HEALTH & SAFETY AUTHORITY

Guidance to Inspectors on the Assessment of Safety Reports

under the COMAH Regulations 2015

Rev. 4 Jan 2017

This document provides guidance to CCPS inspectors on the systematic examination and assessment of safety reports under the COMAH Regulations 2015. The examination is grouped into separate descriptive, MAPP & SMS, predictive, technical and emergency response elements. Criteria and sub-criteria are identified for each element which, if met, will allow the safety report to be accepted. If not met, they will assist the inspector in deciding whether further information is required or whether the safety report is so seriously deficient that it should be rejected and a new safety report required.

Guidance to Inspectors on the Assessment of Safety Reports

Table of Contents

Scope

This guidance is directed to all COMAH, Chemical Production and Storage (CCPS) Inspectors involved in safety report assessment.

It may be given to operators preparing safety reports for assessment but they should be reminded that it is the operator's duty to identify and characterise the major accident scenarios and appropriate risk-reduction and mitigation measures and this internal guidance document does not relieve them of that responsibility. It may be that information should be provided in relation to their particular establishment or immediate environment or relevant major accident scenarios that are not referred to in this document, so it should not be relied on by them as covering all the information that should be submitted in a safety report.

Operators should be advised that, to aid assessment, the report should be submitted as, at most, 2 documents.

Assessment Process

This document provides guidance on the assessment of safety reports under the *Chemicals Act (Control of Major Accident Hazards Involving Dangerous Substances) Regulations 2015* and is designed to be used in conjunction with the current safety report assessment forms. It is not exhaustive and professional judgement should be used in applying it to the assessment of any particular safety report.

In particular, the level of proportionality – the degree to which the demonstration of all necessary measures is required– should be decided very early in the assessment process. The assessor should always begin with a read-through of the report to get a 'feel' for where the relevant information may be found and the level of detail that is necessary.

The assessment of a safety report is conducted in relation to the following five distinct elements:

- *Descriptive,*
- *MAPP & SMS,*
- *Predictive,*
- *Technical,*
- *Emergency Response*.

For assessment purposes, each of these elements is divided into a number of assessment criteria.

Each criterion may in turn be divided into a variable number of sub-criteria for the purpose of detailed assessment: this is addressed in the detailed assessment forms.

The guidance covers all types of safety report assessment, including

- pre-construction,
- pre-operation,
- updates,
- 5-year submissions.

For new establishments, a pre-submission safety report assessment meeting should be arranged with the operator as soon as possible following a formal notification; this internal guidance can be made available to the operator at that meeting, with particular emphasis on the disclaimer under 'Scope'.

The Central Competent Authority will assess a safety report and issue conclusions within 4 months of receipt.

One of two possible initial conclusions can be communicated to operators. They are:

a) The CCA is satisfied the safety report meets the requirements of the COMAH Regulations at this time and no further information is required. The demonstrations in the safety report will be tested during subsequent COMAH inspections.
b) The CCA has determined there are omissions or significant omissions in the demonstration and further information is required (which will be specified in detail in a written communication to the operator, highlighting omissions, serious omissions and potential serious deficiencies).

Note: Under the Regulations, an operator is allowed this <u>one opportunity</u> to provide the further information, within one month from the date of the CCA request or within such longer period as the CCA may specify in writing. The CCA will issue a conclusion within 2 months of the receipt of the further information.

Following the receipt of the requested additional information, the CCA may either reach conclusion (a) above or reject the safety report as not meeting the requirements of the COMAH Regulations 2015, by reason of a serious deficiency of demonstration (a conclusion that can be reached where there are multiple significant omissions or a single serious deficiency), which will be set out in detail in a written communication to the operator, with specific reference to Regulation 11(1) and the requirements of Schedules 2 and 3. **There is no scope to request further information from the operator.** Under these circumstances, the operator will be obliged to submit a new safety report for full assessment and the process must begin anew.

An operator **cannot** begin construction, operation or increase the on-site inventory of dangerous substances to upper-tier thresholds until the CCA is satisfied with the safety report content and has issued a positive conclusion and permission. Inspectors should remind operators of this following the receipt of a notification.

Updates and 5-Year Reviews

Changes from the previously assessed safety report should be highlighted by the operator in a change log.

Where there have been so many changes in a safety report that it is not possible to draw up a change log, the safety report should be treated as new and assessed in full.

Five-year reviews should contain updated information on, for example, the physical establishment, the dangerous substances and their classification, the processes, the workforce location, the population and offsite environmental receptors. Updated maps may be necessary. Account should be taken of technical progress in the identification, management, prevention and mitigation of major accident hazards.

Measures to be implemented, which were identified in the previously assessed safety report, should be adequately addressed by the operator in the review and measures not implemented should be followed up by the assessor. Only selected criteria will need to be evaluated in a five-year review assessment, which will be at the judgement of the assessor and in line with the prevailing CCA policy at the time (In 2016 this requires a review of the predictive elements).

Pre-operation safety reports (POSRs)

Pre-operation safety reports (POSRs) must provide the details of the arrangements and conditions that will be in place when operation commences, so there should not be significant difference between the POSR and the operational safety report: if the POSR does not correctly identify the operational elements then an update would be required prior to operation. It should be made clear to the operator that advance notification is necessary for significant modifications as set out in Regulation 11(6) (c) and Regulation 12.

Significant Omissions and Serious Deficiencies of Demonstration

An omission in respect to one or more of the assessment sub-criteria is one where little or no information or no relevant information has been provided to allow the sub-criterion to be met.

Where one or more sub-criteria have not been met, the higher-level criterion is unlikely to be met. It is likely that at this point that a **significant omission** has been made by the operator.

A **serious deficiency of demonstration** in the safety report (not to be confused with a serious deficiency under Regulation 21(6), which has to be assessed as part of an inspection) will arise where any of the five demonstrations required by Regulation 11(1) cannot be made, because one or more significant omissions have been made, or where the data and information required by Regulation 11(2) has not been provided. However failing to meet some sub-criteria may, in itself, constitute a serious deficiency.

Example of significant omissions:

- Human factors have been taken into account in the risk analysis (Criterion 3.2) evidenced by the failure to do a risk analysis on the human factors causes that make a significant major accident contribution. A decision on the significance of this omission will depend on the weight given by the assessor to human factors in the prevention and mitigation of the identified major accidents at the establishment.

Whether the failure of the safety report to meet a single criterion constitutes a serious deficiency will depend on the particular criterion under assessment.

Example of serious deficiency of demonstration:

- A failure to meet criterion 3.5 – the information used to model major accident hazard scenarios was appropriate – would almost always constitute a serious deficiency of demonstration.

To aid in the assessment, criteria which, if not met on their own will constitute an omission, are indicated by a single * on this guidance. In a similar manner, those marked as ** could constitute a significant omission while those indicated by * could constitute a serious deficiency.**

The assessment process itself is a methodical one, assessing each element in turn in relation to the specified success criteria.

A full assessment will be made of the submitted safety report, even when a serious deficiency of demonstration is determined to be present early in the assessment process.

The reasons for reaching the assessment conclusion will be communicated in writing to the operator. This will give the operator a clear understanding of where the demonstration falls short and thereby allow the operator to focus on what has to be done within the short time available under the Regulations for the submission of further information.

Further information should be integrated into the safety report (which should be supplied as, at most, 2 electronic documents) but it should also be identified for the inspector so as to assist the assessment. This final assessment will examine only those criteria (or sub-criteria) identified as not having been met in the original letter to the operator.

1. Assessment of the Descriptive Elements

Pre-construction and pre-operation safety reports

Pre-construction safety reports and pre-operation safety reports should normally be able to provide details on all criteria in this section, though some revision may be required in pre-operation safety reports to reflect design development since the pre-construction safety report.

The description of the environment and surrounding population should reflect the expected conditions once the establishment becomes operational. Where commencement of operation is phased, the report should describe circumstances as they apply to each phase (including arrangements such as the use of temporary offices and buildings, inclusion of construction contractor populations, and so on).

Overview descriptions of the establishment, particularly where relevant to major accident hazards, emergency response, monitoring, and so on should be described to the extent that information is available at the time of submission of the report.

Descriptive Elements - Significant Omissions and Serious Deficiencies

Examples of significant omissions. A failure to:

- describe the surrounding environment sufficiently, so as to allow the consequences of a major accident to be assessed;
- describe the processes that could give rise to a major accident in sufficient detail;
- provide a dangerous substances inventory, classified in terms of CLP;
- describe the land use in the area surrounding the environment.

Example of a serious deficiency:

A failure to describe any preventive measures to control the major accident risks arising from the presence of a dangerous substance.

1.1 * Sufficient details have been provided to allow communication with the operator

The safety report must have included, as a minimum:

- the registered name of the operator;
- the trade name (if different to above) and address of the establishment (the trade name may be used subsequently in the safety report if the operator chooses);
- if the operator is a trading partnership, the names and addresses of all trading partners, together with the name and address under which the partnership operates;
- the name(s), address, telephone number and email address for contact(s) within the operator's organisation (for communications about the safety report);

- the names of relevant organisation(s) involved in the drawing up of the report.

1.2 ** The environment of the establishment has been described in sufficient detail to allow the consequences of a major accident to be assessed

Factual information describing the environment surrounding the establishment should have been provided. The surrounding environment consists of the natural environment over, below and around the boundaries of the establishment and includes the people in it. The extent of the area described should have taken account of the hazard ranges of the relevant major accident scenarios given in the safety report.

The information should have included a map showing the establishment and its surroundings to a suitable scale (usually at least as detailed as 1:10,000) and should have identified the consultation distance and public information zones.

The *consultation distance* is a distance advised to a planning authority, potentially for control of inappropriate development around an establishment. It is communicated from the CCA to the planning authority and copied to the operator. The consultation distance used to be obtained from a table in the Planning and Development Regulations but the COMAH Regulations 2015 now put the determination of this distance at the discretion of the CCA.

The *public information zone* (PIZ) is the area referred to in Regulation 25(4), which had previously been called the 'specified area'. An operator may propose such an area in the safety report. Under Regulation 25(8), the CCA will communicate the PIZ to the operator following the assessment of the safety report. Where risk-based generic advice for an establishment has been drawn up according to the CCA's published policy, the extent of the outer planning zone (the 1×10^{-7} contour) will constitute the PIZ.

The consultation distance is bigger than the PIZ; this allows very large or sensitive developments to be referred by a planning authority for technical advice, in areas below the 1×10^{-7} risk contour level.

The following areas should have been clearly indicated on the map:

- the land use pattern (such as, industry, agriculture, urban settlements, environmentally sensitive locations, and so on);
- the location of the most important buildings and infrastructures (such as hospitals, schools, other industrial sites, road and rail networks, jetties and so on);
- access routes to the establishment as well as the escape routes from the establishment and other traffic routes significant for rescue or emergency operations.

Separate maps may be required to identify the surrounding population and the surrounding natural environment.

The description of the surrounding population should have included:

- approximate numbers of residents;

- estimated number of people who may use the area (for example, those present at workplaces, attending a football match, religious service, entertainment event, tourists and so on);
- groups of particularly vulnerable people either on account of their sensitivity to the hazards in question (for example, schools, hospitals and nursing homes) or because their number present particular problems in evacuation.

Sufficient information should have been included to allow for the assessment of the indirect impact of a major accident on the public.

Examples of indirect impact of a major accident on the public:

- contamination of drinking water;
- loss of a public amenity following a major accident to the environment.

The safety report should have identified neighbouring establishments, as well as sites that fall outside the scope of the COMAH Regulations. In addition, areas and developments that could be source of, or increase the risk or consequences of a major accident and of domino effects should have been identified.

A description of the features of the surrounding environment that could influence the impact of a major accident should have been provided.

Examples of features of the surrounding environment (<u>only as it relates to major accidents</u>) that <u>may</u> be necessary to include:

- topography, if it could have an effect on the dispersion of toxic or flammable gases or combustion products (including valleys and hills, buildings and so on);
- historical local weather records including wind speed and direction, atmospheric stability and rainfall relevant to the behaviour of the released dangerous substances;
- the underlying and surrounding geology and hydrogeology;
- areas vulnerable to flood risk;
- surrounding water courses (under various flow conditions), underlying aquifers and any drinking water extraction points in relation to the dispersion of liquid contaminants or leachate;
- surrounding water and land quality, including details of local ecology;
- information on sewerage and rainwater systems, if they could be involved in the dispersal of contaminants off-site;
- information on tides and currents that might influence dispersion or accumulation (if marine or estuarine habitats are at risk);
- aspects of the surroundings that may hinder emergency response or mitigation measures.

The built environment around the establishment **vulnerable to the effects of a major accident** should have been identified.

Examples of information on the built environment that may be necessary:

- listed buildings or monuments;
- sections of infrastructure, such as major transport routes or utilities including electricity, gas, telecoms, water sewers and treatment plants relevant to major accident hazards.

The safety report should have identified and described all environmental pathways and receptors that could, in the event of a major accident, be affected by dangerous substances (a range of up to 10 km is considered to be reasonable – that is, if there are effects up to this distance, they should be described. If there are no effects beyond say 500m then no consideration beyond this distance is required).

Information on relevant environmental receptors that could be impacted should have been provided, for example:

- the presence of particular species;
- designated areas (SAC, SPA, SSSI, and so on);
- surface waters, including ditches, and their classification, the direction and rate of flow, extent of flood plains and depths of flood, tides and currents;
- groundwater and aquifers and their classification;
- the location(s) and discharge arrangements of third party service providers such as sewage or effluent treatment plants;
- drinking and industrial water abstraction points (ground and surface), and the extent of source protection zones;
- amenity areas;
- sites of architectural and historical importance;
- soil and sediment;
- agricultural resources (including market gardens and allotments).

Factors (such as hydrology, meteorology, geology, hydrogeology, topography, geography and climate) that could affect the behaviour of accidental releases in the environment should have been described. Surveys may be needed to determine the nature of local ecosystems.

The description of surface waters should have included information on direction and rate of flow, tides, currents and flood plains and their variability with different weather conditions, that is, those matters that might influence dispersion or accumulation in the aquatic environment.

Flood zone mapping should have been presented where the establishment has been identified to be in or close to a flood plain. This information is necessary in consideration of initiation of major

accidents and influence on pathways, escalation and emergency response (including dispersion of substances on- and off-establishment, and the ability to respond to an incident).

Activities beyond the establishment boundary that may interact with the establishment should have been identified including neighbouring industrial facilities; water treatment plants connected by rivers or sewer systems, and upstream processes.

Examples for consideration:

- spills from the establishment causing damage to connected facilities;
- combinations of released substances that may react to produce an environmental hazard;
- upstream processes transferring off-spec material leading to upsets on the establishment.

The history of the establishment and its environment should have been described if necessary (for example, where there might be an implication for a major accident to the environment (MATTE).

The nature of the receptor sensitivity should have been identified and related to the potential major accident hazards at the establishment (the most sensitive features may not be the highest designated sites or features).

1.3 ** The environment of the establishment has been described in sufficient detail to allow the contribution of external factors to major accidents at the establishment to be assessed

The physical environment surrounding the establishment that could have an influence on initiating events or could be an actual initiating event should have been described.

Examples of the physical environment that could influence initiating events:

- underlying geology (to allow the consideration of seismic events and subsidence as accident initiators);
- historical evidence of other external events such as flooding and extreme weather conditions including extreme temperature, rain, wind and lightning.

Other activities in the area surrounding the establishment that might lead to, or exacerbate, a major accident should have been identified.

Examples of surroundings or activities that might cause / exacerbate a major accident:

- other major hazard installations and pipelines in the area;
- any land-use under the establishment;
- air traffic movements near the establishment;
- transport activities such as shipping, major road or rail routes and associated dangerous substance movements;
- human activities such as arson, vandalism and criminal damage;
- high voltage overhead power distribution lines;
- radio transmission masts capable of interfering with safety control or communication systems or of initiating electro-explosive devices;
- wind turbines in very close proximity.

The operator should have identified in the safety report how natural events (for example, earthquakes, floods, high tides, elevated groundwater levels, high winds, high rainfall, cold conditions and so on), may initiate a major accident with environmental impact. Past accidents and historical evidence of other external events that might act as accident initiators or escalation factors such as flooding should have been considered.

The weather conditions that could initiate a major accident should have been identified and there should be a system to alert the operator of these circumstances and the response the operator plans to make if these circumstances occur.

1.4 * An overview of the establishment has been provided, particularly identifying those parts relevant to major accident hazards.

A descriptive overview of the establishment, its activities and processes should have been provided. In this context an overview is a general outline, without extensive detail, to set the context for the reader (P&IDs are not necessary to satisfy this criterion).

Examples of what might be included in the descriptive overview:

- the installations (and relationship between installations) in the establishment with an overview of the activities that occur there including the dangerous substances potentially present;
- the major accident scenarios in overview;
- the main measures for protection and intervention;
- the general security arrangements for monitoring access and detecting intruders.

In addition to the descriptive overview, a site map(s) (at least as detailed as 1:2,500 with a scale and direction indicator) should have been included to highlight important locations and information.

