before remedial or emergency action is taken should be considered. Of particular concern are failures that would allow a large release of distilled spirit to go unnoticed.

Any reliability assumptions about the following should be justified:-

- ROSOVs to terminate a release.

- Operators to perform tasks correctly.
- Instruments to detect a dangerous situation.
- Shut down systems that respond on demand.

Q: If a QRA approach has been adopted, are accessible sources provided for base failure frequencies/probabilities?

Key documents that the safety report relies on should be available to the Assessor, ideally by being included as an annex to the main report. Fault tree analysis, for example, should not be based on failure probabilities given in a confidential report unless the company is prepared to provide HSE with a copy.

The minimum requirements in this respect is references to published work. An Operator's failure to provide any supporting evidence should be considered a failure to comply with the criteria.

Source documents are targets for the follow-up inspection to validate the report, but Assessors should bear in mind their right to request further information from an Operator to help them assess his safety report.

Q: Does the safety report provide, or reference accessible sources for, the predictive models adopted, including the underlying science?

The safety report should provide information on the methods and models used to predict the consequences of major accidents. If a well known computer program such as PHAST has been used, then only details of the input data and the version number are required. If an in-house computer program is used to calculate the consequences of accidents, then the physics on which the predictions are based should be described or reference made to a published article.

Q: Does the safety report describe meteorological conditions, which are appropriate for the site, and in sufficient detail?

A safety report should present wind rose data (wind speed, wind direction and atmospheric stability) for the site in order to establish the frequency and direction of adverse atmospheric conditions. This is particularly important for pool fire hazard.

Operators should demonstrate awareness of the changes in accident consequences with weather conditions by presenting results for different atmospheric stability and wind speed. They should recognise that the wind direction can vary over 360° and that D5 and F2 do not necessarily encompass the full range of consequences of an accident.

High-pressure releases of distilled spirits should be considered where appropriate because spray jets can form significant vapour clouds capable of giving rise to a flash fire followed by a spray jet fire. The orientation of jets is often an important factor. Releases from evaporating pools tend to be passive and treating them as dense may be conservative. The rate of dispersion varies with wind speed and category. D5 is usually the most appropriate weather condition for daytime accidents involving dispersion. The consequences of pool fires should be evaluated for a variety of wind speeds.

Q: Are the features/systems that may limit the consequences of accidents identified?

Operators should not reduce the frequency of an event or the severity of the consequences of an accident on the grounds of the presence of a safety system. For example, the Operator should not claim that a release will be terminated early by a shutdown system that may fail on demand. Nor should he discount an initiating event on the grounds that a permit-to-work system precludes the necessary conditions.

Ideally, the safety report should quantify the consequences of events with and without safety features operating so that their 'value' can be assessed and balanced against their reliability.

Q: Does the safety report contain all the chemical and physical properties needed to assess the risks from the site?

A safety report should present the entire chemical, physical, toxicological and eco-toxicological information that is needed to calculate risk to people and the environment. Toxicity data should also be provided for any toxic substances produced by combustion if appropriate.

Table 1 : Sources of data for Off-site Accident Initiators

Initiator	Method of Model
Aircraft impact	AEA methodology
Seismic event	British geological survey data
Lightning strike	Electricity council data and methodology, BS 6651: 1999
Severe environmental conditions:- Abnormal rainfall Abnormal snow fall Very low temperature High temperature Gale force winds	Historical data plus reasoned argument
Flooding	Site and met office data plus reasoned argument
Subsidence	Historical data plus reasoned argument
Land slip	Historical data plus reasoned argument
Fire or explosion at adjoining plant	Site environs information plus relevant data where relevant
Missile from off-site	Site environs information plus relevant data
Hazardous substance pipeline rupture	Site environs information plus relevant data
Collapse of high voltage cable	Site environs information plus relevant data
Impact by out of control road or rail vehicle	Site environs information plus relevant data
Other	

J.P. Byrne, “The calculation of aircraft risk in the UK”, prepared by AEA Technology plc for the Health and Safety Executive 1997. Contact Research Report 150/1997

The method of measuring the frequency of accidents caused by off-site events should be fit for purpose. In other words it should be proportionate to the level of risk. Thus, if a site is located far away from any airport or flight path (military or civil), then it is acceptable for the safety report to refer to the background crash rate for the UK. On the other hand, if the site is located close to a busy airport then a much more detailed assessment of aircraft impact should be carried out.

Criterion 3.3 “The safety report should identify all potential major accidents and define a representative and sufficient set for the purpose of risk assessment.”

This criterion reminds Assessors that they need to check that:-

- The safety report meets Schedule 4, Part 2, paragraph 4 of the regulations, which requires identification of all possible major accident scenarios.
- If the major accidents are put into groups, the representative accident sequences are suitable and sufficient for risk assessment purposes.

Ideally, the Operator should summarise, in a proportionate way, the results of hazard studies, the methods used and the expertise of the team involved. The scope of the studies and the HAZID process used should also be described. To provide a convincing demonstration that the list of MAs is complete, the process needs to be systematic, ie each

plant and its operational sequences should be considered in turn, including the possibility of interactions. Assessors should judge the completeness and adequacy of the way these issues are dealt with by asking the following questions:-

Q: Is the approach the Operator has adopted to identify all major accidents suitable and fit for purpose?

The report should explain how major accidents have been identified and demonstrate that no important scenarios have been overlooked. When the method of identifying accidents is not systematic or transparent it will be much more difficult to convince the assessor of its completeness. Simple lists of accidents without evidence to show they are comprehensive may be appropriate in some cases, depending of the scale of the risk to off-site populations, but generally Operators will need to demonstrate that no major accident has been overlooked. Assessors should take into account the scale of the hazards when making a decision on this issue (proportionality).

Q: The accidents considered should include those initiated by off-site events.

The accident analysis should identify all potential off-site initiators of major accidents and an indication of their likelihood (see Table 1). On-site accident initiators such as hose coupling failures, overfilling of bulk storage tanks, lifting or movement operations may require a more detailed frequency assessment in order to demonstrate the adequacy of installed safeguard systems.

Q: Have all possible sources of major accident hazard been identified?

Some incidents are characterised by an insignificant failure that, if not quickly attended to, escalates to an event of major proportion. Thus the accident identification process should not be restricted to vessel and pipeline failures, but should address all plant items on which failures have the potential to initiate a major accident. Ground inclination and common drainage systems that can convey a spill a considerable distance and /or result in running pool fires or drain fire/explosions should not be forgotten.

Q: Are the accidents addressed in the safety report representative of the full spectrum of major hazards presented by the installation?

There is no requirement to repeatedly describe the consequences of accidents that have a similar impact on employees, local populations and the environment. The safety report does not have to describe the consequences of all the major accident hazards, but just to identify them. Instead it may define a representative set of accidents that includes the most severe plant failures and consider all possible consequence (eg fireball, jet fire, flash fire, etc). In other words, the consequence analysis can be based on a reduced set of accidents that are representative of the hazards from the site.

Q: Does the 'representative sample' of major accidents include the risk dominating accidents?

The Assessor must be satisfied that the accidents considered dominate the risk and encompass the complete spectrum of severity. Table 2 identifies plant items that contain, or are connected to, large inventories of distilled spirit and lists the most obvious potential accidents or failure modes. While it may not be completely exhaustive for all installations, it can be used as a check list to assess the completeness of the accident analysis. If there are any unexplained omissions that would significantly change the predicted risks posed by the site, it may be deemed to fail to comply with the assessment criteria.

Q: Are the descriptions of accidents in the safety report sufficiently comprehensive to allow the adequacy of the methods for preventing major accidents and for limiting their consequences to people and the environment to be assessed?

The safety report should determine the consequences of essentially identical accidents in very similar plant if the consequences are likely to be different. For example, if a transfer pipe failure can release distilled spirit at say 20 kg/s in one area of the site while a hose rupture on a road tanker can result in a similar release in a different location. Both failures should be considered in the safety report because they may have different consequences. The safety report should also consider failures occurring at the 'worse locations' which may be on pipelines through a congested area where the possibility of a VCE can not be ruled out. A safety report that fails to address the 'worst case' consequences of representative accidents does not meet the assessment criteria.

Q: Have all the potential consequences of each of the reduced accident set been considered?

Failures of transfer systems can give rise to a variety of thermal radiation/explosion hazards that must be addressed in the safety report. For example, the consequences of failure of a large storage vessel that should be considered are poolfire, jet fire, flash fire and possibly a VCE. Some of these events are more probable than others, but those contributing little to the total risk should not be ignored.

The toxic effects of the combustion products arising from wooden casks must be included in the report. Large pools of alcohol can give rise to high concentrations some considerable distance away.

Q: Has the potential for escalation been properly addressed?

Some accidents at an installation can cause other failures in that they may have as severe or even more severe consequences. The safety report must recognise this possibility and address it by postulating accidents in 'worst case' locations. Of particular concern are:-

- Spray jet flames or pool fires that engulf or impinge on tanks, vessels and other plant.
- A VCE that can cause a variety of mechanical failures.
- Road tanker failures and fires that impinge on static plant or equipment.
- VCE or tank explosions that can generate blast over pressure and missiles.
- Other equipment that can generate missiles or impacts.

The site description should be detailed enough to enable the Assessor to identify the most hazardous locations for component failures and hence determine if the accidents considered are 'worst case'.

Types of Accident Suffered by Whisky Production and Maturation Warehouse Sites

Although Operators need to demonstrate the use of a systematic approach to accident identification, Assessors are likely to find that few safety reports present the results of formalised methods such as cause-consequence diagrams or failure modes and effects analysis. An alternative approach that some Operators may adopt involves listing each item

of plant and identifying all its failure modes that would give rise to a major accident hazard. Individual thermal radiation, or explosion hazards are then identified by reference to the following list:-

- Pool fire.
- Cask stack fire.
- Warehouse fire.
- Explosion in a warehouse.
- Fire engulfment of a road tanker, leading to:-
- BLEVE.
- Missile generation.

The accidents that distilled alcohol storage facilities can suffer fall into seven main categories:-

- Loss of containment due to a failure of one sort or another leading to a pool fire (contained or uncontained), tank fire, flash fire, internal or external explosion.
- Overfilling and subsequent ignition of excess fluid released by abnormal operation or failure protection systems (including human error).
- Pipe or pump failure resulting in a pressurised release, which may be contained or uncontained, obstructed or unobstructed. The potential consequences of such failures are pool fire, spray-jet fire, flash fire and explosion when a volatile liquid is released into buildings and congested areas.
- Import/export activity failures involving road tankers.
- Releases into water courses.
- The rapid escalation and domino effects of fire.

The different consequences of loss of containment accidents depend on the sequence of events leading to the fire, explosion or toxic cloud release. A fireball will only result from a massive and rapid release of alcohol vapour and immediate ignition of the release. BLEVE will only occur where flame impingement occurs on a storage vessel or road tanker. A tank fire typically occurs as a result of an internal ignition or burn back and subsequent roof failure, while a flash fire may follow a large release of vapour that disperses and then encounters a source of ignition. Releases into confined spaces with ignition sources may result in explosion.

The stabilised flow rate out of a pipeline is function of the pump characteristics associated with the transport activity. If the whisky is vaporising, the time sequence of the release should be used to determine the most appropriate dispersion analysis (quasi-instantaneous or continuous release). Delayed ignition of a vaporising release into a congested volume may result in an explosion that produces a dangerous side-on pressure

at some distance. Either calculations or reference to an authoritative source should be presented if the possibility of a VCE is discounted.

Criterion 3.3.1 “The safety report should demonstrate that a systematic process has been used to identify all foreseeable major accidents.”

In order to judge compliance with this requirement of the regulations, Assessors can ask the following questions:-

Q: Is it obvious that all major accident scenarios have been identified?

Identification of all major accident scenarios is a very important requirement of the regulations and a safety report that fails in this respect may be considered deficient. Systematic approaches to accident identification include HAZOP, event tree analysis and failure modes and effects analysis. However, the regulations do not specifically require their application. An Operator may be able to demonstrate that all major accidents have been identified without resort to formalised methods by providing a detailed description of the plant and by systematically addressing the hazards from each part in turn.

Q: Does the Operator provide evidence that all major accident hazards have been addressed.?

Operators that have not used a formalised structured method to identify major accidents should provide evidence that no sequence has been overlooked. For example if overfill is identified as a major accident scenario, there may be half a dozen ways in which this can occur as result of equipment failures and human error. The safety report should address each one and show that all necessary measures have been taken to prevent the accident occurring. If sequences are overlooked, the report must be deemed to fail to comply with the regulations, however, the depth of the accident analysis need only be proportionate to the scale and nature of the hazards and associated risks.

Criterion 3.3.2 “The hazard identification methods used should be appropriate for the scale and nature of the hazards.”

Hazard studies employing HAZID techniques are widely used in the chemical industry and can be carried out at various stages during the lifecycle of a plant. They are systematic way of managing hazard over time, from the business requirement stage through to demolition and disposal. HAZID techniques seek to identify hazards in an absolute or relative way. Relative methods use checklists or hazard indices based on experience and lessons from incidents. Absolute methods are based on deviations from design intent eg HAZOP. Details can be found in Lees (1996), Kletz (1999) and CCPS (1989).

Methods (listed in increasing proportionality) that might be used include:-

- Industry standard or bespoke checklists for hazard identification.
- Safety reviews and studies of the causes of past major accidents and incidents.
- FMEA (Failure Mode and Effect Analysis).
- HAZOP (Hazard and Operability Studies).
- Job safety analysis (eg Task Analysis).

- Human error identification methods.

Whatever approach is used, it must be documented as part of the safety report, or separately - in which case the main findings should be summarised in the report. As proportionality increases, and particularly in the case of new novel plant, some use of absolute methods is normally required. Both type of method need to consider 'common cause/mode' failures such as loss of power, or other services.

In order to test compliance with this criterion the Assessor can ask the following questions:-

Q: Does the safety report describe a hazard identification process that instils confidence in its completeness?

The safety report should describe and justify the method used to identify major accident hazards. Assessors who are not convinced that all accident scenarios have been identified may deem the report 'non compliant'. However, use of a formalised accident identification process is not essential and an approach that is not completely systematic, but is seen as 'fit for purpose' is acceptable.

Q: Is the depth and detail of the accident analysis commensurate with the scale of the hazard?

In the main, accidental releases of distilled spirit give rise to fires and possibly explosions, but the hazard ranges associated with them do not always extend off-site. The minimum level of detail in the risk assessment depends on the scale of the risks. In general, the safety report for a site near to a busy shopping centre will need to contain more information than one in an isolated location.

Table 2: Whisky Maruration Warehouse Major Accident Scenarios.

Plant Item Failure	Accident Scenarios				
Storage Tank	Cold catastrophic failure Pool fire Flash fire	Hot catastrophic failure BLEVE Fireball Explosion		Hole in vessel wall Spigot flow Pool fire Flash fire Tank fire Boil over	Flammable head space Internal explosion Missile formation
Transfer Pipework/ Road Tanker Loading and Unloading	Rupture Pool fire Flash fire VCE	Puncture Pool fire Flash fire VCE	Small hole Flash fire		
Maturation Warehouse	Leaking casks Pool fire Flash fire				

Casks/ Cask Storage Area	Flammable head space Internal explosion				
--------------------------	--	--	--	--	--

Criterion 3.4 “The safety report should contain estimates of the probability (qualitative or quantitative), of each major accident scenario or the conditions under which they occur, including a summary of the initiating events and event sequences (internal and external), which may play a role in triggering each scenario.”

Criterion 3.4 is about the completeness of the accident analysis and the quantification of probabilities. It focuses on initiators - have all of them been identified and whether the methods used to determine accident sequence probabilities are appropriate.

The depth of the analysis of the event sequences, which determine the likelihood of realising each major accident scenario needs to be proportionate. At the lowest level of proportionality - provided it is demonstrated that a plant is designed, built and operated to current standards - it will usually suffice for qualitative descriptors of likelihood to be assigned to each MA. For example, the CIA’s guidance on emergency planning for chlorine installations gives the following frequency categories:-

Extremely	<	10^{-6} /year
Very unlikely		10^{-6} to 10^{-5}
Unlikely		10^{-5} to 10^{-4}
Quite unlikely		10^{-4} to 10^{-3}
Somewhat unlikely		10^{-3} to 10^{-2}
Fairly probable		10^{-2} to 10^{-1}
Probable	>	10^{-1}

In more complex situations a satisfactory demonstration under Schedule 4 may require the consideration of the conditions, under which events occur, their likelihood, and how the events interact so that the likelihood of certain major accidents can be estimated. This will require consideration of the whole causation/outcome sequence.

In order for Assessors to form a judgement on these issues, they should ask the following questions:-

Q: Does the report quantify, albeit with limited accuracy or in qualitative terms, the frequency of each major accident scenario?

Assessors should expect to see all events producing a major accident hazard identified and the frequency of each event sequence determined. There is a requirement to demonstrate that the risk from risk dominating sequences is ALARP. The greater the risk to people off-site, the more reliable must be the quantification.

For single event initiators such as aircraft impact and earthquake, probabilities based on historical data are acceptable. But it may not be sufficient for the Operator to use data from published sources for event sequences involving say component failure and Operator error, without justifying their suitability. The safety report should justify the absence of further redundancy and diversity and show that all necessary measures have been taken to minimise Operator error.

Fault tree analysis is not essential to determine accident probability and companies are much more likely to use argument based on the following:-

- Prescriptive legislation.
- Regulatory guidance.
- Standards produced by Industry Associations and other standard making organisations.
- Operating company or market leader documents.
- Historical data.

It is acceptable for the safety report to refer to world-wide failure data on storage vessels of similar size and duty that have been operated and maintained to equivalent standards and deduce, on the basis that the company's standard of construction and operation was at least as good if not better, that the failure frequency of a storage tank or other equipment is similar. However, the evidence in the safety report on construction, maintenance and operation standards would need to be convincing.

Approaches based on well founded argument are acceptable, but a safety report that:-

- discounts some accident sequences;
- fails to consider worst case locations for breaks;
- assumes procedures and/or safety systems function perfectly;

may be judged as failing to meet the assessment criteria.

Base event failure rate data are essential components of quantitative risk assessments, but they must be relevant and applicable to site circumstances. Simply taking a number from the literature without consideration of whether it applies to the site in question is unlikely to be acceptable. On the other hand, use of a failure rate that is not consistent with historical or relevant generic industry data must be justified. It is acceptable for Operators, who have been responsible for accident investigation and storing failure rate data for essential components to use their own data if it is statistically robust.

Q: Have all the sequences leading up to each major event been identified?

All events/initiators identified in Table 2 should be considered even if some of them are not applicable to the site in question.