Examples of locations relevant to major accident hazards that could be identified on the map:

- installations with major hazard potential;
- other installations, including those without dangerous substances, with an outline in general terms of their activities;
- where the people are (for example, in control rooms, office blocks, canteens, security huts), taking into account foreseeable fluctuations (shift working, maintenance activities, contractors or visitors);
- critical activities that relate to the major accident scenarios (the activities themselves should be assessed in more depth in criterion 1.9);
- key abatement systems for mitigating the effects of major accidents, such as drainage and fire water retention facilities, gas cleaning or liquid treatment works, paved areas;
- key control (such as computer control) or isolation systems;
- roads, entrances to the establishment or other features, such as flares or other open sources of ignition;
- essential utilities relevant to the prevention / mitigation of a major accident;
- areas related to emergency response, such as fire water supply, escape routes, access routes used by emergency vehicles and critical communication systems;
- systems for monitoring and detecting toxic products in air, waste water or sewers;
- fire detection systems;
- areas with explosive atmospheres (ATEX zones).

The operator should have described in the safety report the aspects of the establishment that could be a factor in the potential for releases to the environment including:

- location, inventory and conditions of substances dangerous to environment (including non-COMAH substances which may be released in the event of a major accident);
- overview of primary, secondary and tertiary containment systems related to dangerous substances;
- site layout and drainage to include location of penstocks, barriers, valves, capacity and condition of drains;
- location and capacity of sumps, interceptors, fire water lagoons, effluent treatment plants (on and off site) and any other barriers to off-site transport of polluting matter;
- location of discharge points to watercourses / foul sewer / effluent treatment plants / soakaways;
- details relating to safety or environmentally critical valves, instruments, control loops and detection systems;

- monitoring equipment (for example, for toxic products in air, sewers, discharges to water; for fires or explosive atmospheres);
- geographical / geological / hydro-geological features that may impede/facilitate pollutant escape.

1.5 * The maximum quantity of every dangerous substance present (or potentially present) at the establishment has been identified

The safety report must show that the operator has quantified all the dangerous substances present at the establishment, which either meet the criteria laid down in Schedule 1 Part 1 or which are listed in Schedule 1 Part 2 of the Regulations. All dangerous substances should have been included.

Where dangerous substances have not been included in the inventory for tier calculations, the reason for their omission must have satisfied the requirements of Note 3 to Schedule 1 of the Regulations which states:

*"Dangerous substances present at an establishment only in quantities equal to or less than 2 % of the relevant qualifying quantity shall be ignored for the purposes of calculating the total quantity present if their location within an establishment is such that it **cannot act as an initiator** of a major accident elsewhere at that establishment."*

The dangerous substance should also not itself be able to cause a major accident!

The maximum inventories listed should have taken into account the maximum quantity that may be present due to fluctuations in business activity (average quantities are not acceptable).

The safety report must have provided evidence that all dangerous substances, which might be anticipated to be present at the establishment, have been quantified, including:

- raw materials, intermediates, finished products, by-products and wastes;
- dangerous substances produced during process excursions, or other unplanned but foreseeable events;
- dangerous substances which change classification in processing;
- dangerous substances present on road and rail vehicles within the establishment.

1.6 ** A dangerous substance list with chemical names, CAS numbers and names according to IUPAC nomenclature has been provided

Each dangerous substance (**to the extent that it is relevant to a major accident hazard**) should have been systematically named. The following information should have been provided for each dangerous substance or class of dangerous substance:

- the classification under CLP;
- the chemical name (for example, propane, butane) and where appropriate, its common chemical name (for example, LPG);
- the CAS number;

- the IUPAC system name;
- the concentration of any impurity or additive;
- the proportion of each constituent in a mixture, to the extent that they are relevant to a major hazard.

1.7 * The physical and chemical behaviour of each dangerous substance, relevant to both normal operating conditions and foreseeable accident conditions, has been described

Information should have been presented on the properties of the dangerous substances under normal storage and processing conditions and (if they are different) under process upset and foreseeable accident conditions.

Examples of operating conditions that may have to be addressed:

- process operating pressures and temperatures during start-up, regeneration, normal process operation, turnaround, shutdown or other designed mode;
- production of products, by-products, residues or intermediates as a result of normal operations or through foreseeable accidental conditions;
- behaviour of reactor fluids during and following a process upset;
- behaviour of stored materials under normal operation and following loss of utility (for example, refrigerated/heated/inerted storage);
- contamination of products;
- following loss of containment;
- inhibitor stability over time.

Relevant physical and chemical properties (**in so far as any of these are relevant to the major accident hazards**), including data on toxicology, should have been presented in a clear and concise form using appropriate and consistent units of measurement in the SI system.

Examples of physical and chemical properties that may be included:

- flash point;
- flammable range;
- ignition temperature;
- vapour pressure;
- density;
- boiling point;
- reaction data;
- decomposition rates;
- data on sensitivity of explosives.

1.8 * The immediate and delayed harms to human health and the environment have been identified for each dangerous substance

Often the information in the Safety Data Sheet will be unable to satisfy this criterion.

The information presented must have included the physical, chemical or toxicological characteristics of the dangerous substances that may cause harm (related to the major accident) and an indication of the hazards posed. The evidence presented should have addressed both the immediate and delayed effects.

Examples of evidence that may be included:

- hazards to health such as irritation, asphyxiation, cancer or genetic damage;
- lethal concentrations;
- harm caused by fire or explosion;
- effects on the built environment.

An indication of the hazards to the environment (both immediate and delayed) should have been presented including:

- environmental harm criteria (for example, LC_{50} data, critical loads);
- negligible effect criteria (for example, No Observed Effect Levels, Suggested No Adverse Response Levels);
- other potentially harmful properties (for example, BOD / COD, blanketing / smothering or effects on potable water supplies).

Information concerning the acknowledged acceptable limits of exposure to the effects of dangerous substances should have been presented taking account of concentration or any other relevant parameter. Appropriate references to scientific literature should have been provided where necessary to justify the harmful effects, hazardous concentrations and acceptable limits presented. Where information is not known, the significance of the lack of knowledge should have been evaluated and the policy for dealing with it should have been described.

1.9 ** The processes carried out within every installation that could give rise to a major accident have been described

Following on from the general overview description of the establishment under criterion 1.4, the safety report should have included descriptions of the following:

- the purpose of the installations relevant to major accident hazards;
- the conditions under which the dangerous substances are normally held;
- the physical and chemical changes to the dangerous substances arising from the designed purpose of the installation or plant;

- the physical and chemical changes to the dangerous substances arising from foreseeable deviations from the designed purpose of the plant;
- the discharge, retention, re-use and recycling or disposal of residues and waste liquids and solids, or the discharge and treatment of waste gases.

A basic Process Flow Diagram (PFD) should have been provided for each relevant process.

The safety report must have clearly identified plant and activities where a major accident could occur. It must have included a plant diagram / plan identifying:

- key control systems;
- reaction vessels;
- storage vessels;
- pipe-work systems;
- valves and significant connections;
- the location of activities where a major accident could happen (for example, storage in packages).

1.10 * Focused information about each installation has been provided in sufficient detail to support a demonstration that major accident hazards will be prevented or the effects mitigated

The demonstration referred to in this criterion is expected to be made under the section on predictive elements. The objective of this criterion is to establish that sufficient information on the installations has been provided to support that demonstration.

The operator must have included in the safety report focused information about all the installations that have major accident potential. For each one, there should have been a description in enough detail to determine the purpose, location and function of equipment, within the installation, that has a bearing on major accident prevention, control or mitigation.

The purpose of this focused information is to provide enough detail to enable an understanding of the operator's demonstration of safety. Therefore, safety reports should have provided descriptive information pertinent to the demonstration that will be made, at a level of detail appropriate for understanding the arguments presented.

The operator should have provided enough information to justify the subsequent demonstration.

The safety report must have contained plans, maps or diagrams with accompanying descriptions that clearly set out detailed information about the installations with major accident potential.

In particular, information about items of plant such as:

- vessels (for example, location, type, size, pressure, purpose, contents);
- pipe work systems (for example, routes, types, size, pressure, purpose);
- services (for example, steam, air, electricity, fuel, hot water);

- drainage (for example, routes, purpose (for example, foul water, firewater run-off) including details relating to safety (or environment) critical valves, instruments, control loops and detection systems and monitoring equipment;
- stacks, flares and gas cleaners (for example, location, purpose);
- fire-fighting and supply arrangements;
- monitoring equipment (for example, for toxic products in air, sewers, discharges to water; for fires or explosive atmospheres);
- incorporators, rolling mills, manual and power presses, sieves, granulators, mixers;
- zoning and hazardous area classification details.

Many of these will have already been assessed under criteria 1.4 and 1.9.

The safety report must also have included information about:

- the normal operating parameters of plant;
- the designed maximum working capacities, temperatures, and pressures;
- relevant qualitative and quantitative information on energy and mass transport in the process (that is, material and energy balances) in:
  - normal running;
  - start up or shut down periods;
  - abnormal operations.
- the locations of dangerous substances;
- an indication of the chemical and physical state, and quantity of the dangerous substance at each location.

2. Assessment of the MAPP/SMS Elements

Pre-construction and pre-operation safety reports

Pre-construction safety reports and pre-operation safety reports should have demonstrated adequate management of design, construction and commissioning processes prior to the introduction of dangerous substances. The operator should normally be able to provide a pre-operation safety report that covers the relevant Major Accident Prevention Policy (MAPP) and safety management system (SMS) requirements of the COMAH Regulations.

Plant design often undergoes considerable development before and during the construction period and effective management and communications interfaces between operator, contractors and subcontractors is required. Particular MAPP and SMS issues affecting pre-construction safety reports and pre-operation safety reports, as appropriate, include:

- change management (design management and change approval, document control, and so on) during construction and commissioning;
- competency of designers, construction teams, contractor teams;
- management of temporary arrangements or constraints during design, construction and commissioning;
- construction verification systems and commissioning controls, post commissioning checks;
- identification of key roles and responsibilities for management of major hazards;
- communications between operator, designers, construction personnel, commissioning personnel, the CCA and other affected parties;
- SMS review and revision process prior to operation.

Where there are significant gaps in MAPP and SMS content for a pre-construction safety report it may be acceptable and pragmatic to allow the information to be provided in the pre-operation safety report. However, significant gaps in required information for a pre-operation safety report should be strongly justified and accompanies by a revision plan, agreed between the CCA and the operator, to ensure the timely and satisfactory delivery of the missing content.

MAPP / SMS Elements – Significant Omissions and Serious Deficiencies

Examples of significant omissions for this element: a failure to

- include a copy of the MAPP in the safety report;
- describe an element of the SMS such as the change management process;
- explain how the MAPP will be implemented in terms of company structures and the existing management system.

Examples of a serious deficiency for this element:

- the SMS has not been described;
- there are a series of incomplete demonstrations indicating an uncoordinated approach to the SMS;
- the arrangements for systematic identification of major accident hazards and appropriate control measures have not been described;
- information provided in relation to planning for emergencies is inadequate.

General Comments on assessing this Element

The assessment criteria and supplementary guidance given in this section are intended to help generate a consistent approach to the assessment of:

- the constituent elements of a MAPP;
- the elements of a SMS required to implement the MAPP.

The MAPP should comply with the requirements of Regulation 10 and the principles set out in Schedule 2. The description of the SMS should have included the parts of the general management system that cover:

- the organisational structure;
- the roles and responsibilities of personnel involved in management of major hazards;
- the practices, procedures, processes and resources for determining and implementing the MAPP.

Schedule 2 to the Regulations describes the elements that should be included in the SMS that implements the MAPP. The safety report should have provided an overview of the general management arrangements for determining and implementing the policy concerning major accident prevention. Evidence should have been provided that the management risk-control systems which are important for preventing major accidents and limiting the consequences for human health and the environment have been put in place.

Not all of the assessment criteria will be relevant to every operator and establishment. However the onus is on the operator to demonstrate that the MAPP and SMS are adequate in the context of the major accident hazards at the site.

General Assessment Tests

The purpose of the MAPP assessment (and the assessment of the rest of the SMS) is to provide answers to 5 essential questions:

- does the safety report contain a MAPP?
- does the information in the safety report demonstrate that there is an SMS for its implementation?
- does the information provided in the safety report as a whole demonstrate that the MAPP and the rest of the SMS have been put into effect?
- does the information demonstrate that all necessary measures have been taken to prevent major accidents and to limit their consequences for people and the environment?
- does the assessment reveal any serious deficiencies in the measures taken for the prevention and mitigation of major accidents?

The SMS should not be assessed in isolation. The rest of the safety report should have described a series of outcomes that are themselves determined or influenced by the SMS. These include the technical descriptions and predictive elements. The assessment conclusions in relation to these should therefore be taken into account when deciding if the report demonstrates that the MAPP and SMS have been put into effect.

It is also important that the individual elements that make up the SMS are not considered in isolation from each other.

2.1 * The MAPP includes the following commitments and demonstrations:

(a) A commitment to achieve a high standard of protection for human health and the environment

The MAPP should include:

- a statement stating the operator's commitment to achieving high standards of safety and protection for human health and the environment
- an indication that the resources necessary to implement the MAPP will be made available.
- a reference that the COMAH Regulations 2015 and in particular that Regulation 7 will be complied with.

The MAPP should be set out in writing and included in the safety report. It should be signed by the most senior manager or managers with the authority for its implementation.

(b) A demonstration of the operator's overall aims and policies with respect to the control of major accidents and protection of human health and the environment

There should be a recognition in the MAPP and / or safety report that the nature of the operator's activities gives rise to major accident hazards to employees, contractors, visitors, members of the public and the natural and built environment and therefore that the operator has obligations to employees, neighbours and the environment.

The MAPP should have included statements explaining the operator's overall aims and action principles in relation to the control of major accidents and the taking of all necessary measures. Reference should be made to Regulation 7 and may be made to Regulation 10.

(c) A demonstration of the roles and responsibilities of management in ensuring the proper implementation of the MAPP

The MAPP should have described how the policy will be implemented in terms of company structures and the existing management system and in particular the individual and collective management responsibility for this.

(d) A commitment towards continuously improving the control of major accident hazards

A policy on the continuous improvement in the prevention and control of major accident hazards should have been included in the MAPP.

(e) A commitment to taking account of the principles set out in Schedule 2 to the Regulations.

A statement of commitment to achieving a high standard of protection for human health and the environment should have been included; this should be supported by including appropriate objectives under the MAPP elements set out in Schedule 2 which are summarised as follows:

- Organisation and personnel
- Identification and evaluation of major hazards
- Operational control
- Management of change
- Planning for emergencies

- Monitoring performance
- Audit and review

The MAPP should have shown that the operator has considered all the elements and made convincing commitments to achieving the stated aims, which should be realistic and appropriate for the establishment. A commitment to periodic review by senior management should have been included.

This sub-criterion is looking for policy statements only and further details will be required in subsequent sub-criteria.

2.2 ** It has been explained how the SMS fits in to the overall organisational arrangements

Regardless of which SMS model the operator may use, the safety report should have set out the detail on the SMS and how it fits into the overall management arrangements for the site. The safety report should have given an overview of arrangements for the management of safety and demonstrated that the operator's SMS fits in with the overall management system.

Safety management and, in particular, the management of major accident hazards should form an integral part of the operator's overall company management and organisational arrangements.

The safety report should have described the environmental management elements within the SMS.

2.3 ** Organisation and personnel

(a) It has been demonstrated that all necessary roles and responsibilities in the management of major hazards have been clearly allocated at all levels in the organisation

The SMS as described in the safety report should reflect the top-down commitment, environmental awareness and safety culture of the operator's organisation. It should have described how this is translated into the direct responsibilities of personnel involved in the management of major hazards at all levels in the organization.

Information that confirms that the control of major accident hazards is a management function should have been included with an explanation that safety and environmental professionals act in support of line management.

The operator should have included in the safety report, outlining the allocation of roles and responsibilities for all aspects of the management of major hazards from company directors, or senior executives, down to operatives and maintenance personnel. The SMS should include production and technical directors, site managers, operations managers, production personnel, process development managers, design teams, project managers, maintenance managers, personnel managers, training staff, safety professionals, environmental professionals, risk assessors, and so on where appropriate.

The operator should have identified in safety report the key managers and post-holders for each of the responsibilities listed below and shown that the responsibilities of everyone involved in the management of major hazards have been clearly identified:

- providing resources, including human resources, for developing, implementing and maintaining the SMS;
- identifying major hazards and assessing associated risks during the life cycle of the installation;
- ensuring that employees, contractors and others are aware of the major accident hazards and are competent in the systems for controlling them;
- designing new installations and planning modifications;
- identifying, recording and following-up corrective and improvement actions;
- controlling abnormal situations and emergencies;
- identifying relevant training needs, providing training and evaluating its effectiveness;
- implementing the key risk control systems necessary for the control of major hazards;
- coordinating implementation of the SMS and reporting to senior management;
- monitoring performance and carrying out audits and reviews.

(b) It has been demonstrated that the performance of people having a role to play in the management of major accident hazards is measured, that they are competent and that they are held accountable for their performance

Training and competence

The operator must be able to demonstrate that training needs have been identified for the individuals filling the roles identified above and that they have received adequate training to fulfil their roles and responsibilities in relation to the management of major accident hazards.

Responsibilities for management of major accident hazards must be made clear to the jobholder (for example, in job descriptions), and effective compliance checking arrangements for safety critical procedures / tasks should have been described.

In relation to providing and maintaining appropriate levels of competence[*], procedures dealing with the arrangements for the selection, recruitment, training and placement of employees and managers including contractors should have been set out ([*]the Safety, Health & Welfare at Work Act of 2005 states 'a person is deemed to be a competent person where, having regard to the task he or she is required to perform and taking account of the size or hazards (or both of them) of the undertaking or establishment in which he or she undertakes work, the person possesses sufficient training, experience and knowledge appropriate to the nature of the work to be undertaken).