Some events such as aircraft impact, earthquake, dropped load, etc are capable of damaging any item of plant, but a safety report need only consider the event once unless a different hazardous substance can be released, or the severity of the release varies significantly.

The types of fire that may follow a release of distilled spirit are usually obvious and the safety report should calculate the thermal radiation hazard range in each case. The only area of ambiguity concerns VCEs and whether there is sufficient containment or flame accelerating structures to give rise to an explosion. This is a difficult question for the Assessor, particularly as some safety reports may not adopt worst case assumptions. If

sufficient spirit vapour can be released into a confined or congested area, the Assessor may need to consult the MSDU topic specialist about the likelihood and severity of an explosion.

Q: Is the complexity and level of detail of the analysis appropriate to the scale of the hazard?

The frequency of accidents that have severe consequences for local populations need to be determined more precisely than accidents that have only on-site effects and at worst can impact a small number of plant Operators. This implies that the frequency of severe accidents such as a BLEVE or cold catastrophic tank failure should be determined more reliably than the probability of corrosion leaks and leaks on low pressure pipe work, which have less severe consequences.

Operators who adopt a qualitative approach to risk assessment still need to identify risk dominant accidents by some form of ranking in order to demonstrate that all necessary measures have been taken to prevent major accidents.

Q: Does the accident analysis identify and quantify all event sequences.

Accidents that are the result of multiple failures should not be assigned a frequency unless details of the analysis of the mode and probability of each of the failures that comprise the accident sequence are provided. For example, a safety report that simply states that the frequency of over pressurisation and tank rupture due to vent valve failure is 'f' on the basis of historical data should be judged as containing insufficient detail.

Q: Where the likelihood of a major accident scenario is not predicted, does the safety report describe the measures to prevent all conditions and events leading to it?

If a safety report does not predict the frequency of one or more major accidents, it must describe the conditions under which the accidents can occur. It must then show that the installed safeguards ensure that those conditions are very unlikely ever to arise. This demonstration is only possible for certain systems which have been designed to be intrinsically safe. A system that depends on operators and a mixture of active and passive control systems is always at risk from human and equipment failures.

Criterion 3.4.1 “The report should demonstrate that a systematic process has been used to identify events and event combinations, which could cause MAHs to be realised.”

Here reference should be made to Criterion 3.3 and how it was met by the safety report. Essential for the identification of major accident hazards is a detailed description of the site and all its components, with particular emphasis on those containing or connected to large volumes or high flow rate sources of distilled spirit. The safety report should consider each of these in turn, identifying release scenarios and potential consequences and provide estimates of frequency. It is not necessary for the safety report to quantify the consequences of all of these, but a sufficient and representative set must be identified. Assessors may find the following questions useful when judging the completeness of the accident scenarios considered.

Q: Has a systematic process been used to identify events that cause the realisation of a major accident.

It is more important for the Assessor to be satisfied with the completeness of the accidents considered than for the report to use a formalised methodology to identify accident

scenarios. If the accident analysis deals with each item of plant in turn and identifies all initiators and all types of fire/explosion, then it can be considered systematic. However, if by reference to Table 3, the Assessor can identify scenarios that have been overlooked, the report is deficient. The seriousness of the omission depends on whether the consequences to the public are worse than those from other accidents that are dealt with and whether the risk from the event in question is ALARP.

Q: Does the safety report consider the effect of failure of automatic or manually operated safety systems in the sequence of events leading to a major accident?

The accident sequence identification and analysis in a safety report should consider the failure of all automatic and manually operated safety systems and evaluate the consequences in each case. For example it should consider sequences consisting of:-

- (a) A hidden fault (eg a failed ROSOV).
- (b) An initiating event (eg pipe rupture).
- (c) Failure of an operator to respond correctly.

It may use QRA to demonstrate that the probability of such accidents is very low, but their consequences must be determined.

Table 3 : Accident Initiators Requiring Consideration in a Safety Report

Off-site Events	Operator Error	Abnormal Load	Arson or Sabotage	Inadequate Management	Loss of Service
Aircraft impact	system opened	impact by vehicle	fire	corrosion	Loss of electricity.
Seismic event	filled when not closed	impact by missile	explosion	erosion	loss of cooling water.
Subsidence	system overfilled	impact by dropped load	valve opened	vibration failure of process controls.	loss of nitrogen
Extreme environmental conditions abnormal rain fall abnormal snow fall very low temperature high temperature flooding gale force winds lightening strike	containment degraded.	internal temperature or pressure outside design limit.	safety system degraded.	cyclic load.	loss of compressed air
Vehicle/train impact	excess load	external temp/pressure outside design limit.	contamination	inadequate materials or specification.	loss of steam
Land slip	failure to respond correctly to an alarm.	pressurisation.	control system degraded.	chemical attack	
Explosion	incorrect valve action.	under pressure	containment system degraded.	hidden defect in containment system.	
Fire				failure to detect dangerous situation.	
Missile				failure of process controls.	
Import/export pipeline rupture				Safety system / process monitoring devices not maintained and unavailable on demand	

Criterion 3.4.2 “All safety critical events and associated initiators should be identified.”

Safety critical events are those that dominate the risk at different distances from the plant. For distilled spirit storage vessels, the event with the greatest hazard range is usually an uncontained poolfire. The safety critical events for shorter distances are those occurring the

most frequently occurring and rise to that particular hazard range. The questions below will help Assessors determine if safety critical events are dealt with appropriately.

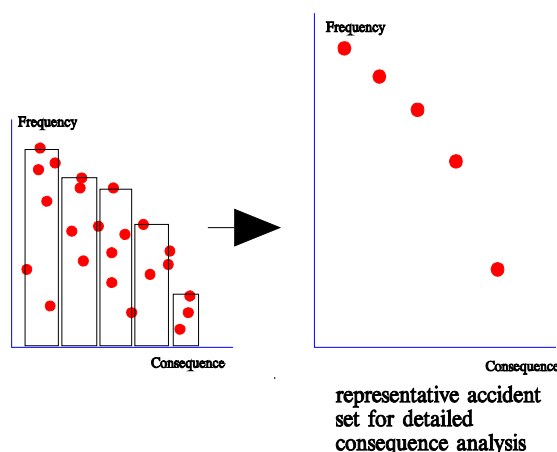
Q: Does the safety report define a safety critical event and describe an approach to their identification?

Some safety reports may not make use of the term 'safety critical event', but all safety reports will calculate the consequences of only a small fraction of the total accidents a site can suffer. These must be chosen carefully in order to ensure they dominate the risk at increasing distance from the site.

The first step in the identification of these risk-dominating events is the quantification of frequency and approximate consequences of all major accidents. These may be grouped into consequence bands as indicated below. The accident at the top of each band is the safety critical event for consequences of that particular level of severity. However, this method should be used with caution since the consequence categories may be quite broad. For example, if a consequence category is defined as one or more off-site fatalities, the most frequent may cause 2 fatalities and would be classed as the SCE, whereas a less frequent event that could cause 200 fatalities would not be identified as a SCE but may be unacceptable and require further risk reduction. It is suggested that the events should also be reviewed qualitatively (i.e. By visual inspection) to identify unusual or high consequence events which should be added to the list of SCEs. In addition, events which in themselves might be low risk, but could escalate to give a more serious event, should be included. The non-QRA approach would group accident according to likelihood and consequences.

The frequency of all accidents in a band can be added together to provide an estimate of the overall frequency of a particular level of consequences. The safety report should then identify a set of representative accidents and frequencies for more detailed consequence analysis.

A safety report that fails to analyse accidents in this way may not be complying with the assessment criteria. However, approaches that are not based on quantification, but never the less rank accidents appropriately, should not be rejected out of hand.



Q: Does the safety report list the safety critical events that have been identified?

The safety report should list the safety critical events for each group of accidents that have similar consequences. In general these will form the reduced set that are analysed in depth

in the report as indicated above where 5 safety critical accidents are used to represent the risk from the site.

Criterion 3.4.3 “Estimates of, or assumptions made about, the reliability of protective systems and the time for operators to respond and isolate loss-of-containment accidents, etc need to be realistic and adequately justified.”

Operators should not base their accident analysis on the assumption that all protective systems will perform perfectly and Operators are 100% reliable. For example, if a whisky transport line is fitted with a remotely operated slam shut safety valve, the safety report should consider the consequences of it failing to isolate a failure on that line. Similarly, if a pipe is fitted with a manually operated shut-off valve, the safety report needs to consider what would happen if it was not closed in the event of a failure down stream. The following questions are designed to provide guidance on this criterion:-

Q: Are appropriate failure probabilities used in the accident analysis?

Operators should not use failure probabilities taken from standard references in their accident analysis without showing that they are applicable to the plant and conditions in question. The Assessor should be particularly concerned about the data used in the determination of the frequency of safety critical accidents.

For example, if the general rate of failure of flexible hose is f , an Operator can only claim a similar failure rate if hoses on his site are inspected and maintained to the same standard as the population to which the failure data applies.

If the Operator determines accident likelihood on the basis of historical data or some other method that does not involve a calculation of accident frequency, the Assessor should be convinced that the probabilities are applicable to the plant in question. This implies that good evidence should be presented to show that the plant is designed, operated and maintained to appropriate standards and that the operators controlling it are adequately trained.

Q: Does the accident analysis make use of optimistically short response times for control/safety equipment?

A safety report that does not examine the consequences of prolonged releases (20 minutes or more), on the basis that a valve will be closed and the release terminated within a shorter period should be deemed to contain an optimistic accident consequence analysis.

Q: Are the assumptions made about operator response reasonable?

The safety report may claim that control room Operators will notice an illuminated alarm indicator immediately or will respond to an emergency perfectly and close valves in a matter of seconds. Such assumptions may be optimistic, but their presence does not necessarily signify that the safety report is deficient if the consequences of much longer response times are determined.

Q: Does the Operator claim that some potentially serious failures will not result in a major accident because a single safety/control system will recover the situation?

Since all safety/control systems can fail, Operators should take the view that whisky spirit can escape from its containment system and that releases of 100% of the inventory of

storage vessels must be considered in a safety report irrespective of the complexity of the safeguards.

Criterion 3.4.4 “The methods used to generate event sequences and estimates of the probabilities of potential major accidents should be appropriate and have been used correctly.”

The conventional methods of determining the frequencies of accidents involving multiple failures are fault tree and event tree analysis or a combination of the two. They are labour intensive and require reliable failure probabilities and experience in their application. Many safety reports adopt a much simpler approach. For example, accident sequences may be broken down into three components - an initiating event, a control system failure and an Operator failure. The frequency of the accident is then determined by assigning probabilities to the components and multiplying them together. While this approach may be acceptable, Assessors should be aware that it can hide a large number of events/failures that are not being quantified. There may be a dozen ways the control system can fail and several ways in which the Operator can respond incorrectly. Since the probabilities of these alternatives are usually additive, the Assessor needs to be convinced that the analysis is not optimistic. The following questions may help the Assessor to reach a conclusion on this issue:-

Q: Does the frequency analysis recognise that failures of complex systems and Operators have many components?

If an explosion or fire in a maturation warehouse can only occur following a series of Operator and control equipment failures, the Operator will need to identify each of these in order to satisfy the Assessor that his calculated event probability is reasonable. If a break down of the individual events and probabilities is not provided, the Assessor is justified in requesting further information from the Operator.

Q: Does the safety report consider the full range of conditions for each accident?

Accident consequences should not be reduced on the grounds that the probability of the wind blowing in a particular direction is low if very similar consequences arise when the wind is blowing in any direction. Nor should risk be based on the probability of a failure in a particular location when failures over a whole range of other locations may have similar consequences. The Assessor must decide the weight attached to such omissions.

Q: Does the analysis take into account uncertainties in the estimation process?

The fact that most failure probabilities are not single values, but distributed about a mean should be accounted for in risk analysis. If there is no information on the probability distribution of the probability, it must be concluded that the upper figure is just as likely as the lower figure.

Q: Does the safety report show that site specific factors have been taken into account in the methods used to generate event sequences and estimates of the probabilities of potential major accidents?

Assessors should be careful not to accept accident analysis from an Operator's 'core safety report' if the safety report in question does not take account of site specific information on accident initiators and initiator probability. For example, a core safety report may give a frequency for aircraft impact based on a background crash rate for the whole of the UK. This would not be applicable to a site located close to a busy airport. Likewise the presence

of a railway line running along a site boundary increases the probability of an accident caused by a derailment.

In general, off-site accident initiators tend to be site specific, but differences in site management, operation and competence (training) of the staff can also significantly affect accident frequency.

Criterion 3.4.5 “The safety report should provide adequate justification for event probabilities that are not consistent with historical or relevant generic industry data.”

Many risk assessments in safety reports make use of industry standard probabilities for events such as pipe rupture, cold catastrophic failure of vessels, Operator response time etc. The Assessor should compare these data against those given in the table below and request the Operator to explain the reasons for any significant difference.

Table 4 : Typical Failure Frequencies

Event	Probability/Frequency
Export/import line failure	$5 \times 10^{-4}/\text{km.yr}$
Lightning strike	$1 \times 10^{-7}/\text{yr}$
Severe earthquake capable of rupturing pipework	$1 \times 10^{-6}/\text{yr} - 1 \times 10^{-7}/\text{yr}$
Sudden catastrophic failure of vessels	$3 \times 10^{-6}/\text{yr}$
Failure of a ROSOV on demand	3×10^{-2}
Failure of an excess flow control valve on demand	$1.3 \times 10^{-2}/\text{yr}$
Failure of an automatic shutoff valve to close	$1 \times 10^{-2}/\text{demand}$
Failure of a level sensor (sticking)	50 per 10^6 hrs
Failure of a flow sensor	40 per 10^6 hrs

Generic or industry standard failure probabilities for valves, pumps, etc are based on appropriate operation under an industry standard maintenance regime, which may be different from that prevailing at a site. Use of such data in risk calculations in a safety report should therefore be justified. Assessment of the justification can be via the following questions: -

Q: Are the failure data derived from long experience of operation in the same industry and under the same conditions?

Failure rate data from the Operator's own and long established data base can usually be accepted, but if data are based on experience in another industry (eg nuclear), the Operator must justify their use in accident analysis by reference to operating conditions, maintenance regimes, etc. If this justification is not present, the Assessor may reach the conclusion that the risk assessment is optimistic.

Q: Is the probability of failure of a particular item of plant based on generic data for an identical component or one that closely resembles it in design, manufacture and operation?

The mean failure frequency of plant components should be increased when they are used under conditions that are different from their design operating conditions. Similarly, the mean failure rate of a component should be increased if it is assumed to apply to another similar, but not identical, component. The increase depends on whether the new conditions make more or less demands on the component. Failure to recognise such reliability

changes can result in an optimistic risk assessment, particularly if the data is used to quantify the frequency of a safety critical sequence.

Criterion 3.5 “The safety report should provide details to demonstrate that suitable and sufficient consequence assessment for each major accident scenario has been carried out with respect to people and the environment.”

The principal hazards from distilled spirit storage are fires and explosions. The hazards arise from leaks in the tanks themselves, casks and ancillary equipment such as transfer pumps, pipe work and flexible hoses, all of which can release significant quantities of liquid on failure. A vapour cloud explosion may be possible depending on the size of the release, the spillage surface, and the presence of confined volumes or adjacent structures that produce flame acceleration. All of these require detailed assessment in the safety report.

The accidental release scenarios that should be addressed in a safety report include:-

- Evaporating pools.
- Pool fire (with toxic combustion products from the wooden casks).
- Flash fires.
- Jet fires.
- Explosion.
- Tank fire.
- Release to the environment.

Assessors can test compliance with Criterion 3.5 by asking the following questions:-

Q: Is the Operator's accident consequence assessment thorough and adequately documented?

A safety report should discuss external events and site incidents that range in severity from catastrophic failure of a storage vessel to a small leak and should identify the measures and precautions taken to reduce their probability. Catastrophic failure can be caused by a variety of off-site and on-site events. Less severe leaks may be the result of mechanical failure, impact damage, lightning, flame impingement or electrical failure.

The accident consequence analysis should be a systematic process comprising the following steps:-

- List the assumptions that will be made about containment failures (size, location).
- Describe the essential features of the model that will be used to calculate the rate of outflow of LPG and the duration of the release.
- List the assumptions used in the assessment.
- Present the results of the assessment to characterise the LPG release.

- Identify the model that will be used to determine the characteristics of the thermal radiation source for scenarios involving immediate ignition (fireball and jet fire and pool fire).
- List the assumptions used to calculate the radiant flux from the burning gas (emissive power, wind speed, etc).
- List the assumptions about the dose received by individuals indoors and outdoors.
- Present the results of individual dose calculations.
- List the assumptions for LPG gas dispersion (flash fire calculation).
- List the assumptions used in the dispersion analysis (stability, wind speed ground roughness).
- Describe the essential features of the model used to calculate the dispersion of release LPG.
- Present the results of calculations of the dimensions of a flash fire.
- Describe the effect of accidents on local populations and the environment.
- Justify why a VCE will not occur.

All of the above steps should be clearly documented in the report. However, omission of one or more of them is not a significant failing if overall the consequence analysis is satisfactory.

Q: Has the Operator selected a set of accident scenarios for the safety report that encompass the hazards and risks from the site and that are sufficient to demonstrate that all necessary measures have been taken to minimise risk?

A minimum accident set for an maturation warehouse/distillery site would be:-

- Warehouse fire.
- Cask store fire.
- Puncture of a road tanker, leading to a spirit pool fire.
- Explosion in a warehouse.
- Catastrophic tank failure - 100% of contents released to bund with 50% bund over top.
- Contained and uncontained vaporising pools with a justification for the assumed pool diameter.
- Storage vessel hole with spigot flow inside and beyond (where justified) the bund.

- Pool fire and running pool fire with secondary plant engulfment.
- Flammable cloud formation - flash fire / VCE (if possible).
- Discharge / filling lines rupture with pool fire engulfment of tankage.
- BLEVE of a road tanker during filling / discharge activities.
- Puncture of a storage tank (>0.1m in diameter).
- Accident involving a cask transporter - loss of the contents of several casks, resulting in a pool fire.
- Pipe line failures (rupture, puncture, small leak) leading to a pool fire, flash fire.
- Spillage into watercourse via the drainage system.
- Contaminated fire fighting water run off into a water course.
- In tank explosion.

Q: Has the full range of consequences been addressed?

The safety report should not discount any scenario unless it can provide good reasons for doing so. Safety reports can discount certain types of accident on the grounds of experiment and historical data, but this must be summarised.

In addition, leaks into an enclosed space, that may result in a confined explosion should not be forgotten.

High pressure pipe work failures should include the formation of a vertical and horizontal jet and the potential for jet flame impingement. In addition leaks into an enclosed space that may result in a confined explosion should not be forgotten.