The operator should have referenced in the safety report any formal personnel performance review and appraisal systems[**] that set objectives relevant to the control of major accident hazards, measure the extent to which objectives are achieved and identify procedures for corrective actions if objectives are not reached ([**]actual performance appraisal records are not required to be included in the safety report). Information about procedures for identifying and taking action on failures to achieve satisfactory performance should have been provided.

The safety report must have shown that the operator has a system for providing and maintaining appropriate levels of management and employee competence. Summaries of arrangements for setting performance standards and targets for line managers should have been included.

It should have been demonstrated that safety personnel report to an appropriate management function and level.

The safety report should have referred to the arrangements for identifying the competence and training needs of all those having a role to play in the control of major accident hazards, including their deputies, from directors or senior executives, down to operatives and including contractors and their employees. Training assessment should be performed as appropriate to determine effectiveness and refresher training carried out as necessary.

Supervision and behavioural safety

The on-site arrangements for supervision of operational and maintenance teams should have been described, for example:

- competence standards have been defined for supervisory personnel including:
  - non-technical skills (leadership, managing poor performance, communicating effectively);
  - technical skills (relevant to the plant and process);
  - management of organisational performance influencing factors within their control (competence assurance, workload, staffing levels, shift work, fatigue);
- supervisory roles and responsibilities have been clearly defined in the context of major hazards and managing compliance with safety critical rules and procedures;
- where appropriate, the limitations of self-managed teams (poor leadership, poor communication external to the team) are acknowledged and addressed.

Where applicable, the limitations of behavioural safety programmes should have been acknowledged, for example:

- a potential bias towards personal injury rather than low probability / high consequence events;
- a tendency to focus on the behaviour and performance of front-line personnel, rather than management.

(c) It has been demonstrated that there are systems for ensuring employees are actively involved in the control of major accident hazards

The safety report should have contained summaries of systems that secure the continued participation, commitment and involvement of employees at all levels. This might include how the workforce is involved in consultative bodies, health, safety and environment committees, safety circles and safety teams.

Descriptions of how the organization encourages and supports employee or safety representatives should have been outlined.

Arrangements for upward reporting of information relevant to the control of major hazards must be addressed.

Examples of employee involvement:

- in HAZOP or risk assessment studies;
- setting standards relevant to the control of major accident hazards;
- devising, reviewing and revising operating and emergency systems, procedures and instructions for the control of major accident hazards;
- the design and procurement of new equipment including the human machine interface to ensure human factors and usability are taken into account;
- accident / near miss investigations;
- audit and review activities.

(d) It has been demonstrated that sufficient resources have been allocated to implement the MAPP

The operator should have included in the safety report brief explanations of how the overall management of major accident hazard resources (including personnel, equipment and finance) are determined and allocated (including arrangements to be implemented following a major accident).

In addition, the process used to determine and maintain the minimum staffing levels required to deliver the necessary measures under all foreseeable operating conditions should have been described. This includes:

- the full range of normal operations (for example, start-up of continuous processes) and maintenance operations (including turnarounds where relevant);
- how staffing arrangements affect the reliability and timeliness of detecting, diagnosing and recovering from major accident hazard scenarios.

Where staffing arrangements have been formally assessed using recognised models, the methodology should have been described.

Explanations of systems for identifying absences of key personnel and arranging competent cover should have been included.

The operator should have demonstrated that an adequate level of supervision is maintained and that personnel are competent to carry out their roles.

The arrangements for detecting, assessing and addressing workloads which are either too high or too low should have been described.

It should have acknowledged that fatigue may result in slower reactions, reduced ability to process information, memory lapses, absent-minded slips, lack of attention and so on. The safety report should have described:

- the framework for managing fatigue using appropriate standards and good practice including:
  - a policy that specifically guards against fatigue by addressing shift patterns, working hours, overtime, and so on;
  - guidance on shift roster design that takes account of shift types, shift length, rest periods, rotation and social factors, and so on;
  - consideration of environmental factors (for example, temperature, noise, ventilation, lighting in control rooms);
  - systematic assessment of changes to working hours and shift patterns;
  - arrangements to set, record, monitor and enforce limits and standards for working hours, overtime, on-call working, shift swapping, and so on);
  - arrangements to capture / monitor relevant data for contractors who carry out safety critical tasks;
  - arrangements to educate personnel and contractors in fatigue risks and sleep management and to report fatigue problems.

Detail of the arrangements for securing financial resources to meet the demands of any improvements or upgrades that may be identified by the risk management process should have been provided.

2.4 *** Identification and evaluation of hazards – it has been demonstrated that there are arrangements for systematically identifying major accident hazards, assessing the risks arising from normal and abnormal operations and determining necessary control measures

To note, there may be some overlap here with relevant criteria in the predictive elements section.

The operator should have described in the safety report the arrangements for systematic identification of major hazards, risk assessment and determination of necessary control measures. These arrangements should include references to procedures for identifying and evaluating the major accident hazards arising from the operator's activities and from the substances and materials purchased, stored, processed or produced.

Outlines should have been included of the operator's arrangements for determining the skills and knowledge required and, where appropriate, the team approach needed to provide the necessary range of theoretical and practical knowledge to implement appropriate hazard identification and risk assessment procedures.

The formal hazard identification and risk assessment techniques (e.g. HAZOP, FMEA, and so on) used at each stage of the life cycle of the process plant or storage facility should have been explained including:

- selection of the site and the siting of buildings within the establishment;
- plant and process design and modification, including historical reference to HAZOPs and other methods of risk assessment used at the time the plant/processes were designed. (*Hazop Guide to Best Practice*, IChem E. 3rd Ed, 2015);

- construction, installation and commissioning;
- start-up, steady state running and shutdown under normal and abnormal conditions;
- routine and non-routine maintenance;
- incidents and possible emergencies including those arising from component or materials failure, external events, human factors and failures of the SMS itself;
- decommissioning, abandonment and disposal.

The safety report should have referenced the techniques used to identify the hazards and assess the risks arising from external factors such as:

- abnormal temperatures, fire, lightning strike, seismic activity, wind, subsidence and land slip, flood, aircraft and projectile impact;
- transport, civil engineering and lifting activities;
- neighbouring activities;
- malevolent or unauthorised action including trespass.

An explanation of the formal hazard identification and risk assessment techniques used to provide continuing review should have been included (e.g. PHR, PHA etc.)

The safety report should have provided a description of the operator's arrangements for risk assessment to take account of human factors including human behaviour and reliability and the potential for human error in relation to safety critical activities.

It should also have included descriptions of how the outcomes of hazard identification and risk assessment have been used to determine the physical control measures and management risk control systems needed for the prevention and mitigation of major accidents.

2.5 ** Operational Control

(a) It has been demonstrated that there are procedures and instructions for safe operation, including maintenance, of plant, processes, equipment and temporary stoppages

The operator should have described in the safety report the risk control systems for controlling the risks which arise at each stage of the life cycle of the plant, processes or storage facilities in question including:

- construction and commissioning of plant, processes, equipment and facilities;
- operation of plant and processes (including as appropriate, start-up, steady state running, normal shutdown, detection of departures from normal operating conditions and responses to them including emergency shutdown and temporary and special operations);
- alarm management;
- temporary stoppages;
- safe operation under maintenance (for example, permit to work, hot work, confined space entry);
- selection and management of contractors;
- Inspection, test and maintenance of plant, equipment and facilities;

- identification of safety critical items of equipment;
- decommissioning of plant, processes, equipment and facilities;
- all safety related procedures (a list only should be included);
- scheduling necessary improvement works relevant to the control of major accident hazards.

(b) A commitment to implement best practice for monitoring and control of plant, processes and equipment with a view to reducing the risk of failure has been demonstrated

The safety report should have set out the operator's policy on reducing the risk of systems failure including detail on the management and control of the risks associated with ageing equipment and the corrosion management policy. It should have been demonstrated that there is an inventory of the equipment installed in the establishment and a strategy and methodology for the monitoring and control of the equipment including a system of follow up and managing corrective actions to 'close-out'.

(c) It has been demonstrated that there is a system(s) for prioritising the achievement of the objectives of the MAPP and for scheduling necessary improvement work in relation to the control of major accident hazards

The safety report should have indicated how priorities are decided i.e. based on considerations of hazard or risk.

Explanations of how improvement work relevant to the control of major accident hazards is scheduled, how the work is resourced, co-ordinated, allocated to individuals or teams to carry out and how timescales for completion are set should have been outlined.

2.6 *** Management of Change – it has been demonstrated that there are procedures for the design of new installations, processes or storage facilities and for modifications to them

The safety report should have described the operator's system for planning and controlling all changes in staffing levels, people, plant, processes and process variables, materials, equipment, procedures, software, design and, where appropriate, external circumstances (for example, fire water, neighbours, and so on) which are capable of affecting the control of major accident hazards.

The safety report should have described the systems for ensuring modifications are adequately assessed, designed, installed and tested.

Modifications to a process and its associated equipment, to structures or to operations and procedures, which could affect the safety of the installation, must be subject to a formal modification system: this includes plant, equipment and software.

Decommissioning of facilities should also be addressed.

Systems of management for the control of modifications must be clearly addressed as part of the SMS, outlining responsibilities, risk assessment and reduction, construction considerations, testing, commissioning and documentation.

The operator's management of change system must address permanent (including new plant or process), temporary and urgent changes.

Descriptions of the management of change system should have been outlined, as appropriate, including how:

- decisions about what constitutes a significant change are made;
- change has been defined;
- responsibilities for authorising and initiating change have been allocated;
- proposed changes are identified and documented;
- safety and environmental implications of proposed changes are identified assessed, and prioritised;
- safety and environmental control measures deemed necessary as a result of change, including provision of information and training and amendment of procedures are defined, documented and implemented (for example, P&IDs are updated);
- post-change checks and reviews are carried out and corrective actions are implemented.

Management of organisational change

The operator should have recognised in the safety report that subtle changes to organisations (for example, reducing staff numbers, combining departments, introducing self-managed teams, and so on) can have a significant impact on the management of major hazards.

It should have been demonstrated that there is a clear policy and procedure which:

- is framed around recognised good practice;
- sets out guidelines on timing the implementation of changes (so that there is sufficient time for consolidation; staggered to avoid too many simultaneous changes);
- explains the assessment process, considering risks and opportunities resulting from the change as well as risks arising from the process of change;
- describes how personnel and contractors will actively participate before, during and after the change;
- explains how all safety-critical tasks and key major hazard responsibilities will be identified and successfully mapped across to the new organisational structure;
- describes how staffing levels will be formally assessed pre- and post- change;
- makes clear links to associated organisational performance influencing factors (workload, fatigue, and so on);
- explains arrangements to ensure training, support and supervision for staff with new or changed roles will be provided and to ensure there is adequate planning for competent cover during the training period;
- where roles and responsibilities are outsourced, explains how intelligent customer capability will be retained;

- explains arrangements for a full review to be undertaken prior to 'go-live'; and how performance should be monitored post-change.

2.7 *** Planning for Emergencies – it has been demonstrated that there are arrangements to identify foreseeable emergencies by systematic analysis and to prepare, test and review emergency plans and to provide specific training for all persons working in the establishment.

To note: planning for emergencies may be addressed at a high level in this section, and in more detail under Element 5

The operator should have demonstrated that on-site emergency plans have been drawn up in order to take all necessary measures to limit the consequences for human health and the environment of the foreseeable emergencies that could occur.

The safety report should have described the operator's procedures for systematically identifying the foreseeable emergencies and the planned response to such emergencies.

In addition, the procedures for preparing, reviewing, testing and keeping up to date emergency plans, at suitable intervals of no longer than three years should have been outlined.

The operator should have shown that likely human behaviour and response under emergency conditions has been taken into account, in the development of emergency plans.

It should also have been shown that arrangements to provide realistic training and preparation for all those likely to be involved in the response to an emergency are in place along with arrangements for communicating plans to all those who may be affected by an emergency.

2.8 *** Monitoring performance

(a) It has been demonstrated that there is a proactive means of safety performance measurement which provides information on whether the measures taken to guard against major accident scenarios are operating as intended and complying with the objectives of the MAPP

Regulations 10 and 11 and Schedule 2 (vi) impose a mandatory requirement for safety performance indicators. (*Developing Process Safety Indicators* (HSG 254) provides excellent guidance on this topic).

A description of the process relating to performance measurement should have been outlined including:

- identification of key risk control systems necessary for the control of major accidents;
- development of means by which the performance of key risk control systems can be monitored;
- setting of indicators which provide information on whether those key risk control systems are operating as intended;

- tolerance levels set against each indicator;
- reporting to senior management on a routine basis;
- involvement of senior management in the setting and reviewing of performance indicators and tolerance levels;

It is not expected that performance indicators are set against all elements of all risk control systems on a complex installation, or that collection and analysis of data should be unnecessarily resource intensive. Neither is an overload of indicators required. It is important to have manageable number of carefully selected and targeted good quality indicators, to provide assurance across the whole business. Typically, the safety report may have included examples of the types of process safety performance indicators measured, a summary of significant findings and how senior management acted upon those findings.

(b) It has been demonstrated that there is a system for reporting major accidents and near misses, particularly those involving failure of the protective measures for control of major accident hazards

The safety report should have described the operator's arrangements for reporting major accidents, incidents and near misses. The operator should include descriptions of arrangements to produce 'lagging' performance indicators and report to management. The following elements should have been recognised:

- major accidents as defined in COMAH;
- other relevant injuries and causes of ill health;
- other significant events leading to loss or environmental harm;
- incidents, including individual behaviour, with the potential for harm or loss or environmental damage, particularly those with the potential for major accidents;
- hazardous conditions, including process deviation or loss of containment.

The safety report should have referred to Schedules 6 and 7 of the COMAH Regulations which set out the criteria for notifiable accidents and incidents.

(c) It has been demonstrated that there are mechanisms for investigation and taking corrective action in cases of the proactive performance measures showing a deterioration in risk control measures and in relation to any incident or event with the potential to cause a major accident

The safety report should have described the operator's systems for investigation to determine the immediate and underlying causes of failure. It should have been demonstrated that this information is used to determine the necessary corrective actions. The arrangements for both active and reactive monitoring should have been described.

Examples of activing monitoring measures:

- arrangements for identification;
- inspection and test of critical plant, premises, equipment, control systems and instrumentation;
- assessment of compliance with training, instructions, safe operating procedures and working practices important for the prevention and mitigation of major accidents.

Examples of reactive monitoring measures:

- arrangements for accident, near miss and incident reporting;
- arrangements for accident, near miss and incident investigation.

Investigation procedures should include:

- investigation initiation (can be based on of failures identified through either the active or reactive performance monitoring systems);
- early evaluation to identify immediate risks;
- taking prompt action on immediate risks;
- decisions made on the level and nature of investigation based on considerations of potential rather than actual outcome;
- determining the immediate causes;
- determining the underlying human and management-related causes;
- trending of information collected through investigation, to highlight common or wider problems in the prevention and mitigation measures;
- reporting to senior management and action by them.

Both active and reactive monitoring systems should ensure that all circumstances surrounding the failure, including human factors, are considered.

Example of information that could be included to demonstrate human factors are integrated into an investigation:

- the investigation is clearly defined (procedures, checklists) so that investigators are encouraged to determine why human failures occur;
- a systematic approach is adopted (for example, investigations follow a path similar to human failure analysis in reverse);
- immediate causes (active human failures) as well as latent human failures (for example, decisions remote in time and place from the incident) are addressed;
- contributory factors are identified at job, individual and organisational levels.

2.9 ** Audit and review of the MAPP and SMS – it has been demonstrated that there is a review process which uses information from performance measurement and audit to facilitate the update of the MAPP and SMS

Audits are necessary to ensure that the operator's organisation, processes and procedures as defined and, as actually carried out in practice, are consistent with the SMS, and that they are effective. To ensure that their assessment is objective, audits must be carried out by people who are competent and sufficiently independent of the operational management of the unit being audited.

The safety report should have described the arrangements for ensuring that the operator's management activities, risk control systems and physical controls for the prevention and mitigation of major accidents, are assessed periodically by independent auditors.

The descriptions should have included an explanation of the audit system which the operator has adopted including the purpose, responsibility, resources, audit plan, audit protocols, procedures for reporting and follow up on recommendations of the audit. Typically, the safety report may include a copy of an audit plan and an example of a completed audit.

Review is an essential process for determining if the SMS is appropriate to fulfil the operator's MAPP and the objectives set within it. It may involve considering whether the MAPP and objectives should themselves be modified. Review is necessary for determining required improvements to management systems, physical controls or the MAPP itself. The safety report should have summarised the operator's arrangements for carrying out reviews, explaining who carries them out, when they are carried out and how they are carried out.

Information from performance measurement and auditing needs to be adopted by the operator. Therefore senior management should be involved in audit review and in the consideration of the results of performance and audit, along with consideration of the suitability of the actual procedures and arrangements for performance measurement.

The way corrective actions are decided and responsibilities assigned must be addressed. The operator should have demonstrated that results of reviews are communicated within the organisation. Any system of updates to the MAPP or SMS must include a review by senior management.

The safety report should have indicated that results of audits and reviews are documented and published within the organisation.

2.10 *** It has been demonstrated that there are arrangements for communicating and co-operating with, and securing the co-operation of, other organisations

The safety report should have outlined the operator's arrangements for co-operation and communication with organisations external to the operator who may have key roles to play or may be able to provide information (such as change in legislation, technical standards or information on accidents in similar sites), necessary for the prevention and mitigation of major accidents. This should include operators of other establishments which might be affected by the major accident hazards and contractors and their employees.