The number of fatalities and individuals with severe burns from fires and explosions should be determined. The effect of blast should also be quantified in terms of the number of buildings in each of several damage categories and the envelope of a flash fire should be superimposed on a map so that the effect of wind direction on the number of casualties can be assessed.

The accident analysis should address the effect of other variables such as time of year, time of day and day of the week if they have a significant effect on the off-site consequences. A limited analysis that neglects variability in accident consequences may not meet the assessment criteria.

Q: Does the safety report outline the principal features of the mathematical models used in the consequence analysis?

A safety report should include a brief description of the essential features and assumptions of the mathematical models used by the Operator to determine the consequences of major accidents. If the models are part of a well-known software package, then only the name of the software is required, but full details of the input should be provided. In-house models and any validation studies that have been carried out to support them should be described

in detail. The main equations of a model should be given in an appendix if they have not been published elsewhere.

The fact that an Operator has used a well-validated model to determine the consequences of an accident does not guarantee that the results are reliable. Assessors should recognise that the predictions of consequence analysis are more important than the means by which they were obtained. Assessors may feel that a safety report that fails to provide input data details for predictions, which appear optimistic, fails to meet the criteria.

Q: Does the severity of the predicted consequences influence the amount of information the Operator should supply on how they were determined?

The level of detail that should be provided on the calculation of the consequences of an accident that do not extend off-site is less than if the hazard range encompassed a large number of people. It is not possible to be prescriptive on this issue and Assessors are expected to use professional judgement when deciding if the Operator has provided sufficient information on his consequence analysis. However, the following examples may help Assessors make a judgement on this issue.

If the footprint of a flash fire defined by $\frac{1}{2}$ LFL does not encompass any off-site populations, then the flash fire hazardous area can be equated to this area and the flash fire risk dismissed in one or two sentences. On the other hand, if a hazard footprint encompassed a densely populated area, the Operator should provide a more detailed analysis with a discussion of the most appropriate concentration based on a risk assessment. Alternatively, consideration should be given to any arguments and data which the company may wish to put forward in support of the use of LFL as the flash fire criterion. The arguments would include a validated peak concentration dispersion model rather than a time averaged model. If the LFL contour fell a few metres short of a densely populated area, then again the Operator should consider the probability of a flash fire extending beyond the LFL boundary.

Q: Does the accident consequence analysis extend to all dangerous substances on site?

Whisky maturation warehouse sites sometimes hold a variety of other hazardous materials, which may need to be considered in the report. These include a natural gas supply to a boiler, a LPG cylinder, dangerous powders and/or toxic substances in tanks or drums.

Criterion 3.5.1 “Source terms used should be appropriate and need to have been used correctly for each relevant major accident.”

The source term for an accident sequence expresses ‘how much’, ‘for how long’ and in ‘what form’. For example, a spill of whisky from a bulk storage vessel is characterised by the release rate, the duration of the release and its location (whether or not it is retained in the bund). Assessors can use the following questions to test the adequacy of the description of accidents given in a safety report:-

Q: Do the source terms for each accident encompass an adequate range of release rate and include the ‘worst case’?

Since release rate is effectively determined by hole size and driving force (pressure or liquid head), the accident consequences described in a safety report should encompass a range of hole size and include the largest possible failure. This means guillotine rupture of a pipe and catastrophic failure of a vessel leading to an instantaneous release of the whole contents.

The 'worst event' should be assumed to occur under 'worst conditions', which are when a storage vessel or tank is full, when the pressure in a pipe is a maximum and when the filling pressure or flow rate is a maximum.

Q: Are pessimistic assumptions used to quantify source terms?

The flow rate of liquid through a hole or from a pipe depends on the assumptions made about the hole or pipe size, pump characteristics, discharge coefficient, the pipe roughness, the friction factor, etc. The values assigned to these parameters should ensure that the calculated consequences of accidents are not optimistically small. For example, use of a low value of discharge coefficient should be justified and the choice of parameters used to calculate the evaporation of a pool should be explained. If in doubt, the assessor should consult the relevant MSDU topic specialist.

Q: Does the safety report show that site specific factors have been taken into account in the use of source term models?

The source terms for accidents should account for site-specific features. These relate to:-

- The frequency of releases.
- The magnitude of releases.
- The duration of release.

and could include parameters such as:-

- The size and type of storage vessels.
- The number and capacity of road tanker deliveries per year.
- Whether the site is manned 24 hours/day.
- Tank padding pressure and the maximum value this could rise to in the event of a failure.
- The maintenance schedule for key safety features such as ROSOVs.

Criterion 3.5.2 “The material transport models used should be appropriate and need to have been used correctly for each relevant MAH.”

The transport models used to determine the consequences of accidents include those used to characterise pool evaporation, and gas dispersion. The thermal radiation from pool fires can be calculated using standard equations, but complex models may be required to evaluate the consequences of releases to water from sites located close to rivers or an estuary.

It is often difficult for an Assessor to reach conclusions about the adequacy of the consequence analysis, but the answers to the following questions may provide the basis for an assessment:-

Q: Are the predicted hazard source dimensions in accordance with those calculated by HSE models?

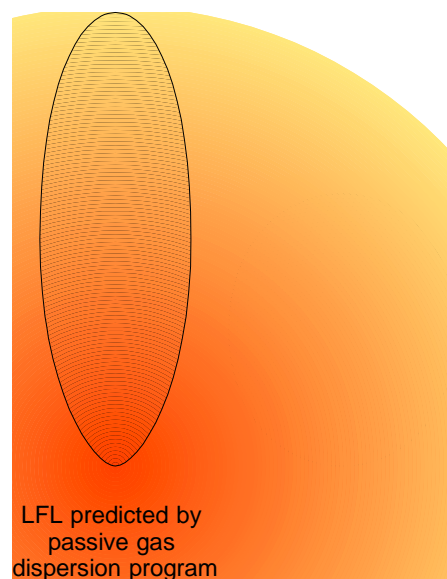
The agreement between hazard range predicted by HSE models and those in a safety report should be within $\pm 50\%$. Greater differences are acceptable if the consequences do not include fatalities, but when they do, and the reason for a significance discrepancy is not obvious or is due to an inappropriate assumption, Assessors may judge safety report to be deficient.

Q: What sort of dispersion model is used to calculate the dimensions of a flammable cloud of evaporating alcohol?

The molecular weight of alcohol vapours is greater than that of air, but the plume from an evaporating pool usually disperses passively. Several integrated dispersion models that determine the correct dispersion model from the substance properties and the characteristics of the release are available, but their use requires careful evaluation of the source term assumptions. The topic specialists should be consulted if the predictions appear to be optimistic.

Q: Does the dispersion model take account of obstacles such as buildings and changes in topography?

Accidental releases at ground level have to disperse around site buildings, and in doing so become more dilute. This implies that when gas has to move around buildings the concentration at a particular distance from the release point is lower than that predicted by dispersion over a smooth flat terrain. On the other hand the concentration will be higher if the gas is constrained from dispersing sideways by buildings on either side of a street. Both of these aspects should be addressed in a safety report.



Q: What wind speeds are considered for dispersion calculations?

In general, for continuous releases, the higher the wind speeds the more rapid is the dispersion and shorter is the hazard range. D5 weather conditions occur frequently in the UK and should be used to calculate the hazard range for daytime releases. Dispersion is reduced under stable atmospheric conditions, hence F2 weather, which characterises night time conditions, generally produces the greatest hazard range. However, buoyant clouds tend to ascend when the wind speed is low and reduce ground level concentrations. Under

any stability, increases in wind speed tend to decrease the predicted hazard range unless building wake effects are modelled.

A safety report should calculate the consequences of accidents under a range of weather conditions including those that maximise the hazard range and are most typical at the plant location.

For instantaneous releases, these general observations may not be applicable.

Q: What ground roughness values are used for the dispersion calculation?

The rougher the ground over which a flammable gas is dispersing the more rapid is the rate of air entrainment and the shorter is the flammable hazard range. A ground roughness value of 0.1 corresponding to elements on the ground about 0.5-1 metre high is recommended for dispersion over agricultural land. A roughness value of 0.3 should be used for dispersion over a suburban area. Although higher roughness values may be assigned to some industrial sites, their use results in a reduced hazard range that could, under certain circumstances, be optimistic. An Operator should make a special case for use of a ground roughness value of more than 0.3. A value of less than 0.1 may be considered appropriate for dispersion over water i.e. at estuary or coastal sites.

Q: What averaging time is used for dispersion calculations?

Due to the variability of atmospheric conditions a dispersing gas plume meanders and the concentration at a fixed point down wind of a release fluctuates. Most dispersion models account for this phenomena by introducing an averaging period. The longer this is, the more allowance is made for the variations in wind direction and the smaller is the predicted concentration.

There is not a consensus on the most appropriate averaging period for dispersion calculations, but widespread support exists for use of 600 seconds and 10 seconds for continuous and instantaneous releases. In some passive dispersion models the standard deviations are linked to specific averaging times.

Since criteria 3.5.2 is concerned with the appropriateness of transport modelling assumptions, and averaging time can have a significant affect on the predicted hazard range, it is important that the Operators state the values used in the dispersion analysis. This requirement is not restricted to averaging time; Operators are obliged under criterion 3.5 to provide details of all important modelling assumptions and input.

Criterion 3.5.3 “Other consequence models (eg BLEVE, warehouse fire, etc), used should be appropriate and need to have been used correctly for each relevant major accident.”

Aside from vapour transport models, the consequence analysis for an distilled spirit storage area needs to include models for thermal radiation from different types of fire and for the over pressure produced by explosions. It is important that these models do not underestimate the hazard range, but it is difficult for an Assessor to make judgements about the level of pessimism in a calculation if full details of the model are not supplied. Toxic effects and toxic combustion products should also be included in the report, but their assessment presents problems. The following questions may help Assessors judge if the consequence analysis is based on appropriate assumptions:-

Q: Is the orientation of pool fires chosen to maximise their consequences?

The thermal radiation received by a target from a pool fire reaches a maximum when the wind is blowing the flames towards it. A consequence analysis will be optimistic if it only considers the thermal radiation from pool fires in low or zero wind speeds.

Q: Does the consequence analysis take into account local ground features to evaluate uncontained releases of whisky spirit?

Low pressure releases of spirit generally end up running along the ground until reaching a natural or man made bund or drainage system. Bunds contain and limit pool size and evaporation therefore a report that fails to address bund over topping should be considered to contain serious omissions. Uncontained pools can spread over a large area and cover different surfaces. Their evaporation rate is generally much higher than that of bunded pools, hence their associated hazard range can be significantly greater.

At typical distillation and warehouse sites, uncontained evaporating pools of up to 50 metres radius should not be discounted without justification. Running pool fires engulfing road tanker loading facilities and other sensitive plant should be included in the report as should their consequences on entry in to drainage systems and/or an interceptor. Pool depth is an important parameter and assumed values should be justified taking account of surface type. A few millimetres may be appropriate for flat smooth concrete, but several centimetres is reasonable for rough hard-core.

Q: What is the assumed inventory and dimensions of an evaporating pool or pool fire?

The modelling assumptions and in particular the assumed inventory and dimensions of a pool are of major significance and should not be subject to excessive optimism. Increasing the pool radius significantly increases the evaporation rate. It is reasonable to assume that accidents involving an instantaneous release of the whole contents of storage vessel produces a surging liquid wave, capable of over topping most bund walls.

Uncontained pools have a significantly greater hazard range than bunded releases. Catastrophic tank failures should assume the tank is filled to its maximum inventory level and that 50% of the contents may overtop the bund. Assessors may conclude that hazards based on less severe accidents are optimistic.

Q: What atmospheric humidity is assumed for thermal radiation calculations?

The thermal radiation emitted by a fire is attenuated by water vapour in the atmosphere, therefore the flux at a target is inversely proportional to the humidity. In the UK, humidity varies considerably, but an average value of 60% is often assumed for hazard calculations.

Q: What surface emissive power is assumed for pool fires and other thermal events?

HSE recommends a surface emissive power in the range of 50 - 150 kW/m² for hydrocarbon pool fires and 150 - 300 kW/m² for fireballs. The corresponding value for a jet fire is around 200 kW/m², alternatively the fraction of the total heat of combustion that is radiated can be set to about 0.2. Any thermal radiation calculations based on significantly lower emissive powers than these are likely to be optimistic - see Table 5.

Q: What stored energy figure is used in explosion calculations?

There are several methods of calculating blast over pressure from flammable gas explosions, but assessors should be aware that the TNT model is considered over simplistic because gas explosions have different characteristics to TNT explosions. The multi-energy

method based on lines 2 and 7 is preferred, but if a safety report calculates over pressure on the basis of an equivalent mass of TNT, it is reasonable to set the mass of TNT to twice the mass of gas in the confined or congested volume. The TNT equivalent of most hydrocarbons is 0.42 M, where M is the mass of vapour in the cloud and major deviations from this require a good explanation.

[Q: Does the safety report show that site specific factors have been taken into account in the use of other models?](#)

The models used to calculate the consequences of fires and explosions should account for site specific factors such as:-

- Pressure relief set point and capacity of pressure relief valves on bulk storage vessels.
- Bunding arrangements at road tanker loading/unloading facilities.
- The presence of cask stores.
- Congested areas.
- Neighbours that could be affected by thermal radiation or overpressure.

Table 5 : Effect of Input Parameters on Predicted Accident Consequences

Parameter	Accident Type/Phenomena	Acceptable Value	Direction to Reduce Severity of Consequences
Wind speed.	Passive, or buoyant dispersion of flammable vapour.	2m/s F stability	+
		5m/s D stability	+
	Pool fire.	10 - 15m/s towards the target.	-
	Warehouse fire Cask pile fire	5, 10 and 15m/s 5,10 and 15 m/s	
Ground roughness.	Cloud dispersion.	0.3m (suburban environment). 0.1m open countryside	+
Averaging period.	Passive dispersion.	600s plume 10s puff	+ +
Elevation of fireball	Fire engulfment of a road tanker resulting in a BLEVE.	Touching the ground.	+
Humidity.	Fireball and jet fire.	60% or less	+
Surface emissive power.	Fireball.	270kW/m ²	-
	Spray jet fire.	200 kW/m ² or 0.3 % of heat of combustion	-
	Pool fire.	50 - 150 kW/m ²	-
	Warehouse fire Cask pile fire	250 kW/m ² 170kW/m ²	
Stored energy in hydrocarbon cloud.	VCE	0.42 TNT equivalence	-
Variation in pool depth and radius.	Evaporating pool.	1- 10 cm or depth as dictated by containment area and release volume.	+
		Up to 50m diameter unless plant detail justifies a lesser radius.	-
Spillage surface.	Evaporating pool.	Must reflect spillage surface. Typically concrete for bunds. Tarmac for roads and other areas. Loose chipping in other areas.	Lowest Highest

Criterion 3.5.4 “The harm criteria or vulnerability models used to assess the impact of each MAH on people and the environment should be appropriate and have been used correctly for each relevant major accident.”

A safety report should calculate thermal radiation and explosion over pressure hazard ranges and casualties for several severity levels, which for thermal radiation, may include:-

- dangerous dose of thermal radiation for vulnerable people (500 tdu);equivalent to 4.9kw/m² exposure for 1 minute.
- dangerous dose of thermal radiation for average members of society (1000 tdu);equivalent to 8.2kw/m² exposure for 1 minute.

- significant likelihood of death (1800 tdu); equivalent to 12.8kw/m² exposure for 1 minute.

For over pressure the appropriate hazard ranges correspond to:-

- window breakage (40 mbar);
- houses uninhabitable but repairable (100 mbar);
- severely damaged houses (200 mbar);
- houses completely demolished (500 mbar).

Toxic gas exposure estimates for indoor and out of doors should be based on the dangerous toxic load $C^n t = A$ (ppmⁿ min) relationship where concentration is raised to a power “n” depending on the hazardous substance. A “dangerous toxic load” typically represents, a dose that would result in:-

- 1-5% fatality.
- 50% hospitalisation.
- Severe distress for the remainder.

However the “A” value can be modified to account for populations of different sensitivity. A lower value of “A” may be appropriate for predicting the effects of a release into an old persons home.

For secondary fires:-

- Spontaneous ignition (25.6 kW/m²).
- Piloted ignition (14.7 kW/m²).

It is very important that the full spectrum of casualties is calculated, not only for risk evaluation, but also for emergency planning purposes. Some safety reports may contain casualty estimates based upon other criteria such as a dose that relates to a value considered immediately dangerous to life and health (IDLH). Assessors should be check that such predictions are not overly optimistic.

The following questions may assist the Assessor to judge the adequacy of the accident consequence analysis:-

Q: What hazard ranges for thermal radiation has been calculated?

Although HSE has published its thermal radiation criteria, some safety reports calculate hazard ranges to different dose and flux levels. One of these is 300 tdu, which is the dose to cause blistering of the skin. It extends beyond the 500 tdu range and may be regarded as pessimistic, but any dose implies an exposure duration and Assessors need to understand the assumptions being made before making judgements about acceptability. In particular significant departures from the following assumptions that lead to shorter hazard ranges should be justified:-

- The exposure period for fireballs is the fireball duration (no escape).

- Average members of the public escape from long duration fires at 2.5 m/s.
- The escape speed for the old and very young is closer to 1 m/s.
- The distance to shelter in suburban areas is typically 50 metres.
- The distance in rural areas is more likely to be at least 75 metres.

Individuals escaping from a source of thermal radiation reduce the dose they receive on two counts. Firstly they increase the distance between them and the fire, (and thereby reduce the level of received thermal flux) and secondly, they can reduce the exposure period by going indoors.

HSE has two criteria for thermal radiation flux to buildings based on the ignition of American Whitewood (see Consequence Assessment in part 2), and while these are useful for assessing risk to occupants of houses, they provide little information on the hazard flux for a maturation warehouse storage facility. In this context the actions of the local fire service are important because they may be able to keep adjacent items of plant cool with water sprays. However, a safety report should assume that plant in the vicinity of a major fire do not receive water spray protection for 20 minutes. Predictions based on a much shorter response time for the fire brigade are likely to be optimistic. Operators must consider the consequences of late arrival of fire fighting services, but it is permissible for them to make judgements about the probability of such an occurrence.

Q: What hazard ranges for blast overpressure is calculated?

The effects of blast over pressure on buildings and on people cannot be predicted precisely, but HSE has published tables of the consequences of a range of side-on over pressure. Different over pressures can be used in consequence calculations provided they convey a realistic picture of the scale and extent of the damage from an explosion. To this end, the following data are useful: -

- 2.5 mbar or 250 Pa - lower limit of window damage.
- 50 mbar or 5000 Pa - lower limit of damage to doors, cladding and people.
- 150 mbar or 15000 Pa - lower limit of severe structural damage to buildings.
- 250 mbar or 25000 Pa - lower limit of significant likelihood of severe injury.