External organisations include:

- neighbouring establishments / other operators or companies;
- contractors and their employees;
- local emergency services;
- authorities responsible for preparation and maintenance of EEPs;
- enforcing authorities and professional bodies;
- employer associations / industry associations;
- local authorities or other relevant bodies.

The safety report should have described the arrangements for supplying the information required under Regulation 25(4) to those people and institutions off-site liable to be affected by a major accident.

It should have been demonstrated that there are systems for gathering information from external sources necessary for the control of major accident hazards. This should include descriptions of the arrangements for communicating changes in legislation, developments in technical standards and management practices and information on incidents with major accident potential occurring elsewhere in the world.

2.11 * It has been demonstrated that there are arrangements for communicating information, important for the control of major accident hazards, within the operator's organisation

The safety report should have identified the arrangements for the effective communication of issues relevant to the MAPP– be it through written communications, visible behaviour or through face to face discussions. The process of communicating the MAPP should have been demonstrated, for example:

- meaning and purpose of the MAPP;
- visions and beliefs which underlie the MAPP;
- commitment of senior management to the implementation of the MAPP;
- plans, standards, procedures and risk control systems relation to implementation and measurement of performance;
- comments, suggestions and ideas for improvement;
- performance monitoring and auditing activities;
- lessons learned from accidents and other incidents;
- shift handover and other critical communications.

The safety report should have outlined the arrangements to demonstrate line managers' commitment to the MAPP through their visible behaviour, for example, participating in safety meetings, accident investigations and participating in active monitoring activities.

Written communication relevant to implementation of the MAPP might include documentation of:

- roles and responsibilities of relevant personnel;
- procedures and instructions for safe operations;
- information on safety performance;
- safety meetings;
- shift meeting where employee feedback is obtained.

Example of arrangements for communicating information at shift handover:

- the standard / procedure for shift handover which has been implemented;
- support equipment which is provided (structured written or electronic logs);
- allocation of time for incoming and outgoing shifts to discuss plant status face-to-face;
- arrangements to minimise distractions during handover;
- arrangements to schedule maintenance within shifts, or control maintenance work that crosses shifts.

Example of arrangements for remote communications:

- remote communication equipment (for example, radios, intercoms, intranet) is suitable and reliable;
- users are competent in the use of equipment and associated radio protocols.

3. Assessment of the Predictive Elements

Predictive Elements - Significant Omissions and Serious Deficiencies

Examples of significant omissions for this element - a failure to:

- set out the approach to risk assessment;
- take account of human factors in the risk assessment;
- provide an appropriate risk analysis (i.e. not a poorly documented or sparsely detailed risk analysis or one that appears over-optimistic);
- provide sufficient information to enable the assessor to use the source terms for verification;
- use appropriate and realistic failure frequencies, reliability data or response times.

Examples of serious deficiencies for this element - a failure to:

- identify all potential major accidents;
- provide clear criteria for eliminating identified major accidents from further consideration;
- carry out a suitable and sufficient analysis of the local consequences of a major accident;
- demonstrate the risks are sufficiently low;
- draw appropriate conclusions from the risk analysis for emergency response planning.

General comments on assessing this element

The assessment of the predictive elements of the safety report follows a logical pattern. The information to satisfy the criteria may be in one section of the safety report or scattered throughout **and some information will contribute to satisfying more than one criterion**. As a result there may be some repetition of the information that is required by the criteria of this section.

Risk analysis and risk assessment are terms that are used quite a lot in relation to predictive elements, sometimes inter-changeably, and it is worth noting the difference at the outset.

According to IEC 31010:2009, risk assessment includes the elements of risk identification, risk analysis and risk evaluation. Risk identification is the process of finding and recognising risks and includes the process of hazard identification. Risk analysis consists of determining the range of consequences and probabilities of identified events and the effectiveness of existing controls. The methods used may be qualitative, semi-quantitative or quantitative. Risk evaluation is the process of

comparing estimated risk levels with pre-defined tolerance criteria to inform decisions. For the operator, risk evaluation will be about evaluating the risks that have been identified and analysed to determine whether they are tolerable.

The assessor should always begin with a read-through of the report to get a 'feel' for where the relevant information may be found.

The first predictive element criterion is designed to assess whether the operator has set out the approach to risk assessment that will be followed in the safety report. This is necessary in order for the assessor to be able to put the subsequent assessment in context and judge subsequent criteria. **Failure to set out the approach to risk assessment should be regarded as a serious deficiency**.

Human factors play a role in all major accidents and the operator should have systematically addressed this in the safety report and this is assessed by predictive element criterion 3.2.

The third predictive element criterion requires that all major accidents have been identified. The identification of major accidents should have been carried out in a systematic way, using recognised and appropriate methodology.

For many establishments, the number of major accident scenarios identified may be too large for each to be examined in detail in the safety report. Therefore it is permissible for the operator to reduce those in the safety report to a representative and manageable number; how the operator has gone about this is addressed by predictive element criterion 3.4.

As the operator progresses to demonstrate the detailed risk analysis, the information that is used must be suitable and predictive element criterion 3.5 addresses this. So high risk and high consequence scenarios should have been chosen and when the consequences are being evaluated, appropriate source terms and modelling conditions should have been used.

The likelihood or probability of the initial loss of containment occurring should have been addressed, or for operators providing a more qualitative analysis, the conditions under which the accident could occur: this is assessed by predictive element criterion 3.6.

The operator will have (or will commit to having) various measures or barriers in place that will reduce the likelihood of the loss of containment identified under predictive element criterion 3.6. The reliability of these measures, whether they can prevent the major accident from progressing, how reliable they are, whether the time for them to become effective is reasonable are all addressed by this criterion.

The next predictive element criterion (3.7) checks that, taking account of the local circumstances, the consequences of the identified major accident scenarios have been appropriately set out. How will human health and the environment be affected? Have the appropriate harm levels been chosen?

In the penultimate predictive element criterion (3.8), the significant question, which will build on all the previous criteria, is asked: does the operator demonstrate that the risks are sufficiently low – in other words have all the necessary measures been taken (or be about to be taken)?

The final predictive element criterion (3.9) seeks confirmation that the information in the safety report is suitable for the internal emergency plan and for the local competent authorities (LCAs) to draw up the external emergency plan (EEP).

Overall, the risk assessment should have assessed the risks to people, both on and off-site, and the risks to the environment.

Although the risk assessment is central, it is important that the safety report highlights the safety culture of the operator and does not solely focus on the risk assessment, which in many cases will have been led and written by an outside safety expert.

The CCA is unequivocal in the view that the safety report should be owned by the operator, because it is the operator that bears the legal responsibility to manage the risks. Operators are expected to be familiar with their safety report and to use it as a living document for the management of the major accident hazards. This aspect can be pursued in subsequent routine inspection.

Proportionality is key to the assessment of this element: the depth of the analysis in the operator's risk assessment should have been proportionate to:

- the scale and nature of the major accident hazards presented by the establishment;
- the risk posed to neighbouring populations and the environment.

A view on 'proportionality' in relation to the predictive elements should be taken at the start of the assessment process for this element. A core judgement to be made will be whether the risk analysis requires a quantitative approach. Sometimes a semi-quantitative or even a qualitative approach will be sufficient.

Examples of where qualitative or semi-quantitative analysis may be sufficient:

- A simple site remote from population and sensitive environments with a single dangerous substance of limited hazard may require only a simple qualitative risk analysis as the basis on which to demonstrate that the necessary prevention and mitigation measures are (will be) in place.
- A simple plant with a total inventory of 30 tonnes of chlorine and remote from population and sensitive environments may only need to demonstrate compliance with published guidance / standards for the safe handling of chlorine, with supporting statements to demonstrate that the risks to people off-site and the environment are sufficiently low.

Where the qualitative route has been taken, the operator should have demonstrated that all major accident hazards have been identified, that their extent and severity have been assessed and that all necessary measures are being taken. Quantification of the possible consequences will be required in every case to help the LCAs to develop EEPs.

Examples where a quantitative risk analysis may be necessary:

- a site in a populated area;
- an establishment with a large on-site population;
- a complex pharma-chemical site with many processes and several hazardous materials in the vicinity of population and sensitive environments.

Before getting deeper into risk quantification, operators should have considered hazard elimination and the adoption of inherently safer design. Good practice should be in place: where relevant good practice has not yet been fully established, operators would be expected to apply risk-reducing measures in the short period until it is established.

In evaluating the outcome of the operator's risk analysis, the concept of risk tolerability is an important element for consideration. The HSE ALARP[1] concept is widely used as a means of demonstrating risk tolerability.

In the ALARP approach, the operator should have:

- demonstrated that the risks to people are negligible (the risk of fatality of an individual is less than 1×10^{-6}/year) or
- demonstrated that the risks of individual fatality are greater than this but less than 1×10^{-3}/year (1×10^{-4} offsite) and are therefore tolerable, provided they are as low as reasonably practicable (this is the ALARP region).

If the risks are greater than $1 \times 10^{-3/4}$/year they are intolerable and a site inspection is warranted and a subsequent prohibition of activity may be necessary.

In rare cases, a societal risk assessment may be necessary to demonstrate that risks are sufficiently low; where there are credible accidents with the potential to cause a large number of fatalities this should be addressed by the operator in a societal risk analysis. Societal risk implications may be very important at the Intolerable/ALARP boundary and a societal risk assessment may be required if the individual risk level is close to the boundary.

For environmental risks, a similar approach can be taken although it is more common to demonstrate that there is no pathway to environmental receptors, usually through the use of suitable containment systems. Failure of containment systems should be addressed in the safety report. The Guideline on Environmental Risk Tolerability for COMAH Establishments (by CDOIF[2]) sets out a comprehensive approach to evaluation of the tolerability of MATTEs.

The decisions on whether the risks are sufficiently low (and whether all necessary measures have been taken) are made by exercising professional judgement on whether the residual risks (after implementing the risk-reducing measures that have been identified as necessary) are reasonable when set against the technical possibilities for further risk reduction and the cost of such risk-

[1] http://www.hse.gov.uk/risk/theory/alarpglance.htm
[2] http://www.hse.gov.uk/aboutus/meetings/committees/cif/environmental-risk-assessment.pdf

reduction measures. Some operators have adopted this approach and defined their own risk tolerability bands (in some cases more stringent risk criteria are set for new plant - typically an order of magnitude lower than the band for an existing plant).

This implies that existing control measures should be periodically reviewed to ensure they are properly applied and still appropriate. This will depend on technological progress, changes in society's perception of the particular risks, changes in understanding of the risk analysis, the uncertainty attached to the risk estimates and new lessons from accidents and incidents etc. Such reviews should figure prominently in safety report updates (see Regulation 11).

In any case, the criteria that have been used to judge if the risks are tolerable should have been set out. The assessor should be able to judge if the criteria are appropriate (using the HSE ALARP approach, as described above, as the benchmark) and to judge whether operators have demonstrated compliance with their own criteria in the safety report.

Some of the risk analysis material concerning the impact on the natural environment and human health may already have been documented for other purposes and it may be possible for the operator to reuse some of this information. It is not necessary to repeat the work but the original documentation must have been clearly referenced and, normally, copies of the appropriate parts of it attached to the safety report.

3.1 ** The operator's approach to risk assessment has been adequately described.

The operator should have included in the safety report a summary of the methods used for hazard identification and for risk analysis as well as the criteria used to judge the significance of the residual risks when control measures have been implemented.

In the first place, having identified all the relevant hazards using an appropriate method, a means of eliminating hazards should have been considered, then reducing the event likelihood and finally mitigating the associated consequences.

The safety report must have included a summary of the method(s) used for the risk analysis, which could be either qualitative or quantitative (a view on proportionality must be made by the assessor here).

All operators will be required to have employed a systematic method of hazard identification.

If a non-quantified approach has been taken because the risks are low or simple to evaluate, the basis for demonstrating that the residual risks are both tolerable and ALARP should have been given. One or more of the following may be acceptable, if supported by well-reasoned argument:

- industry standard good practice;
- regulatory guidance;
- industry association guidance.

However this will very much depend on local circumstances. Good practice may not be enough to make the risks tolerable and satisfy the overall requirement that all necessary measures are being taken.

If a quantified risk analysis (QRA) has been carried out, the following approach should have been presented:

- extent of the analysis to be conducted (plants/processes assessed);
- method to identify major accident event sequences (e.g. Hazard and Operability Studies – HAZOP or other systematic method);
- how the consequences of the accidents will be identified in clear terms;
- the source for the appropriate failure rates (identified from reputable sources);
- analytical approaches to be used in more complex situations (event tree analysis (ETA), fault tree analysis (FTA), failure mode and effect analysis (FMEA)).

The adequacy of the risk analysis will depend mainly on the:

- degree to which the expertise and experience of those conducting it matches the site-specific hazards and risks;
- methods used;
- data and assumptions adopted;
- depth of the assessment.

Some scenarios include a significant, predominant or solely environmental hazard. For the analysis of environmental accidents, the ALARP framework can be used and the risk evaluated as intolerable, tolerable if ALARP or broadly acceptable.
The process of environmental risk analysis involves three steps:

- Identification and evaluation of source – pathway - receptor linkages for different credible accident scenarios. This includes demonstrating an understanding of the hazards of the establishment and the sensitivities of the environment.
- Identification of tolerability criteria for relevant receptors, dependent on the receptor type and potential level of consequence to the receptor.
- Evaluation of risks to the receptor, through examination of accidents scenarios (their consequences and frequencies) and comparing these to the tolerability criteria.

A zone around an establishment which may be impacted over the specified thresholds should be clearly identified.

MATTEs are most frequently due to liquid releases (including firewater) impacting on land and water. The prevention measures of most relevance to environmental protection are therefore those which reduce the risk of accidental liquid releases or enable their retention on site.

MATTE incidents caused by aerial dispersion are less frequent, but aerial pathways should not be overlooked. Where the potential for such a MATTE has been identified, efforts should be focused on measures for prevention and mitigation (these would also be suitable topics for follow-up during inspection).

The general approach to the risk assessment should therefore be set out at the beginning of the process. The operator should have described the competence and expertise of those making the assessment, how the risk analysis will be carried out and how the significance of the risks will be assessed.

If the operator would later rely on cost-benefit arguments to claim that all necessary measures are in place, this should also have been set out early in the report.

The criteria that would be used to judge if the risks are tolerable should have been clearly summarised early in the predictive elements section of the safety report. The assessor should be able to judge if the criteria are appropriate (by reference to ALARP).

The approach of the operator to the review of the risk analysis (when, under what conditions it will be reviewed) should have been clearly stated.

3.2 ** Human factors have been taken into account in the risk analysis.

Plant personnel are an important part of the safety system. They can contribute to the initiation of a major accident as a result of error ('human factors'); it is widely accepted that virtually all major accidents include human factors among the root causes. Therefore the role that process personnel play in controlling hazards and risks should have been identified in the risk analysis. Equipment and procedures should have been designed to minimise human error.

The risk analysis should have considered all types of human error that could contribute significantly to the initiation or development of a major accident. Supporting documents (link tables, LOPA analyses, bowtie diagrams, and so on) clearly illustrate the part played by people in initiating, preventing, controlling and mitigating the consequences of major accident hazards.

Example of where human error should be considered:

If an operative is required to take certain actions following an alarm, such as initiating a plant shutdown that will prevent a major accident from developing, the risk analysis should have made assumptions about the likelihood that the correct action will be taken: if the economic consequences of emergency shutdown are great, the operative may very well hesitate or fail completely to initiate the shutdown. Generally, a lower reliability is assigned to human response interventions than automated responses.

The potential for dependency between successive human tasks should have been recognised and accounted for in the safety report. For example:

- the human error probability for one task may be significantly influenced by an error in a previous, related step / task;
- different people doing the same task may make the same error;
- the same person may make the same error during a number of tasks;
- a checker may fail to detect an error, for the same reason the user made the error.

If a task is critical to the prevention of a major accident and an unrealistically high level of human reliability (a low probability of failure on demand) has to be assumed to make the risks ALARP, this may not be acceptable as it places an undue burden on the operative that would not be supported by current reliability analysis techniques. Instead automatic control and protection systems could have been used to reduce the reliance on the operative to intervene. There is a very strong burden on the establishment operator to adequately justify any other approach.

Examples of what could be addressed under human factors assessments:

- systematic identification of the potential role of human failure in accident initiation or escalation;
- a structured approach to identifying all safety-critical and key safety-related human tasks;
- reliability of control measures dependant on human action;
- determination of the minimum staffing levels required to deliver the necessary measures under all reasonably foreseeable conditions, including plant upsets;
- risks of undue fatigue in key staff, allowing for overtime, shift patterns and so on.

The safety report should have described:

- the methodology for identifying safety-critical tasks (including routine, non-routine, abnormal and upset, first line emergency response, safety critical maintenance, inspection and testing activities);
- the methodology used for task and human failure analysis, for example:
  - structured on-plant task analysis, to gain a thorough understanding of the task and identify safety-critical steps;
  - systematic identification of the different types of human failure (slips, lapses, mistakes, violations, and so on) using a recognised methodology (for example, Human-HAZOP guidewords);
  - a framework to evaluate local performance influencing factors;
  - active involvement of front-line personnel who currently perform the task being analysed (with support from competent facilitators).
- a suitably prioritised programme of task and human failure analysis that accounts for the full range of safety critical tasks and major accident hazard scenarios;
- arrangements to ensure that those who undertake or facilitate task and human failure analysis are, and remain, competent to do so.

The safety report should have considered an adequate range of human failings. The following types of events may warrant consideration from a human factors perspective:

- failure to successfully carry out an operation that is part of normal duties;
- 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);
- failure to detect failed components during testing;
- introduction of failures by damaging equipment or leaving equipment misaligned during testing or maintenance.

Examples of the type of issues that should have been addressed in the safety report, but are more often not, are given the example below.

Example of direct human initiated major accident scenarios:

- loading wrong reactants into a batch reactor;
- not specifying the relief vent size to be capable of relieving pressure build-up in a runaway reaction situation.

The operator should have demonstrated in the safety report that the systems and procedures for selection, training and supervision of operatives are fit for purpose.

The safety report should have described how the probability of operative error has been reduced, in particular:

- how operative errors have been identified;
- the measures that have been taken to reduce their probability;
- how they have been accounted for in the major accident analysis.

Examples of common human factors analysis gaps to look out for in safety reports:

- The potential for an operative to override designed safety features was not considered – there should be some mention of 'violations' or 'breaking the rules' as well as 'human error'.
- The hazard analysis failed to identify anything other than errors of omission (operative failing to act) - errors of commission (an operative making an action. but the wrong one), or decision making errors should also have been considered.
- The role of people other than as front-line operatives (for example, maintenance personnel, supervisors, designers) was not considered.
- No consideration was given of the possibility of a hardware failure with a simultaneous human error.
- An operative being required to do a critical task that would probably be more reliably done automatically.
- Undue reliance placed on operatives to identify and respond rapidly to alarm conditions (justification of the human error probability should have been included where this is done).
- A reliance on 'heroic' acts by operatives to recover situations (for example, going into a danger area to take some preventative or mitigating action).

When quantitative human reliability assessment has been used to determine human error probabilities (for example, for initiating events and layers of protection), the competence of the person carrying out the assessment should have been explained, together with the underlying assumptions of the assessment and the way the generic human error probability data has been applied.

3.3 *** All potential major accidents have been identified.

A listing of **all** the identified major accidents should have been included by the operator in the safety report, along with their broad consequences and broad probability of occurring.

The consequences identified should have included estimates of the number of casualties and/or environmental effects. Describing consequences as for example, 'catastrophic', while useful, may not assist in making transparent the subsequent reason as to why one accident has been selected in preference to another for the detailed analysis.

Where a risk-consequence matrix has been used to rank major accidents, its suitability should have been referenced to an appropriate source to demonstrate its fitness-for-purpose (or a clear justification should have been presented).

The accident scenarios identified should have covered situations where protection and mitigation measures (either actual or proposed for further risk reduction) have failed to operate and should have included the worst case on-site and off-site scenarios for both human health and the environment.

The hazard identification methods used should have been appropriate to the scale and nature of the hazards – more elaborate methods should have been used for complex scenarios.

Examples of hazard identification methods that could be used to identify major accident scenarios for detailed analysis include:

- HAZOP;
- safety reviews and studies of the causes of past major accidents and incidents;
- industry standard or bespoke checklists for hazard identification;
- FMEA;
- Process Hazard Analysis (PHA);
- job safety analysis (for example, Task Analysis);
- human error identification methods;
- FTA;
- ETA.

A systematic process should have has been used to identify the sequence of events that led to the major accident. If the accident analysis deals with each item of plant and process in turn and identifies all initiator and all types of fire/explosion/toxic release, then it can be considered to be systematic.

A safety report can be considered seriously deficient if significant scenarios have been omitted.

The seriousness of the omission will depend on whether the consequences to human health and the environment are worse than those from other accidents that are dealt with and whether the risk from the scenario in question is ALARP.

Example of scenario omission that will lead to lead to serious deficiency conclusion:

- failure to examine the consequences of a confined explosion in a cylinder filling plant where that had the potential to produce high energy missiles capable of puncturing a storage vessel.

The 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 – however this is more likely to be achievable on small or less complicated establishments.

Examples of different plant that would have to be systematically described:

- pipe on a pressurised storage system;
- vessels;
- ROSOV;
- excess flow control valve;
- automatic shutoff valve;
- level sensor;
- flow sensor.

The above are plant items connected to a large inventory of LPG and would each have to be considered in determining their possible roles in a major accident.

In more complex situations, one technique on its own may be insufficient to identify the human/management errors and procedural/hardware failures that could lead to a major accident. Programmable electronic systems should not have been neglected in the analysis either.

The scenarios considered must have included those initiated by off-site as well as on-site events.

Examples of off-site accident initiators:

- aircraft impact;
- subsidence;
- extreme environmental conditions (abnormal rainfall or snowfall, very low or high temperatures, flooding, gale force winds, lightning strike);
- vehicle/train impact;
- land slip;
- explosion;
- forest fire;
- missile;
- pipeline rupture.

Some of these off-site initiators may be very unlikely and be ruled out with minimum explanations (e.g. aircraft impact can be ruled out if establishment is not on a flight path or near an airport).

All possible sources of major accident hazard should have been identified.

The assessor could use the ARAMIS MIMAH methodology to assist in checking that appropriate major accident scenarios have been identified by the operator.

The safety report should have presented a review of past accidents and incidents with the same substances and processes used, and demonstrated that the lessons learned from these have been considered. It should have referred to the specific measures taken to prevent such accidents.

If scenarios that would significantly change the predicted risks posed by the site are omitted without justification, the **safety report should be deemed to fail to comply with this assessment criterion**.

The safety report should have demonstrated that an appropriate methodology has been used to identify the major accident scenarios with an environmental impact taking account of:

- source, pathway and receptor trios;
- the worst case failures;
- domino and / or escalation of major accidents;
- the behaviour of substances under normal and abnormal conditions;
- the direct and indirect effects of major accidents (for example, fire-fighting water and explosions).

Source details should have been defined for each accident scenario including:

- substance released;
- size, rate / duration of release (including both the initial release and anticipated actions of emergency responders, for example, use of water sprays and / or foam blanket for fire fighting or suppression of vapour);
- conditions of release (pressure, temperature, phase);
- location, elevation, direction of release.

Potential releases should have been identified including a consideration of worst case failures (inventory and process) and the sensitivity of the receiving environment (number and types of sensitive sites).

Pathways by which the substance reaches the environment should have been identified, for example, by using maps and plans indicating where aerial dispersion and deposition may impact sensitive receptors or where run-off of spilled substances and fire fighting water could take place, it's pathways on and off the establishment and areas affected.

Substance behaviour upon release should have been identified, for example, reactions with air / water / other substances, changes of phase, dispersion characteristics (dense or buoyant behaviour) and so on.

3.4 *** Clear criteria have been described for eliminating identified major accident scenarios from further consideration: if necessary a suitable subset of potential major accidents has been selected for detailed risk analysis.

Where an operator has identified a large number of different types of major accident, it is not necessary to further address each one in detail in the safety report. The operator should set out a logical rationale for selecting a representative subset for detailed analysis.

Accident scenarios for very improbable initiators (for example, meteor strike, simultaneous multiple failures of demonstrably reliable systems, terrorist activity) can usually be neglected, but events like cold catastrophic failure of vessels (LPG) and guillotine rupture of pipework should not have been discounted.

Example where a scenario may be omitted from further consideration:

A toxic gas consequence assessment may have shown that any failure resulting in a release smaller than that equivalent to a 10 mm diameter hole would not produce a major accident hazard or significantly contribute to risks to current on-site or off-site population (but a substantial length of vulnerable pipework within a small area could mean this is a significant risk for a section of the on-site population, which should not be omitted!).

The operator should have taken of account of smaller releases that could trigger other events leading to event escalation, for example, a smaller flammable release into a confined space, which might ignite and explode and trigger a more severe accident.

Small scale releases should not have been eliminated ‘unjustifiably’. It is reasonable for an operator to reduce the number of release cases by defining a scale of event that will not lead to a major accident and by grouping or aggregating events.

The criteria should have been applied at an early stage to limit the scope of the predictive aspects of the risk analysis.

The criteria used must have taken account of high frequency as well as high consequence events.

Where a matrix system has been used to rank the scenarios, an explanation should have been provided on how the choice for detailed analysis has been made between scenarios assigned the same likelihood and /or severity.

If the operator has not quantified accident frequencies, but uses terms such as *high*, *medium* and *low* probability, the accidents should be ranked according to their perceived severity. Without any quantification it can be difficult to determine if an accident that seriously affects a few people with 'medium likelihood' is worse than one that fatally affects many people with 'very low likelihood'.

Worst case accidents should have been included as well as accidents that are more probable, but with lesser effects.

Most safety reports are unlikely to determine the consequences and frequency of all possible accident scenarios, but all risk dominating accidents should have been dealt with comprehensively.

The safety report should have clearly stated why the consequences of some major accidents have not been described, if that is the case.

Example of where consequences do not need to be described:

If six different accidents resulted in a similar rate of release of LPG, with smaller duration and dispersion characteristics, the consequences of only one of them need to be described. The relative likelihood of the others should be evaluated to demonstrate that the risks are ALARP.

The subset chosen for detailed analysis should represent the range of accidents that are possible on the establishment.

The operator should have made clear that the conclusions that will be drawn and the measures that will be implemented for the subset will also apply to the full set of scenarios.

Failure to include 'worst case' representative scenarios will mean this criterion has not been met.

3.5 ** The information used to model the major accident scenarios in the detailed risk analysis was appropriate.

The information required for this part of the risk analysis is diverse and extensive. The detail required is both process and location specific. The criterion can be broken down into the following:

1) A representative range of major accident scenarios have been chosen for detailed modelling.
2) Worst case major accident scenarios have been modelled both with and without the control measures in place.
3) A full range of lesser accident scenarios have been modelled both with and without the control measures in place.
4) The accident scenarios have included those with off-site initiators (if any) and those due to escalation of smaller scenarios within the establishment.
5) The modelling has been carried out using appropriate computer models.
6) An appropriate range of atmospheric stability conditions have been used, taking account of the local conditions (wind direction, wind speeds, topography, humidity, and so on).
7) The source terms used in the modelling have been clearly set out and appropriately used.

These will now be explored in more detail.

1) A representative range of scenarios has been chosen

An adequate range of major accidents, broadly classified as loss-of-containment accidents, should have been covered.

Examples of the range of major accident scenarios that might be covered:

- vessel or pipework failures, including bund failure and fire engulfment;
- explosions (batch reactors runaway, tank explosion due to operative error by for example adding the wrong substances), BLEVEs;
- large fires (warehouses, pool fires, and so on) including toxic impacts;
- events influenced by emergency action or adverse operating conditions etc. (for example, allowing a fire to burn rather than applying water or dumping reactor contents to drain to avoid explosion, abnormal discharge to the environment, and so on).

All foreseeable causes (initiating events) of the major accident scenarios chosen for detailed analysis must have been considered.

Insights gained from the study of previous accidents and incidents can be a useful starting point: the causes of similar accidents in other industries should have been considered.

A safety report that unreasonably discounts some accident sequences or fails to consider worst case locations for pipe breaks or assumes procedures and/or safety systems function perfectly should be judged as failing to meet this assessment criterion.

Example of the consequences that should be determined for the following minimum set of accidents for an LPG site:

- catastrophic failure (100% of contents released) - fireball and flash fire or pool fire;
- localised failure of a pressure vessel above liquid level - jet flame & flash fire and possible explosion;
- localised failure of a pressure vessel below liquid level - jet flame and flash fire and possible explosion. Pool fire or flash fire/explosion for a refrigerated vessel failure;
- pipe failures (rupture, hole diameter equal to pipe radius, flange leak);
- BLEVE of vessels including storage vessel, road tanker, cylinders in a stack;
- overfilling - ignited pressure relief valve discharge, or spill of liquid if refrigerated;
- vaporiser leak jet fire, flash fire, explosion;
- leak inside cylinder filling plant - confined explosion.

2) Worst case major accident scenarios have been modelled, both with and without the control measures in place.

The operator should have determined in the safety report the consequences of worst accident scenarios on the assumption that all control and mitigation systems have failed on demand and operational conditions correspond to the worst case (which of course will have a very low probability).

Ideally, the safety report should have modelled events both with and without the safety features in operation so that subsequently in the report the 'value' of the safety barriers can be assessed and balanced against their reliability.

Examples of inappropriate discounting of scenarios

- It should not have been claimed as a reason for not modelling the worst case consequence that a release will be terminated early by a shutdown system that may fail on demand.
- An event should not be discounted on the grounds that a permit-to-work precludes the necessary conditions for it to be initiated.

Accident scenarios should not have been unreasonably discounted for assessment of consequences.

3) A full range of lesser accident scenarios have been modelled, both with and without the control measures in place.

Lesser accidents are usually more likely to occur than the bigger accidents and their aggregated risk may be quite high. Therefore the consequences of, for example, different size pipe leak breaches should be determined.

As in the previous section, the features/systems that may limit the consequences of the lesser accidents should have been identified: the severity of the consequences of an accident should not have been reduced on the grounds of the presence of a safety system – both cases should have been considered, with probability arguments applied subsequently as necessary.

The full range of consequences should have been addressed. The safety report should not have discounted any scenario unless it has provided good reasons for doing so.

Example: considering and discounting scenarios:

- If an unconfined explosion of LPG is discounted, it must be on the grounds of experiment and historical data.
- High pressure pipe work failures should include the formation of a vertical and horizontal jet and the potential for jet flame impingement.
- Leaks into an enclosed space that may result in a confined explosion should not be forgotten.

Examples of events to be modelled on an LPG site:

An instantaneous release of the whole contents of storage vessels and various other scenarios that could result in a continuous release of several tens of kg/s and give rise to a variety of fires should have been considered. The failure of associated plant (for example, vaporiser and cylinder filling machine) giving rise to a variety of hazards including a confined explosion should also have been addressed. The consequences of each accident under a range of conditions that encompass the full severity range should have been determined. Both day and night time conditions should be considered for accidents affected by stability (that is, those involving dispersion): only D_5 and F_2 conditions need to be considered (because increased wind speed shortens the hazard range). A range of wind speeds should be considered for jet fire events. The safety report should have described the consequences of the worst conceivable accidents when a vessel is full. The analysis should not be overly conservative: if unrealistic hazard ranges are predicted, the EEP of the LCAs could be ill-conceived and could put lives at risk by spreading the response too thinly.

4) The accident scenarios included those with off-site initiators (if any) and those due to escalation of smaller scenarios within the establishment.

Escalation scenarios example on an LPG site:

- jet flames that impinge on tank vessels leading to BLEVE;
- VCE that can cause a variety of mechanical failures;
- pipe whip leading to rupture of nearby pipes or plant;
- explosions in buildings that can generate blast overpressure and missiles;
- missiles generated by compressors;
- fire in a cylinder stack.

Domino events and escalation must have been considered. Consequence assessment should always consider the location and precise circumstances of the release. See 3.3 for examples of off-site initiators.

5) The modelling has been carried out using appropriate computer models.

The safety report should have provided or referenced accessible sources for the predictive models employed. If a well-known computer program has been used (for example, ALOHA or PHAST or EFFECTS), then only the details of the input data and the version number need to have been given.

If an in-house or obscure computer program has been used to calculate the consequences of major accidents, then the physics on which the predictions are based should have been described or reference should have been made to a published article supporting its use for the purpose employed.

The endpoints modelled to should have been appropriate:

A range of endpoints for the major accidents should have been considered, so that corresponding 'hazard zones', defining the extent of affected areas, are capable of being mapped out (see criterion 3.7).

For people, the endpoints considered should have included those that will allow differentiation between the numbers potentially requiring hospitalisation or likely to suffer serious injury or fatality.

A range of potential harms to the environment should have been considered, for example to LC_{02} or LC_{03} and 'negligible effect' criteria for the relevant sensitive species.

Examples of reasonable assumptions for modelling:

- In the case of catastrophic failure of a bulk tank, it is reasonable to assume 50% overtops the bund (in the absence of a specific calculation).
- In the case of fires, a surface emissive power [SEP] of 50-150 kW/m^2 for hydrocarbon fires is usual, with 150-350 kW/m^2 used for fireballs.
- For a Jet Fire 200 kW/m^2 is often used.

The accident consequence analysis must have been thoroughly and adequately documented.

Failures occurring at the 'worst locations' – for example on pipelines through a congested area, where the possibility of a VCE cannot be ruled out should have been considered.

Example of multiple potential consequence events:

Failures of LPG storage systems can give rise to a variety of thermal radiation/explosion hazards that must be addressed in the safety report. For example, the consequences that should be considered for the failure of a large storage tank are fireball, jet fire, flash fire and VCE (if possible).

The site description should have been detailed enough so that the most hazardous locations for component failures can be identified and from this it can be determined if the accidents identified included 'worst case'.

In the case of thermal radiation effects, consequences down to at least 4kW/m^2 should be considered.

Other important endpoints to be used are for piloted ignition of wood (14.7 kW/m^2) and spontaneous ignition (25.6 kW/m^2).

For toxic gases, fatality, defined injury endpoints as described previously, ERPGs, TEELs and AEGLs are all endpoints suitable for use: but the endpoints selected should have enabled the full spectrum of casualties to be estimated.

6) An appropriate range of atmospheric stability conditions have been used, taking account of the local conditions (wind direction, wind speeds, topography, humidity etc.).

The meteorological conditions for the site should have been described in sufficient detail. Wind rose data (wind speed, wind direction and atmospheric stability) should have been presented to establish the frequency and direction of adverse atmospheric conditions (where these were relevant to the major accident hazards).

The wind direction can vary over the full circle of 360°C with varying probability. D_5 and F_2 weather stability modelling conditions do not necessarily encompass the full range of consequences of an accident .Warehouse fires and jet flames are 2 examples where higher wind speeds may be relevant.