A safety report that presents hazard ranges corresponding to higher over pressures than those above is not providing the full picture of the potential damage caused by explosions.

Criterion 3.5.5 “Are the assumptions in the accident analysis justified and not unduly optimistic.”

The assumptions being referred to here are those made about the response/effectiveness of accident consequence mitigation systems and include such things as the time to detect a large release of distilled spirit and the probability that a slam-shut will close on demand, or an operator will act in a predetermined way. The safety report should determine the consequences of worst accident scenarios on the assumption that all control and mitigation systems fail on demand and operational conditions correspond to worst case. Such a scenario should have a very low probability. The analysis should also consider the effect of

various combinations of partial success of the control and mitigation systems in order to determine the risk dominating accidents.

A safety report that minimises accident consequences on the assumption that installed mitigation systems work perfectly is underestimating risk. Assessors can judge this aspect of safety reports by reference to the following questions:-

Q: Are the accident source terms 'worst case'?

The safety report for a whisky distillery and maturation warehouse facility should consider an instantaneous release of the whole contents of a storage vessel to an uncontained evaporating pool with and without early ignition and with subsequent dispersion of the vapour and fire.

Various other scenarios that result in a continuous release of several 10s of kg/s and give rise to a variety of fires which may engulf other plant and escalate the accident should also be considered. In addition the safety report should address failure of pipelines at "worst" locations, and failure of other items of plant such as a transfer pumps or flexible connections. The conditions that could give rise to a VCE or BLEVE should be identified and the consequences of these events determined. Environmental hazards must also be adequately addressed.

Q: Are the full range of consequences of each major accident determined?

A large release of distilled spirit can give rise to a variety of hazards that may include warehouse fire, warehouse explosion, cask store fire, pool fire, explosion, discharge to a water course and contamination due to fire water run off. A safety report should address each one paying particular attention to releases of vapours into confined or congested areas where significant over pressure can follow ignition.

Q: Does the accident analysis examine the effect of different conditions and assumptions on the predicted consequences?

The consequences of many severe accidents depend on the environmental conditions, the state of the plant at the moment of failure and the location and type of failure. Since there are many combinations with roughly equal probability, the safety report must determine the consequences of each accident under a range of conditions that encompass the full severity range.

Both day time and night time conditions should be considered for accidents affected by stability (ie those involving dispersion). It is important that a safety report describes the consequences of the worst conceivable accidents at a site, which occur when warehouses are full, cask stores have the maximum number of casks, and bulk storage tanks are filled to capacity. If the accident analysis in a safety report is based on average inventories, it should be judged as incorporating too much optimism.

Q: Does the safety report fully describe the models used to predict accident consequences?

A safety report should describe the mathematical models used to predict the consequences of accidents. If the Operator or his consultant used well known software to calculate the consequences of accidents, information on the input data files should be provided so that Assessors can check its appropriateness and degree of conservatism both of which provide an insight into the Operators approach to accident consequence analysis. If doubts remain,

entering the Operator's input data into an HSE model can check the predictions in the safety report.

A difference in opinion about the severity of accident consequences may occur from time to time. It does not imply a major failing of the safety report but one which the Assessor should try to resolve by communication with the topic specialist, and, if necessary, with the Operator.

Criterion 3.5.6 “Estimates of the severity and extent of each major accident consequences are realistic.”

COMAH Regulations Schedule 4, Part 2, Section 4(b) requires operators to provide an “assessment of the extent and severity of the consequences of identified major accidents”. This is extended by SRAM Criterion 3.5.6 which requires that this assessment is realistic.

Duty holders should provide explicit information (perhaps in tabular form) which links each scenario with the number of people who may be affected (as a minimum) and preferably estimates of the number of fatalities and hospitalisations and those receiving minor injuries for each wind direction (where appropriate). This will provide the assessor with the information needed to determine the significance of each scenario.

We believe it is necessary if we are to be able to make a judgement on “all necessary measures” and the suitability of the information provided for offsite emergency plans (Schedule 4, Part 1, Section 4 and SRAM Part 2, Chapter 1).

Safety reports should determine the consequences of the worst accidents, but the analysis should not be overly conservative. If unrealistic hazard ranges are predicted, the off site emergency plan devised by the Local Authority may be ill conceived and under some circumstances, lives could be put at risk by spreading emergency services too thinly. The Assessor can gauge the degree of conservatism in the calculations by asking the following questions:-

Q: Are the input data for mathematical models reasonable?

Reasonable values for some of the more important input data for accident consequence modelling are shown in Table 5. Assessors should compare these values with those used by the Operator and make judgements about the realism of the consequence predictions.

Criterion 3.6 “Do the findings and conclusions in the safety report demonstrate that the measures adopted to prevent and mitigate major accidents make the risks ALARP?”

The findings and conclusions from the predictive risk analysis should summarise the relationship between hazards and risks and demonstrate that the measures adopted to prevent and mitigate major accidents make the risks ALARP.

The assessment team must come to an agreed view on whether the report meets the requirements of criterion 3.6. Guidance is provided in SRAM Part 2 Chapter 1 for this purpose. The predictive assessor needs to form their own view on how the report meets this criterion so as to contribute into the team's overall conclusions. The assessment guidance is repeated here and expanded upon where relevant for LPG installations.

Most safety reports will not present particularly reliable accident probabilities and in many cases the degree of uncertainty attached to consequence predictions will be unknown. This is relatively unimportant if the scenario is not risk dominant, but when it is, or could be, uncertainties should be offset by extra conservatism. Risk calculations based on optimistic assumptions and highly uncertain data should be treated with great caution, but Assessors should bear in mind the following typical levels of uncertainty:-

Table 6 : Typical Uncertainties in Consequence Modelling

Hazard	Typical Parameter Value	Acceptable Range
Fireball Mass Size Surface emissive power Height of centre Duration View factor Hazard range	100% of release $R=29M^{1/3}$ 200kW/m ² R $t=4.5M^{1/3}$ Sphere touching ground	50% - 100% +/-10% of R 100-200kW/m ² R - 2R +/- 10% of t +/-20% of calculated value +/-50%
Flash fire Mass Buoyancy Dispersion Hazard range	100% of release Neglect Passive model	0-50% No hazard due to lift-off of gas +/-50% on length and width +/-50%
VCE Volume of congested area Stored energy MEM line number Blast over pressure Hazard range (to x mbar)	Actual volume $3.5 \times 10^8 \text{J/m}^3$ 7 and 2 MEM predictions	+/-30% Actual value about half of this 9-5 - 3-1 0-100% 0-150%
Evaporating pool / pool fire Area Depth Containment Substrate surface nature Evaporation rate Burning rate Hazard range basis Thermal radiation Flame tilt Wind speed	Bund area: contained Up to 50m diameter; uncontained. Contained: based on bund area & volume released. Uncontained: 1-5cm depending on ground. Up to 50% over top for tank failure in bund. Concrete / Tarmac / Chippings. GASP or Pentax Poolfire 6 output. Total heat radiated = Assumed SEP x Flame area (SEP = 150kW/m ²) Thomas approach for flame height Dependant on wind speed - Pool fire 6 model D5, 10,15: F2	0-10% 50m likely maximum 0 - 10% 0- 100 % 30 - 70% +/- 30% +/-25% 100-200 +/- 30% of calculated height Check against site specific data
Maturation Warehouse Fire Fire Spread Time Combustion Product Release Flame Pillar Height	Exponential Spread or Quadratic spread 5% of burning rate from wood to CO 6% of burning rate from alcohol to CO Using Burning Rate typical 0.09 kg/s/m ² and surface area of casks on fire	15 - 30 mins 1 - 10% 1 - 10% Up to 120m (400ft)

Irrespective of the mix of argument, semi-quantitative evidence and quantitative analysis used to determine risk, an Assessor should have confidence in the results and concur with the conclusions presented in the safety report.

While the probabilities of worst case scenarios that are not risk dominating do not need to be quantified precisely, the calculation of their consequences should be reasonably reliable so that the emergency services can plan an appropriate response. In this context overly pessimistic predictions are almost as bad as grossly optimistic predictions. The information that emergency planners may require for each accident scenario and for twelve different wind directions is:-

- Probable number of casualties with mild burns or superficial injuries.

- Probable number of people requiring hospitalisation.
- Possible number of deaths.
- The need to evacuate the area around the site.
- Amount of property destruction.

Assessors are required to judge if the risk quantification, risk reduction measures and residual risk meet all the assessment criteria. In effect, they need to take a view on the reliability/accuracy of the predicted hazard ranges and risks and hence upon the acceptability of the predictive analysis. The following set of questions may aid this process:

Q: Does the safety report combine the magnitude of the various consequences assessed with event frequencies, or the likelihood of initiating conditions, to estimate the risk to the most exposed person or groups of persons, on-site and off-site?

There are several ways, in which the results of a risk assessment can be presented including:-

- Contour plots of individual risk of death based on certain assumptions about the individual (ie he is out of doors and he remains out of doors for 30 minutes).
- Risk of death of the individual who is most at risk by being in a certain location for long periods.
- Dose versus distance for accidents with different probability.
- An F/N plot where N is casualties or individuals receiving a dangerous dose.
- A cumulative frequency/N plot.

In order to judge the acceptability of a safety report that presents the results of a QRA, the Assessor may have to make reference to HSE guidance on the tolerability of risk. Since this is expressed in terms of individual risk of death, risk of death is the most useful end point for a risk calculation. However, this does not imply that other representations of risk are unacceptable, merely that they are more difficult to interpret.

A safety report that presents only a table of hazard range and relative likelihood does not comply with the assessment criteria.

Q: Does the safety report show that these risks are negligible or, where not negligible, are ALARP?

It is a requirement of the regulations that Operators demonstrate that all necessary measures have been taken to make residual risks ALARP. The process of "demonstration" is not clearly defined in the regulations, but is interpreted to mean, "justify by well founded arguments or reference to reliable data". In this context Assessors should expect to see risk dominant sequences broken down into a series of events and failures with the probability of each one estimated (either qualitatively or quantitatively as appropriate) by reference to historical data, a respected authority, or by formalised methods such as fault tree analysis. The Operator should be able to show that there is redundancy and diversity in control systems, that operator error is fully accounted for and that the more common initiating

events will not progress to a major accident. All of this should be supported by sound arguments about the absence of further measures that could be introduced to reduce the risks still further.

If the Operator presents a risk assessment based on good practice, industry standards and compliance with HSE recommendations, then it is still possible to show that the residual risks are ALARP by use of cost benefit analysis. In this case, the Operator should list additional safety features that could be incorporated and show that their cost far outweighs the reduction in risk.

Q: Are the risks broadly consistent with HSE guidance on the tolerability of risk?

The Assessor should check that the accumulated probability of death of the off-site individual most at risk from all accident sequence is less than 10^{-4} . If it is not, it is probable that either the safety systems on the plant are deficient (ie risks are not ALARP), or that the accident analysis is overly conservative. In either case the Assessor should reflect his concerns in his assessment report.

Situations may occasionally arise when the safety report fulfils the requirements of the regulations, but the Assessor feels that the societal risk from the installation is uncomfortably high. In such cases, the safety report should not be deemed deficient, but the Assessor should convey his/her feelings to the Assessment Manager for the safety report.

Q: Has the Operator demonstrated that additional safety measures cannot be justified on cost benefit grounds?

The Operator should systematically examine the risk dominant accident sequences and identify additional measure that would reduce the residual risk. He should also justify why none of them have been implemented. Such arguments remove the grounds for rejecting the safety report and open up the possibility of a dialogue about which improvements would be cost effective.

Q: Does the safety report use quantitative arguments for the ALARP demonstration - if so, are the risk criteria stated and justified?

The level of quantification expected for the various types of risk assessment are dealt with by other criteria. The number of failure cases and the depth of analysis increases with proportionality. For a QRA of a complex site a few hundred different MAs may need to be analysed. The presentation of the quantitative arguments may need to be coupled with cost benefit analysis in order to provide the justification that all measures necessary have been taken.

If quantitative arguments are used the methods, assumptions and the criteria adopted for decision making should be explained. For example in the case of fatality risks to people off-site it is common practice [HSE, 1992] for the maximum tolerable level of individual fatality risk to be set at 10^{-4} per year and for the broadly acceptable level to be set at 10^{-6} per year. The corresponding figures for workers are 10^{-3} and 10^{-6} . There are no commonly agreed criteria for lower severity levels, however, HSE have published harm criteria for LUP purposes for a variety of substances, ie the 'dangerous dose' level, which is equivalent to a 1% chance of fatality when a healthy person receives the dose.

Risk Reduction Measures

The safety report should demonstrate that a systematic and sufficiently comprehensive approach to the identification of risk reduction measures has taken place.

Where proportionality indicates that a site could rely on qualitative ALARP demonstration, operators may refer to relevant standards or guidance on good practice to support their demonstration that adequate safety and reliability have been incorporated and that by the measures provided have reduced the risks to as low as is reasonably practicable (ALARP). In making this demonstration operators need to consider the particular circumstances of their site and the consequences of identified major accidents **both on and off site** and decide whether there is anything further which is reasonably practicable before they can complete their demonstration of ALARP. Focus should be placed on **preventing** major accidents but the risks off-site in particular can be reduced by mitigation measures to reduce their consequences.

Where proportionality indicates that something more than a qualitative demonstration is required, the safety report should show that a systematic assessment of additional risk reduction measures has been carried out. In some circumstances there may be risk reduction measures that are reasonably practicable in addition to existing published industry good practice.

Determination of whether risks have been reduced ALARP involves an assessment of the benefits arising from the reduction in risk achieved by particular measures, an assessment of the cost in time, money or trouble of implementing those measures and a comparison of the two. Where there is deemed to be a 'gross disproportion' between the two i.e. The risk reduction being insignificant in relation to the cost then such measures can be ruled out as not reasonably practicable.

Q: Are the standards employed in the risk assessment relevant and up-to-date?

Operators often refer to standards in their risk assessment. These may be a failure frequency, an HSE guidance document or a plant design and operating standard. In each case, the Assessor should consider if the standard is applicable to the Operator's plant and if it is appropriate, given that HSE guidance and standards are updated from time to time. British Standards are revised at regular intervals and while not all the data in the standard may change, a major accident somewhere in the world can lead to a revision of failure frequencies of certain plant items.

At five-year updates HSE expects Operators to carry out a reappraisal of the risks from their operations and to examine if recent technological advances offer opportunities for risk reduction.

Assumptions and Uncertainties

The main conclusions on the measures necessary to control risks should adequately take account of the sensitivity of the results of the analysis to the critical assumptions and data uncertainties.

One of the purposes of the risk assessment in a COMAH safety report is to demonstrate that sufficient control measures are in place to reduce the risks from the installation to a

tolerable level. This is possible if the Operator has accounted for uncertainty in both the frequency and consequences of accidents. Considerable uncertainty is tolerable in the frequency and consequences of accidents that are, beyond a shadow of doubt, not risk dominating, but Operators should present sensitivity studies that show their predictions for safety critical events are not seriously in error. Assessors can ask the following questions to test compliance with this criterion:-

Q: Has the uncertainty in consequences arising from different mathematical model input data been addressed?

The extent of a flash fire envelope and the volume of a congested plant enveloped by a cloud of alcohol vapour depends on the weather conditions assumed for the dispersion process. Since the magnitude of the hazard is inversely proportional to wind speed under both D and F stability, it is important that the consequences are evaluated at typical low wind speeds (F2 and D5). Input data for most other accident scenarios are fairly well defined, with the exception of emissive power. Assessors should check that values used in the accident consequence analysis are close to those shown in Table 5 and applicable to the local weather conditions experienced at the site location.

Q: Has the uncertainty in accident frequency been properly accounted for in the reliability of installed protective measures?

Particular areas of concern include ventilation rates of maturation warehouses, electrical circuits in warehouses, bulk storage facilities and the ability of bunds to contain spillages. The safety report should quantify uncertainties in the predicted failure frequency and factor these into the final risk assessment. Since road tanker hose failure is relatively common, it be essential that it is fully addressed in the safety report.

Q: Have the uncertainties attached to the risk calculations been addressed and justified?

A safety report that fails to mention uncertainties in the risk estimates should be considered deficient. Individual uncertainties attached to calculated hazard ranges should to be estimated by discussion of both model inadequacies and imprecise input data. The safety report should justify the results, if necessary by reference to confidence levels. Assessors can find uncertainty information in Table 6.

With regard to uncertainty in the reliability of containment and control systems, it is reasonable to assume that standards that have been developed over many years provide adequate protection. However, if a site makes use of new technology, for which an historical database is not available, then the safety report should discuss uncertainty attached to failure probabilities.

Operators who base their safety report on QRA, should take account of the potential for protective devices not to function e.g. remotely operated shut off valves and excess flow devices may fail to operate effectively when called upon. The Operator should recognise that other protective systems may also fail and should describe the measures in place to show that his ranking of risk is not seriously flawed.

Most risk assessments, even those not based on quantification, make use of a variety of input data which have uncertainties attached to them. Operators should describe the effect uncertainties can have on their predictions and demonstrate, by reasoned arguments, or quantitatively, that even under worst case assumptions the risks are ALARP.

Links to Emergency Planning

The conclusions drawn from the risk analysis with respect to emergency planning should be soundly based.

A safety report does not need to describe the off-site emergency plan, but it should provide guidance for the Local Authority on the severity of the risk dominant accidents. This information should be presented in an easy to assimilate form such as a table that summarises accident probability and likely numbers of casualties in three severity groups (mild burns or superficial injuries, hospitalisation and fatalities) for at least two weather conditions. It should also indicate the number of people likely to be made homeless by the effects of explosions. The information should be tabulated for a representative range of weather conditions and for all wind directions.

The safety report should also indicate any significant differences in the numbers of casualties due to seasonal changes, the accident occurring at week end, at night or on function days. In addition to the consequence information, it should present probability data in order that emergency planners can tailor their resources around the accidents presenting the greatest risk.

Of particular concern is whether the Operator will detect the occurrence of an escape of distilled spirit, either in a maturation warehouse or bulk storage area, and be able to take appropriate steps remotely to minimise its consequences. Assessors should be convinced that remote monitoring of all safety-related parameters is adequate and protected by redundant and diverse equipment appropriate to the level of hazard and risk.

Q: Does the safety report give the distances to a range of consequence levels of relevance to emergency planners?

In the event of a major accident the emergency services will want to know where to deploy their staff in order to bring relief to the maximum number of people in the shortest time. Depending on the accident, the consequences could be mainly down wind (flash fire) or isotropically distributed around the site (VCE if possible). In each case the maximum distance out to which people are likely to be injured is of vital importance.