Example of reasonable modelling assumptions:

- High pressure LPG jets can be horizontal or vertical and dispersion calculations assume that the gas is cold and dense ('dense gas' model) and is modelled under D_5 weather conditions. Wind has the effect of reducing the length of a high pressure jet so 15m/s wind should be considered for vertical jet fire events. This should be reduced to 2 m/s wind for horizontal jet fires.
- An assessment of the consequences in two weather stability/wind speed combinations (i.e. F_2/D_5) will suffice for most scenarios involving toxic gases.
- The worst consequences for toxic substance generation from warehouse fires will be in high wind speed conditions (i.e. D_{10}-D_{15}). This is because an intense fire generates a buoyant smoke plume which normally rise high into the atmosphere. However, if a passive dispersion model is used to predict down-wind concentrations then D_5 modelling will give conservative results. After 30 minutes of fire, warehouse plumes should be considered to be too buoyant to affect ground level receptors.

7) The source terms input to the models have been clearly set out and appropriately used.

Sufficient information should have been given to allow the assessor to determine the source terms ('how much, for how long and from where') for all accidents.

Any containment system or item of plant can fail and release its contents.

Examples of information relevant for source terms:

- pressure and volume of large vessels and other plant containing significant amounts of liquid or gas;
- diameter and length of pipe to an isolation valve that can be closed (pipeline failures);
- list of related equipment (e.g. pumps, vaporisers, cylinder filling equipment) together with the operating pressures and temperatures.

Examples of source terms for a chemical warehouse:

- the area of the warehouse fire;
- the rate of plume development in the event of a fire;
- the quantity of chemicals that could, under worst circumstances, leave the site in fire-fighting water.

Example of level of source term detail required:

A high pressure release from a pipe or vessel is characterised by the release rate, the duration of the release and its form (e.g. liquid or gas and whether as a vertical, horizontal or obstructed jet).

An adequate range of release rates should have been considered and should include 'worst case'. Release rate is effectively determined by hole size so accident consequences should have encompassed a range of hole sizes and include the largest possible failure i.e. guillotine rupture of a pipe and catastrophic failure leading to an instantaneous release of the whole contents of a vessel. Pessimistic assumptions should have been made in quantifying source terms. Site specific factors should have been taken into account in relation to:

- the frequency of releases;
- the magnitude of releases;
- the duration of releases.

Example of parameters to be included for an LPG site:

- size and type of storage vessels;
- maximum stack of LPG cylinders;
- number and capacity of road tanker deliveries per year;
- whether the site is occupied 24 /7;
- maximum tank padding pressure;
- the maintenance schedule for key safety features, for example, ROSOVs.

The assumptions used in the accident analysis related to the operating conditions of the installation or establishment should have been clearly stated and justified.

Example of similar consequences which should be examined separately:

If a pipe failure can release gas at 20 kg/s and failure of a cylinder filling machine can also give rise to a 20 kg/s release, the safety report should consider both failures because they may have different consequences.

On the other hand, pipe failures of 20 kg/s can be grouped together as a single case for consequence modelling.

Examples of what should be included in the systematic consequence analysis expected for an LPG facility:

- the assumptions made about containment failures (size, location);
- the essential features of the model that will be used to calculate the rate of outflow of LPG and the duration of the release;
- the assumptions used in the assessment;
- characterisation of the LPG release;
- the model used to determine the characteristics of the thermal radiation source for scenarios involving immediate ignition (fireball and jet fire and pool fire);
- the assumptions used to calculate the radiant flux from the burning gas (emissive power, wind speed);
- the assumptions about the dose received by individuals indoors and outdoors;
- the results of individual dose calculations;
- the assumptions for LPG gas dispersion (flash fire calculation);
- the assumptions used in the dispersion analysis (stability, wind speed ground roughness);
- the essential features of the model used to calculate the dispersion of release of LPG ;
- the dimensions of the flash fire;
- the effect of accidents on local populations and the environment;
- justification where a VCE was been excluded.

Example of a systematic consequence analysis for a chemical warehouse:

- Clear and reasonable assumptions were made about the location of the source of the fire.
- The essential features of the model used to calculate fire growth, buoyancy of the plume and plume development were set out.
- A description of the plume dispersion mode has been provided.
- The assumptions used to run the dispersion model (stability, wind speed and ground roughness) have been clearly stated.
- The toxicity endpoints modelled were clear and appropriate.
- The method to calculate toxic dose was clear and appropriate.
- Presentation of the modelling results has been made in terms of concentrations and dose down-wind.
- Presentation of the modelling results of thermal radiation to demonstrate any potential escalation effects.

3.6 ** The Loss of Containment (LOC) failure frequencies, the reliability of equipment and the human response times that have been used were appropriate and realistic.

Under this criterion it will be assessed whether

- appropriate loss of containment failure frequencies were used, taking account of local conditions and compliance with good practice;
- the control measures in place have been clearly identified and a suitable reliability assigned to them;
- sound methods have been used to calculate the overall risk.

The methods that have been used to generate the estimates of the probabilities of potential major accidents should have been appropriate and used correctly.

If a QRA approach has been taken, accessible sources should have been provided for base failure frequencies/probabilities (e.g. FRED[3], BEVI[4] etc.) for loss of containment.

Base event failure data are essential components of QRAs. Figures must be relevant and applicable to site circumstances. Taking a value from the literature without consideration of its applicability to a site should be considered unacceptable: use of a failure rate that is not consistent with historical or relevant generic industry data must have been justified.

[3] http://www.hse.gov.uk/landuseplanning/failure-rates.pdf
[4] http://infonorma.gencat.cat/pdf/AG_AQR_2_Bevi_V3_2_01-07-2009.pdf

The operator must have presented evidence to demonstrate that the event sequences triggering the scenarios were correctly identified and clearly justified.

The accident analysis should have identified and quantified all event sequences resulting from a single failure.

Examples of likelihood range to be considered:

- The frequency of accidents resulting in a large release of gas should be determined more reliably than the frequency of flange leaks on low-pressure pipe work.
- The complexity and level of detail of the analysis should have been 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 affecting a small number of employees.

There should have been a consistency in the risk and consequence models used. If the Purple Book/BEVI failure frequencies were used they should have been used in conjunction with the method for estimation of effects described in the Yellow Books[5] (or methods based on this) If FRED failure frequencies were used they should have been consistent with the endpoint and scenario advice given by the HSE. If the LUP approach of the CCA is used, then the consequence assumptions and failure frequencies should **both** have been used. As the CCA's LUP model balances relatively high event frequencies with non-conservative consequence modelling assumptions, it should not have been used by operators pursuing a qualitative demonstration. For example, a much higher SEP figure (the default figure in the software programme) should have been used for hydrocarbon fires (see 3.5.4 – examples of reasonable assumptions for modelling).

Other appropriate methods include the use of relevant operational and historical data, FTA and ETA, or a combination of these. The methods and assumptions used should therefore have been described. In particular, failure rate data used for the base events in the FTA should have been clearly justified for the site-specific circumstances.

Site specific factors should have been taken into account in the methods used to generate event sequences and estimates of the probabilities of potential major accidents. For example, frequency for aircraft impact based on background crash rate would not be applicable to a site located close to a busy airport. In general, off-site accident initiators tend to be site specific but differences in site management, operation and competence (training) of staff can also significantly affect accident frequency.

Generic or industry standard failure probabilities for valves, pumps etc. are based on appropriate operation under stated conditions with an industry standard maintenance regime (which may be different to what an operator actually does). Use of such data in risk calculations should have been justified.

[5] http://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS2/PGS2-1997-v0.1-physical-effects.pdf

Where failure rate data is being derived from industry experience it should be from a long experience of operation in the same industry and under the same conditions. Failure rate data from the operator's own long established database can usually be accepted but if the figures are based on experience in another industry their use must have been justified by reference to operating conditions, maintenance regimes etc.

If the probability of failure of a particular item of plant is based on generic data, then it should be identical to it or closely resemble it in design, manufacture and operation. The mean failure frequency of plant components should have been increased if they are used under conditions that are different from the design operating conditions. Similarly, the mean failure rate of a component should have been increased if it is assumed to apply to another similar, but not identical, component.

It will not be sufficient to have used data from published sources without justification as to their suitability, unless it has been shown (e.g. through a sensitivity analysis) that the conclusions of the risk analysis are not sensitive to such information.

Figures derived from Fault Tree Analysis (FTA) in particular should be scrutinised to confirm they are not unduly optimistic or out of line with historical experience or the results of other methods.

Conditional failure probabilities / reliability figures for equipment used in the accident analysis should have been appropriate. Key documents that the safety report relies on this respect should have been made available (for example, as an annex to the main report - unless already publicly available).

The frequency analysis should have recognised that failures of complex systems involving operatives have many components. If a dangerous situation can occur following a series of operative and control equipment failures, each of these must have been identified to show that the calculated event probability is reasonable.

Where figures have been taken from standard references, they must have been applicable to the actual plant and conditions at the establishment. If accident likelihood is determined on the basis of historical data or some other method that does not involve a calculation of accident frequency, good evidence should have been presented to show that the plant is designed, operated and maintained to appropriate standards and that the operatives controlling it are adequately trained.

The reliability, effectiveness and independence of barriers should have been justified in proportion to their importance in prevention and /or mitigation.

Optimistically short response times should not have been used for control/safety equipment.

The operator's justification may have included quality procedures, plant experience or other acceptable evidence and the independence and reliability of these should be assessed. These assumptions/justifications should be for verification during subsequent routine inspection.

Reasonable assumptions should have been made regarding operative response. The safety report may have claimed that control room operatives will notice an illuminated alarm indicator immediately or will respond to an emergency perfectly and respond appropriately in a matter of

seconds. Assumptions in this vein may be over-optimistic but they do not necessarily signify that the safety report is deficient, provided the consequences of much longer response times are also included.

Example of assumptions on reliability of response requiring justification:

In a scenario where an operative has to intervene to close an isolation valve manually, the release duration should be determined by the time taken for the operative to intervene successfully from the initial alert to completion of the action which will prevent the major accident from proceeding, allowing for the distractions and other duties that may be required of the responder. Modelling release duration of less than 20 minutes in such cases will require justification by the operator. This should be verified subsequently (during routine inspection) by the assessor.

Operative response times of less than 10 minutes should always be queried.

The full range of conditions should have been considered for each accident. Accident consequences should not have been reduced on the grounds that the probability of the wind blowing in a particular direction was low, if very similar consequences would have arisen when the wind blows in any direction.

Risk should not have been 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 safety report should have assumed that plant in the vicinity of a major fire would not receive water spray protection from external responders for at least 20 minutes, unless this can be justified by local circumstances.

Predictions based on a much shorter response time for the fire brigade to respond are likely to be optimistic. Operators must have considered the consequences of the late arrival of fire-fighting services, but they can have taken into account the probability of such a late response.

The risk analysis should have taken account of uncertainties in the estimation process. Most failure probabilities are not discrete values but distributed about a mean. If these are critical to meeting the tolerance criteria then some sensitivity analysis would have been appropriate.

Where the estimates of the likelihood of the safety critical events are seen to be sensitive to the data and assumptions used, suitable and sufficient justification should have been provided.

Accident analysis should have addressed the effect of other variables (e.g. time of year, time of day and day of week) if they have a significant effect on the consequences: **a limited analysis that neglects variability in accident consequences will not meet the assessment criteria.**

Example of reliability assumptions that should be justified:

- **R**emotely **O**perated **S**hut-**O**ff **V**alves (ROSOVs) will terminate a release.
- Operatives will perform safety critical tasks correctly under stress.
- Instrumentation will always detect a dangerous situation.
- Shut-down systems will respond on demand.

Example of need for a clear statement on response conditions and assumptions:

If it is assumed that an alarm will be responded to immediately, or that a hardware failure will be detected immediately, then the control room must be permanently manned and instruments that would detect the failure should have a status indicator. Even then, the possibility of a delay before remedial or emergency action is taken should have been considered.

In the case of a pharmachem site, a chemical warehouse or other types of establishment, assumptions used in the accident analysis that should have been justified include:

- the local fire brigade will reach the site within 20 minutes (or similar);
- sprinklers will extinguish all fires;
- the site isolation system will function perfectly when called upon.

Examples of some other assumptions that require explanation:

- the reliability of shut-off valves on site drains (manual and automatic);
- the likelihood that an operative will be directed (and be able to respond within the appropriate timeframe) to isolate the site in an emergency;
- the reliability and capacity of a bund to hold up fire-fighting water, foam and spilled dangerous substances and to not allow any to leave the site or the containment area.

It is important that prevention and mitigation measures identified for any accident subset have been explicitly linked back to the full accident set.

The safety report should have considered all possible consequences of an event, particularly those involving escalation and determined the probability of escalation effects.

Where a sequence or combination of events may lead to a major accident, an assessment must have been made of the effects of failure of the plant and equipment designed to prevent, detect, or mitigate the hazardous conditions.

Example of a sequence of events leading to a major accident, involving a failure to respond:

An automatic isolation system fails and the operative fails to respond correctly to an alarm and therefore the system is not brought back under control and a loss of containment occurs.

For very hazardous events, the reliability of automatic systems should be sufficiently high to render the risks sufficiently low, even allowing that the probability of the operative failing to respond is relatively high.

Human error should also have been addressed as an accident-initiating event in addition to escalation arising from intervention activities.

A system that depends on operatives and a mixture of active and passive control systems is always at risk from human and equipment failures.

Example of where plant design may render an event improbable:

- A vessel that is unlikely to be pressurised because it is fitted with at least two sufficient and independent vents to atmosphere.
- A containment system that is too small to generate a major accident.
- A vessel that is unlikely to be punctured by missiles because it is totally enclosed by a very strong barrier.

The potential for escalation should have been properly addressed.

The effect of failure of automatic or manually operated safety systems in the sequence of events leading to a major accident should have been considered.

Examples of failure of automatic or manually operated safety systems:

- a hidden fault (e.g. a failed ROSOV);
- an initiating event (e.g. pipe rupture);
- failure of an operative to respond correctly.

Consideration should have been given to accidents directly initiated by human action. QRA may be used to demonstrate that the probability of such accidents is low, but their consequences must have been determined.

Safety critical events are those that dominate the risk at different distances from the plant.

All safety critical events and associated initiators must have been clearly identified. Some safety reports may not have used the term 'safety critical event' but the safety report should include them in the sub-set to be given detailed consideration.

Example of a safety critical event:

For pressurised storage vessels containing highly flammable substances, the event with the greatest hazard range is usually a fireball resulting from immediate ignition of an instantaneous release to atmosphere of the whole contents.

The non-QRA approach groups accidents according to their broad likelihood and consequence. The frequency of occurrence 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 have identified a set of representative accidents and frequencies for more detailed consequence analysis.

A safety report that fails to analyse accidents as outlined above will fail to meet this assessment criterion. However, approaches that are not based on quantification, but nevertheless rank accidents appropriately, should not be rejected out of hand.

In summary, the risk analysis should have made clear the events that are critical from a safety viewpoint. This will have required consideration of the likelihood of the various major accidents and the associated consequences.

Operators should have used appropriate methods for assessing the probabilities of each of the listed major accidents.

Implementation of control and protection measures that would reduce the risk arising from these events should have been considered and implemented where necessary.

Where potential control measures have been rejected, the reasons should have been clearly justified.

All the potential consequences of each reduced accident set should have been considered.

While some events are more probable than others, those contributing little to the total risk should not have been automatically ignored.

3.7 *** A suitable and sufficient analysis of the local consequences has been carried out.

The consequence assessment models used (for example, the dispersion model used to calculate the dimensions of a flammable cloud of LPG, BLEVE or toxic effects of a warehouse fire) must have been appropriate and used correctly.

The consequences identified should have clearly set out the severity of the effect and the number of people potentially affected. The environmental consequences should have been tailored to the local environment and been as specific as necessary to describe the effects.

Consequence analysis for an LPG storage site (and possibly a site storing highly flammable liquids) should have included thermal radiation from the different types of fire and for the overpressure produced by explosion.

The harm criteria or vulnerability models used to assess the impact of each major accident hazard on people and the environment should be appropriate and have been used correctly for each relevant major accident. The safety report should have calculated thermal radiation and explosion overpressure hazard ranges and casualties for several severity levels.

The number of fatalities and persons with severe burns from the effects of fires and explosions should have been determined.

The effect of blast should have been quantified in terms of the number of buildings in each of several damage categories and the envelope of a flash fire should have been superimposed on a map so that the effect of wind direction on the number of casualties were capable of being assessed.

The safety report should have provided information on the assessment of the environmental consequences of a major accident regarding:

- all the factors that may determine the extent of environmental impact (for example, ignition, detection, secondary containment failure, drains, emergency procedures, and so on);
- the resultant environmental concentrations for each of the set of releases;
- the effects in the environment determined from the predicted environmental concentrations and toxicity data (the severity of the MATTE);
- the length, area or volume of the environment affected (the extent of the MATTE);
- the criteria used to define harm for the extent and severity conclusions;
- estimated duration of the defined harm period (based on natural recovery periods, without mitigation).

It should have been demonstrated that the approach / methodology is appropriate. While all scenarios require consequence assessment to determine whether or not they present the risk of a MATTE, the detail presented for each scenario should be proportionate to the overall risk.

Example:

For many fire events there is a greater risk of harm from fire-fighting water run-off than aerial dispersion and thus more effort should be placed on quantifying impact from run-off.

The extent of the consequential environmental impact should have been assessed and described for each MATTE scenario or each representative set of releases, taking account of worst case scenario consequences.

It should have been demonstrated that an appropriate method has been used to calculate release rates and the specific values of any variables, such as:

- toxicity relationships (for example, dose-response relationships);
- negligible effect criteria (for example, No Observed Effect Levels);
- Suggested No Adverse Response Levels.

A safety report that minimises accident consequences on the assumption that installed mitigation systems work perfectly is underestimating consequence (as well as risk).

Examples of scenarios that require justification for an LPG plant:

- A forklift driver cannot puncture a storage vessel with the forks of the vehicle, due to momentary inattention, because the vessel is protected by vehicle impact barriers.
- A high level instrument and other alarm systems and/or a procedure will prevent overfilling.
- An explosion in an enclosed building (cylinder filling plant) has a low probability of initiating an even more severe accident because of the separation distance or the presence of blast protection features.

Sensitivity tests of the results should have been undertaken, related either to the choice of harm criteria or model selected, or the way they were used, particularly when the scale and nature of the hazard and risk was significant. The sensitivity of the results to assumptions that are pivotal to the analysis must have been tested (e.g. release rate/duration, weather frequency).

3.8 *** It has been demonstrated that the risks are sufficiently low.

The findings and conclusions from the risk analysis must have summarised the relationship between the hazards and risks, and demonstrated that the measures adopted to prevent and mitigate major accidents have made the risks sufficiently low **or** identified measures to reduce this risk to a tolerable level within an acceptable timeframe.

The analysis and the comprehensiveness of the presentation of the risk assessment should generally have been proportionate to the scale and nature of the site, and should have been sufficient for demonstrating that all necessary control measures have been taken.

The safety report must have demonstrated that low frequency events with severe consequences are being adequately controlled and that all necessary measures have been taken to prevent their occurrence.

Generally, where qualitative arguments were made in the safety report they should have at least been based on currently accepted good practice for engineering and safe systems of work

There must have been clear links between the conclusions and:

- the analysis of the risks, including hazardous event likelihood and the associated consequences;
- the measures (technical or procedural) taken to make the risks sufficiently low.

The consequences and/or risk to the most exposed person or groups of persons on-site and off-site should have been estimated.

The results of a QRA can be presented as contour plots of individual risk of fatality based on certain assumptions about the individual (for example, out of doors and exposed for the duration of the release or to a maximum of 30 minutes).

Where necessary (a significant number of casualties) a societal risk assessment should have been carried out.

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

The safety report should have demonstrated that the risks are negligible or ALARP.

In the absence of a QRA, the 'all necessary measures' arguments should have been made qualitatively and a case built on relevant good practice and sound engineering principles.

Examples of sources of good practice:

- legislation;
- guidance;
- standards produced by standard-making organisations;
- guidance produced by a technical Body, IChemE or AIChE for example;
- guidance agreed by an organisation representing a particular sector of industry;
- standard good practice adopted by a particular sector of industry.

Should any conflict arise between sources of good practice, the safety report should have demonstrated that an appropriate source was used.

Where good practice has been used as the sole justification of 'all necessary measures', several stringent requirements should have been met:

- the practice should have been relevant to the operator's situation;
- thestandard followed should be up-to-date and relevant;
- where a standard allows for more than one option for conformity, the chosen option should have made the risks sufficiently low;
- any standard applied must have been relevant in the major accident hazard context.

If a qualitative risk assessment has been presented, then it should have been demonstrated that the residual risks were ALARP - this could have been by the use of cost benefit analysis (CBA). Additional safety features should have been identified ('Is it possible to do more?') and it should have been shown that the cost of implementation would have far outweighed the reduction in risk ('It is not justified to do more').

More complex situations may have required the presentation of quantitative arguments coupled with cost benefit analysis in order to provide the justification that all measures necessary have been taken.

The operator should have shown that:

- there was redundancy and diversity in control systems;
- operative error was fully accounted for;
- the more common initiating events would not progress to a major accident.

This should have been supported by sound arguments about the absence of further measures that could be introduced to reduce the risks still further.

If quantitative arguments have been used, the methods, assumptions and the criteria adopted for decision-making should have been explained.

Major accident risks are additional to 'normal' industrial risks. Therefore operators should not have used unacceptably optimistic criteria.

It should be remembered that risks should always be as low as reasonably practicable. For new plant a lower maximum tolerable risk level should have been adopted.

Operators should have stated and justified the benchmark criteria adopted for their environmental impact assessments. Risk may be assessed by:

- qualitative descriptions (for example, low / medium / high risk);
- simple relative scoring systems (for example, 1-5, 1-100);
- quantitative modelling parameters (for example, environmental harm index).

Risk results should have been summed over all events and scenarios to give the total risk to each environmental receptor from the establishment (to be used when considering tolerability).

Risk results may also be presented as individual scenario / event risk (useful to identify the significant risk contributors -If this approach is used, the tolerability criteria will need to be suitably adjusted).

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

It is not in the spirit of risk assessment to use it solely to demonstrate that existing controls or the adoption of current good practice make the risks sufficiently low. Risk assessment is also an opportunity to systematically assess the current situation or decide the best option for designing a new facility. It is a chance to take account of technological advance, to seek inherently safer designs, and to take account of improvements in assessment methods and views on good practice and so on.

Whatever additional measures have been identified in the report as being reasonably practicable should have been implemented or be planned for implementation within a reasonable period of time.

The justification for the rejection of possible risk reduction measures must have been well-argued and supported with evidence.

Explicit links must have been made from the detailed risk assessment to the measures in place for the prevention and mitigation of all identified major accidents.

A safety report based on a QRA should have taken account of the potential for protective devices not to function, for example, remotely operated sprinkler systems, ROSOVs and excess flow devices may fail to operate effectively when called upon. The operator should have recognised that other protective systems may also fail and should have described the measures in place to show that the ranking of risk was 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 have described the effect uncertainties can have on their predictions and have demonstrated, by reasoned arguments or quantitatively, that even under worst case assumptions the risks were ALARP.

The uncertainty in consequences arising from different mathematical model input data should have been addressed.

The uncertainty in accident frequency should have been properly accounted for in the reliability of installed preventive and protective measures.

The safety report should have quantified uncertainties in the predicted failure frequencies and factored those into the final risk assessment.

The uncertainties attached to the risk calculations should also have been addressed and justified. **A safety report that fails to mention uncertainties in the risk estimates, where these could have a material bearing on the demonstration of having taken 'all necessary measures' should be considered deficient.**

Individual uncertainties attached to calculated hazard ranges should have been estimated by discussion of both model inadequacies and imprecise input data. The safety report should have justified the results, if necessary by reference to confidence levels. 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 for a single piece of plant. However, the risks arising from the presence of multiple items of such plant should have been analysed and evaluated. If a site uses new technology for which an historical database is not available, the safety report should have discussed the uncertainty attached to failure probabilities.

The risk analysis must have determined whether the residual risks (determined by the reliability of the control measures etc.) are sufficiently low or whether more needs to be done. LOPA or similar techniques are often employed by operators for this purpose

It must have been clear from the safety report that the conclusions drawn from the detailed risk assessment applied to all the relevant plant including plant not specifically addressed in the detailed assessment.

The operator should have shown in the safety report that control measures implemented to reduce or remove the likelihood of human failure are matched to the human failure types identified and where necessary, optimise the local performance influencing factors that make the error more likely.

Training and procedures are almost always the measures chosen to reduce the potential for human failure. However, they should not be accepted as the sole barriers against human failure. The safety report should have demonstrated that, where necessary:

- the human contribution to failure has been removed, for example, by a more reliable, automated system;
- automation has been selected for the right reasons – that consideration has been given to involving the operative in the process and of the potential for alarm overload.

3.9 *** The conclusions drawn from the risk analysis are soundly based with respect to emergency planning.

The worst-case scenarios for people and the environment must have been considered.

The analysis should not have been overly optimistic or pessimistic as this could have resource implications for the emergency services.

Guidance should have been provided for LCAs on risk dominant accidents. The safety report should have provided a sound basis for emergency planning and should have identified a representative set of accidents spanning the severity range and calculated the consequences of each in terms of 3 levels of impact:

- number of people receiving minor injuries;
- number requiring hospitalisation;
- number of fatalities.

For the environmental impact assessment, levels of harm to the environment should have been considered. For releases resulting in environmental damage a range of representative conditions should have been considered e.g. to cover the range of flow rates in watercourses and to account for the effect on different species.

The safety report should have indicated the number of people likely to be made homeless by the effects of an explosion.

In the cases of toxic airborne releases, information should have been tabulated for a representative range of weather conditions and for all wind directions. It should have indicated where there was any significant difference in the numbers of casualties due to seasonal factors or the accident occurring at week-ends or during night hours. Probability data should have been presented so that emergency planners could tailor their resources around the accidents presenting the greatest risk.

Distances to a range of consequence levels should have been provided. In the event of a major accident the emergency services would want to know where to deploy their staff in order to bring relief to the maximum number of people in the shortest time. The maximum distance out to which people are likely to be injured is of vital importance. The Local Competent Authority will advise the operator as to which endpoint they require.

The area within which information will be supplied to the public should have been provided.

The information to be supplied to the public under Regulation 25(4) should have been included and be consistent with the risk analysis in the safety report.

4. Assessment of the Technical Elements

General comments on assessing this element

The operator should have demonstrated that safety and reliability have been accounted for in the design, construction, operation and maintenance of any installation, storage facility, equipment and infrastructure connected with the operation and **which are linked to major accident hazards inside the establishment**.

The safety report should have:

- identified the hazards and the major accident scenarios;
- described the control measures and demonstrated a clear link to the major accident scenarios;
- explained the decision criteria for selecting the necessary measures to ensure risks are tolerable and ALARP;
- demonstrated adequate diversity and redundancy in the control measures (appropriate to the risk).

Mechanical safety

The findings of the hazard identification process should have been presented to demonstrate that safety critical mechanical equipment has been considered. There are two main functional categories:

- items containing dangerous substances which (on failure) have the potential to lead to a loss of containment (pipework, storage tanks, pressure vessels, rotating shaft seals, joint / seals, secondary containment);
- items which play a role in the prevention or mitigation of major accident hazards (relief valves, cooling pumps, emergency isolation valves, none return valves, excess flow valves, support structures.

The safety report should have described how systems and procedures (for example, management system controls for maintenance and inspection schemes) play a role in the prevention of major accident hazards. It should also have shown a clear link between identification and analysis of hazards with the selection of measures. A suitable hierarchical approach to the selection of measures should have been demonstrated.

Electrical, control and instrumentation safety

The operator should have described in safety report:

- how necessary instrumented safety functions are identified for major accident scenarios and by whom;
- how the required integrity of instrumented safety functions is determined and by whom;
- how, in general terms, other electrical, control and instrumentation measures such as fire and gas systems are applied to major accident scenarios (for example, by reference to process risk assessments).

The safety report should have contained (where applicable) a sample SIL determination record (for example, LOPA / risk graph output / QRA).

Pre-construction and pre-operation safety reports

The mechanical engineering assessment of a **pre-construction safety report** should focus on the front-end engineering design, identifying the technical requirements for the project (specifications for major equipment items, design code requirements and so on). The focus should also be on the conceptual design of a new installation - including demonstration that inherent safety principles were adopted within the design selection process. The identification of potential major accident hazards and associated technical measures to prevent loss of containment should have been considered.

The type of human factors information provided during the design phase should include reference to ergonomics standards and guidance and the human factors methods that were used to inform the design. A human centred design approach should be adopted where humans play a key role in the safe operation and maintenance of plant and processes. Task analysis may be used as a design tool to determine where machine interfaces are required, and to determine the likely staffing and competency requirements for operation. Design risk assessments should take account of human interactions with the system and the types of human error that could occur. This analysis can inform the appropriate allocation of function to human and / or machine. Overall, the information provided should demonstrate a structured approach to the inclusion and assessment of humans in the design.

The assessment of a **pre-operation safety report** should focus on amendments made to the design and construction and any additional information since the pre-construction safety report and whether the plant meets the design intent. Commissioning controls will also be an important assessment issue.

Where humans have to be accommodated for within the design there should be a process that ensures the 'as constructed' plant and process meets the intended design. This may be achieved by using methods such as walk through / talk through analysis. Prior to operation, there should be evidence of formal procedures being in place and arrangements being made for the selection and training of operators and maintenance staff. For major hazard risk these should include required responses to foreseeable upsets and emergencies. Overall, the information provided should demonstrate that a systematic structured approach has been applied to the inclusion and assessment of humans in the design and construction of plant and processes.

For large projects (involving external design / construction contractors) the operator's arrangements for managing outstanding issues / actions ('snag items') identified during 'pre-handover' inspection should have been described. Residual issues classified as 'low-risk' at the project handover stage (for example, incomplete painting of pipework systems) may impact in-service integrity, if timely remedial action is not taken.

Technical Elements - Significant Omissions and Serious Deficiencies

Examples of significant omissions – a failure to:

- identify all foreseeable causes of major accidents;
- describe or provide sufficient detail on the design basis / design standards adopted for mechanical plant and equipment forming the primary containment boundary;
- describe how the identification of potential direct causes of loss of containment (such as corrosion, erosion, and so on) has been conducted;
- provide sufficient information to support the necessary demonstrations, for example:
  - the absence of design, construction (where relevant) and maintenance records. A logical reason for the absence of documentation generated by the application of relevant good practice would be failure to apply relevant good practice;
  - inadequate description of chemical reaction hazard assessment methodology or management of change procedures;
- provide adequate information on control and instrumentation systems;
- demonstrate a system of prioritisation of maintenance for safety critical plant;
- describe how the safety management system addresses engineering issues such as:
  - functional safety management;
  - management of explosion protected (Ex) equipment;
  - technical competence of engineers, technicians and managers;
- address a topic that is likely to be relevant, for example:
  - functional safety at a chemical processing establishment;
  - lightning protection at a flammable storage warehouse;
  - electrical power systems at a large establishment
- recognise where the establishment is vulnerable to human failure and show that there is a system to identify appropriate control measures (for example, task analysis and human failure analysis) for safety critical operations and safety critical maintenance, inspection and testing activities;
- describe how operator interaction with process control systems (manual or via a DCS system) have been optimised, including allocation of function and design in accordance with ergonomic standards.

Examples of serious deficiencies – a failure to:

- consider safety and reliability at the design stage;
- consider safety and reliability in relation to operation;
- provide adequate information on the controls to prevent major accidents during maintenance activities;
- describe the maintenance and inspection regime to ensure the integrity of critical mechanical plant and equipment which contains hazardous substances;
- describe the procedures for assessing the mechanical integrity of proposed modifications to critical plant and equipment;
- demonstrate that the risk is acceptable, for example by submission of a seriously flawed SIL determination record that shows protective layers thought to reduce risk from an unacceptable level are invalid;
- demonstrate that there are no electrical ignition sources in an area where an explosive atmosphere was likely or very likely to be present;
- demonstrate that high power electrical equipment adjacent to major hazard plant is of adequate strength and capability;
- identify additional measures to make the risks tolerable where hazard studies show that there is an unacceptable risk associated with a particular hazard;
- provide a technical measure that would be regarded as good practice (for example, bunding or adequate pressure relief) without a suitable alternative;
- consider control measures other than human performance, for example, human response to an alarm as the only control measures for a process deviating from safe operating parameters.

4.1 *** It has been demonstrated that safety and reliability have been considered at the design stage

1) The establishment and installations have been designed to an appropriate standard

a) Mechanical safety

This criterion applies to all structures important to safety, such as pipe bridges, major vessels, pipework, rotating machines (including pumps and compressors) and valves, if they feature in major accident scenarios.

Examples of what could be included:

- reference to international design codes and standards (including justification of any deviations / exceptions adopted);
- reference to principal design parameters (design pressure / temperature) and category of construction (if applicable);
- if in-house design codes and standards have been adopted, their relevance and how they have been validated should have been provided;
- if no standards have been used, it should have been demonstrated how fitness for purpose of plant / equipment is assured;
- a description of design reviews conducted (for example, where novel designs are employed).

b) Electrical, control and instrumentation safety

The general approach to the application of electrical, control and instrumentation design standards should have been described.

c) Process safety

i. Hazard Studies

The safety report should have described:

- the link between the design and the associated hazard studies;
- how a hierarchical approach has been used and where inherent safety designs have been introduced where reasonably practicable (this may be difficult for existing plant but is relevant to the design of new plant and modifications).

It should have been demonstrated that the hazard studies (for example, HAZID, HAZOP, Fault Trees, FMEA, hazardous area classification, chemical reaction hazards assessment, SIL, LOPA assessments) are:

- sufficient to identify the hazards arising from the processes and the dangerous substances involved;

- appropriate for the scale and nature of the hazards presented (where appropriate by comparison with published standards);
- carried out by competent personnel with sufficient resourcing and independence;
- used correctly to inform decision making.

ii. Process description and use of standards

The safety report should have included the following:

- a clear description of each process summarising each stage and key control measures (for example, process flow diagrams);
- references to standards and codes of practice used as the basis for the design of the process and the selection of appropriate risk control measures;
- a demonstration that where the above standards and codes have been revised or new standards created, these have been considered (for example by gap analysis) and incorporated into installations, where this is reasonably practicable (this is particularly important if the changes relate to incident history or safety alerts);
- a demonstration that global or company standards (where they are used) align with appropriate published standards and guidance;
- the identification of where the design of equipment is not covered by published standards and codes together with a demonstration that safety and environmental protection is not compromised and that the risks are ALARP.

d) Human factors

The operator should have shown the following in the safety report:

- that there is a clear policy and / or procedure to ensure the application of inherent safety principles at the outset of the design and modification process;
- an acknowledgement that training is a weak control measure and therefore prioritises automation and user-centred design over procedures and training;
- that the implications of introducing human failure into an automated system (via design, inspection, testing, maintenance, and so on) have been acknowledged and addressed;
- where possible the human performance is further assured by mechanical or electrical means (for example, sequentially interlocked valves;
- that where procedures and training are to be relied upon as a risk control measure, it has been demonstrated that these tasks have been identified and analysed, that the analysis supports the development of the procedure and the procedure is used as the basis of the competence management system;
- that plant, equipment, workstations and control systems are designed with human performance in mind;
- how human factors are integrated in the design and commissioning process for all large projects. That;
    - human factors principles are integrated into design and development;
    - human factors are considered throughout the development lifecycle;

- relevant front-line personnel (both operations and maintenance) are actively involved in the design process;
- usability / operability are assessed and inform a user centred design;
- the design process identifies the procedural and training needs of relevant users;
- relevant general design standards have been applied on site.

2) A hierarchical approach has been used

This criterion has a closely defined four stage hierarchy: **eliminate** (inherent safety), **prevent**, **control**, **mitigate**, in that order of priority. There should be a clear policy and / or procedure to ensure the application of inherent safety principles to new designs and modifications. The approach to selecting prevention or mitigation measures should be proportional to the risks.

A hierarchical approach should have been considered in the safety report in relation to:

a) Mechanical safety

- appropriate selection of equipment to minimise or prevent the likelihood or consequences of failure, for example:
  - use of seal-less pumps;
  - use of corrosion resistant materials.

b) Electrical, control and instrumentation safety

The safety report should have described the application of suitable layers of protection. A typical approach could be:

- robust process control (including human interaction);
- alarms to indicate excursions from normal operating envelope;
- designated safety instrumented systems;
- a final protection system (often mechanical - that is, pressure relief systems – however it could be a high integrity safety instrumented system);
- mitigation systems.

The number of layers and the amount of risk reduction for each layer should be relevant to the consequence / severity of the range of potential hazardous events.

c) Process safety

The safety report should have considered (as appropriate):

- the use of less hazardous substances;
- reduction in the quantities of dangerous substances stored or used in the process;
- intensified processes (for example, use of smaller volume continuous / semi continuous processes instead of large batch processes, provided they can be properly controlled);
- inherently safer processes (for example, eliminate or reduce the risk of a runaway reaction);
- identification of the operational measures which prevent excursions / loads;
- demonstration of redundancy, diversity and availability of preventive measures;
- control systems (hardware) for hazards including corrective systems, shutdown/shutoff, venting and disposal;
- adequate preventive measures in the absence of control systems (for example, if a runaway reaction cannot be controlled, there are good measures to a standard or best practice for prevention of the runaway);
- the prioritisation of passive measures over active measures.

d) Human factors

The safety report should have considered (as appropriate):

- a hierarchy of control measures that aim to remove reliance on humans or improved system design where human performance has an unacceptable probability of failure;
- whether manual intervention in critical high-hazard systems (for example, manual emergency shut down of a continuous process) can be justified.

3) The layout of the plant prevents or reduces the development of major accidents

The plant layout should have been designed to prevent and / or mitigate major accidents. Plans, maps or diagrams showing the layout of process equipment, hazardous inventories, the separation of hazardous and less / non-operational hazardous areas, emergency utilities (for example, firewater) should have been provided (see also criteria 1.9 and 1.10).

The following should have been considered in the safety report:

a) Mechanical safety

This criterion is particularly relevant to pre-construction and significant modification safety reports where good layout (in the design phase) can significantly reduce risk.

The operator should have discussed in the safety report how the following were considered (where applicable) during design of the plant layout:

- plant separation / orientation (for example, equipment that might fail catastrophically, would it creating missiles);
- access requirements for periodic maintenance / inspection;
- providing for the removal of heavy plant and equipment for periodic maintenance / replacement;
- construction / maintenance activities (so to minimise the risk from dropped objects or eliminating the need to lift over live plant).

b) Electrical, control and instrumentation safety

Factors that could be considered include:

- the layout of control, instrument and electrical equipment has taken account of the needs of normal operations, maintenance and testing requirements and emergency operations;
- the location of occupied buildings, including control rooms;
- the layout of control room equipment has taken account of normal and emergency control conditions (for example, ergonomics of normal and emergency control panels);
- minimised vulnerability, and potential for common cause failure, of essential services to safety critical instrumented systems and key process control applications.

c) Process safety

- The safety report should have considered (as appropriate):

The safety report should have considered (as appropriate):

- separation of hazardous plant from the site boundary to reduce off-site risk, and to reduce the risk to the plant from off-site causes such as fires;
- safe positioning of occupied buildings;
- separation between hazardous plant(s) and storage areas to limit the spread of fire and other domino effects;
- segregation / separation of incompatible materials;
- separation of hazardous plant and processes from ignition sources, roadways or other activities that may impact on safety;
- adequate ventilation to aid rapid dilution of flammable atmospheres;
- low congestion of structures or lack of obstacles to gas flow that could aggravate the pressure effects resulting from the ignition of a released flammable substance;
- access for emergency services;
- adequate shelter for use during a toxic release, and adequate means of escape during other emergencies;
- access for inspection, testing, maintenance and repair, at all times throughout the life of the plant;
- hazardous interaction of released materials;
- human emergency response to process events (for example operatives being able to do what they need to do in the event of an emergency);
- vented material (for example, to mitigate exothermic runaway) goes to a safe and suitable location;
- the risks associated with equipment being adjacent to each other have been considered;
- separation of known ignition sources from large potential inventories.

d) Human factors

The safety report should have considered (as appropriate):

- plant and equipment, including layout on site, are designed with human performance in mind (for example, accessibility for inspection, testing and maintenance);
- the working environment (noise, temperature, lighting, and so on) has been considered;
- plant and components are clearly identified and labelled so as to reduce the likelihood of error;
- up-to-date P&IDs, schematics, line-diagrams, job-aids and other diagnostic tools are available for maintenance personnel.

4) The utilities necessary to implement any measure specified in the safety report have suitable reliability, availability and survivability

a) Mechanical safety

The safety report should have described:

- the potential effects of utility failure (in relation to major accident hazards);

- the likely impact of utility failure on safety critical mechanical equipment (for example, primary containment systems);
- the measures taken to ensure safety critical utilities will be available when required.

Examples of information that could be provided:

- design standards for equipment incorporated within safety critical utility supplies;
- details of the monitoring, testing, maintenance and inspection regimes employed for equipment incorporated within safety critical utilities (including back-up systems);
- utility failure (mechanical aspects) included in HAZOPs, PHA's, PHR's and so on.

b) Electrical, control and instrumentation safety

This criterion is generally more relevant to establishments that operate large or complex utility networks or rely on specific utilities to manage major accident scenarios. Electrical aspects of the criterion are generally more relevant to establishments that manage high voltage equipment (including through third parties) or large distribution networks.

The safety report should have demonstrated that the electrical and instrument air supplies (and any other fluid used to provide motive force to instrumentation, for example, nitrogen) have been designed to have suitable reliability, availability and survivability, including:

- the standards applied to the design of utilities;
- the sources of supply;
- the utilities that are essential for the operation of safety systems;
- the integrity requirements for utilities;
- any instrumented safety systems employed to maintain the integrity of utilities, for example, level alarms on fire water vessels;
- the use of diverse and / or back-up utilities;
- how it has been determined that electrical distribution equipment will not be overstressed;
- the standards that were applied to the design of electrical power system earthing;
- how the ignition risk from excessive stress voltages in Low Voltage (LV) distribution systems is managed;
- how high energy electrical equipment that poses a risk to major hazard plant has been identified and is being managed.

Where appropriate, the following records (or equivalent) should have been included in the safety report:

- a sample of a current electrical signal line diagram demonstrating diversity and / or redundancy of electrical supply;
- a sample fault energy level calculation for a typical High Voltage (HV) and a typical LV switchboard;

- a sample protection co-ordination study for a typical HV and typical LV substation / switchroom showing that adequate selectivity and protection has been achieved.

c) Process safety

The following may need to be considered:

- the role and significance of the utilities has been considered in design, construction, operation and maintenance, to ensure that these utilities and facilities will be available when required;
- the effect of loss of key utilities has been considered as part of a structured hazard identification / analysis process. This should have ensured that control systems and safety systems fail to a safe state and that the consequence of failure of a utility does not act as a major accident initiator. This includes the effects of loss of electrical supply on other utilities such as firewater provision, instrument and compressed air, nitrogen supplies;
- the reliability of safety critical utilities has been determined and independent backup supplies provided where necessary;
- each utility and its back-up system has been described;
- utilities which are essential for operation of key safety systems have been identified including the significance of a utility to a particular process (for example, cooling fluid to a vessel in which an exothermic reaction is performed). The reliability of back-up systems should have been demonstrated through monitoring, alarm and testing regimes.

Examples of utilities that should be addressed:

- water;
- steam;
- air;
- electricity (total or partial loss, power surge);
- cooling / heat transfer systems;
- inerting media.

Example where a utility should not be considered for prevention / mitigation:

- where water pressure and reliability of supply is critical, mains water supply should be avoided.

d) Human factors

The following may need to be considered:

- where appropriate, there is some means of ensuring that power supply to human control systems survives during a major accident, for example, via an uninterruptible power supply (UPS);
- UPS systems provide sufficient time to enable orderly shutdown and / or evacuation;
- UPS systems support all necessary instrumentation and equipment:
    - o control room interfaces; SCADA systems; mimic panels;
    - o level monitoring and gauging equipment;
    - o process alarms;
    - o site wide evacuation alarms;
    - o radio base stations;
    - o land line communication systems;
    - o ROSOVs and other remotely operated shut-down equipment;
- Hat there is adequate emergency lighting to carry out relevant shut-down tasks and, where appropriate, hand-held torches are available.

5) Appropriate measures have been taken to prevent and contain releases of dangerous substances

The operator should have described in the safety report the means by which dangerous substances (gas, liquid or solid) could be accidentally released from containment and the measures which have been provided to prevent such an occurrence. The suitability of measures to prevent or minimise releases should have been demonstrated.

i. Primary containment

All process, storage and any other equipment containing dangerous substances should have been designed to appropriate standards.

ii. Secondary and tertiary containment

The measures used to limit the consequences of loss of containment of a significant quantity of a dangerous substance should have been identified. The adequacy of the design and the capacity in relation to the maximum expected spill should have been demonstrated. The possibility of bund overtopping and containment of firewater[6] should also have been accounted for.

iii. Venting systems

The design basis for any venting system should have been justified taking account of foreseeable hazards (including loss of utilities or the effects of fire) and the safety consequences of venting.

iv. Isolation arrangements

[6] Guidance note to the industry on the requirements for fire-water retention facilities, Environmental Protection Agency 1995.

The emergency automatic and manual isolation arrangements to manage a release should have been described and justified including consideration of the time required to isolate. Appropriate performance standards for emergency isolation should have been stated and justified.

v. Detection of releases

The measures to detect a loss of containment or other incident at an early stage should have been described (for example, gas detection, level monitoring, loss of pressure, visual methods (cameras)).

The safety report should have described the mechanical measures in place to prevent and / or to contain releases and the integrity (function, reliability) of such measures and their survivability (that is, in the event of a fire / major accident).

The integrity and survivability (where applicable) of mechanical measures such as the following could be included:

- emergency shut-down valves (including fire-safe valve seating arrangements and discussion on performance standards, where applicable);
- manually operated isolations in safety critical duty;
- excess flow valves and non-return valves;
- rotating equipment (for example, protection arrangements from reverse rotation / overspeed, cavitation, dry running, deadhead connections, seal failure);
- joints (suitability for intended duty of flanged / screwed joints, couplings);
- temporary repairs (for example, clamps, wraps);
- dry break couplings;
- bellows and flexible joints;
- secondary containment.

The preventative and mitigatory measures that are in place for each scenario that could result in a MATTE should have been described. It should have been demonstrated that appropriate measures are in place to:

- stop or reduce a spillage at source;
- confine the spillage (the preference is for permanently engineered secondary containment systems fitted with an isolation device but other mobilizable resources may be considered if sufficient demonstration is made - for example the use of sandbags, drain seals and so on);
- recover and / or treat the spillage (for example, pumps, chemicals for neutralising or absorbing the spillage);
- for tertiary containment, effluent treatment, emergency shutdown and isolation systems (for example, penstocks and so on);
- the operator to deploy off-site measures if dangerous substances leave the site boundary.

6) All foreseeable direct causes of loss of containment that could lead to major accidents have been considered in the design of the installation

It is not acceptable for the safety report to have no explanation of how the identification of direct causes of loss of containment has been conducted. The following direct causes of loss of

containment (where applicable) should have been considered in the design of the installation and the selection of mechanical measures:

a) Corrosion (internal or external)

- systems for selection of materials for process equipment and systems that may be exposed to internal and external corrosive environments;
- variations in process conditions have been considered – the equipment design and materials of construction should accommodate foreseeable changes in the process conditions, such as variations in temperature, corrosive species (for example, during cleaning);
- consideration of inspection requirements during design (for example, to facilitate the detection and monitoring of corrosion under insulation);
- the potential for corrosion has been eliminated or reduced (for example, dead legs have been removed, buried lines minimised);
- corrosion is prevented or controlled by other means such as cathodic protection and / or the use of coating systems;
- corrosion is managed in other ways, such as employing corrosion allowances.

b) Erosion

- the effect of solids, abrasion, cavitation and phase changes.

c) External loading

- consideration as to the suitability of plant, equipment and structures to survive anticipated loadings from external sources, such as wind, rain and snow, as well as process and dynamic loadings (for example, design of equipment and piping system supports for use during construction and normal operation);
- assessment of potential risks to plant from lightning. Suitable protection systems to prevent / mitigate fire / shock and to provide surge protection systems should be installed where necessary (with references to suitable industry standards).

d) Impact

- during operation (for example, road tanker / fork lift truck impact);
- during construction and maintenance activities (for example, from swinging loads, dropped objects;
- from blast loadings (for example, due to catastrophic failure or adjacent equipment).

e) Pressure

- the installations are protected from the effects of excessive pressure and / or vacuum, and designed to recognised standards;
- pressure fluctuations are recognised as inducing fatigue failures.

f) Temperature

- high temperatures are accommodated in the design (for example, creep resistance) and / or protection systems are in place to prevent damage from excessive temperature;
- low temperature effects are avoided or controlled (for example, brittle failure, freezing effects);

- changes in temperature are controlled (for example, thermal fatigue).

g) Vibration

- consideration of both process-induced and machine-induced vibration (high and low frequency , as well as water hammer)
- show elimination (by design), prevention or control of vibration where possible;
- vibration induced fatigue is recognised (for example, provision of suitable supports for small bore connections).

h) Wrong equipment

- controls exist for the specification and supply of safety critical equipment and spares;
- management policies to minimise loss of containment (for example, avoiding the use of small bore fittings where possible).

i) Defective equipment

- identification / monitoring of pre-existing (design / construction) flaws in areas of high stress.

j) Ageing plant

- this refers to damage or material deterioration of plant or equipment. Ageing mechanisms (such as corrosion, erosion and fatigue) lead to an increased risk of loss of containment (see Research Reports RR509[7] and RR823[8], www.hse.gov.uk for guidance).

The safety report should have described (where applicable):

- the specified design basis for major equipment items and how the impact of the selected design (for example, pressure / temperature rating, material, corrosion allowance, and so on) on in-service operating parameters, inspection, testing and maintenance requirements is assessed;
- procedures for identifying ageing and determining the condition of mechanical plant and equipment (for example, from comprehensive inspection / maintenance history, measured corrosion rates or operational performance);
- assessment procedures / justification required prior to operating plant beyond its specified design lift (rather than repairing / replacing the plant). Requirements for increased inspection (to inform the assessment or to monitor ongoing condition of plant) should also have been described, where appropriate;
- reviews / gap analysis completed to compare the design of older plant (potentially affording lower integrity) with relevant up-to-date design principles and the consideration of further measures (such as de-rating equipment or reducing fill levels on storage tanks) to reduce risk to ALARP where appropriate;

[7] http://www.hse.gov.uk/research/rrpdf/rr509.pdf.

[8] Managing Ageing Plant, A summary guide, HSE Books

- any requirement for fitness-for-service / remnant life assessment techniques (such as API 579, BS 7910) to be employed, to enable major equipment items to be returned to service following inspection.

k) Human error

The safety report should have identified where operator error could be a direct cause of loss of containment without the structural failure of the primary containment boundary. This would include:

- identification of sources of human error in process operations (for example, mal-operation of valves and equipment, lack of hazard awareness, poor communication, unrealistic demands, lack of specific training or knowledge, and so on);
- identification of measures aimed at minimising human error (for example, dedicated storage and transfer systems, coupling design to prevent cross connection, and so on);
- assessment of the extent of safety criticality attached to human actions and how the design caters for this;
- realistic performance standards for safety critical functions during normal and emergency conditions;
- use of 'defence in depth' to minimise the effect of human failure;
- control of process design functions to minimise design error;
- control of maintenance and inspection activities to reduce human contribution to loss of containment during system invasive activities;
- training implications for loss of containment, hazard awareness, equipment specific training, and so on;
- failures derived from misuse of safety system overrides during normal operation or after maintenance, under temporary operating arrangements and so on.

7) The containment structure has been designed to withstand the loads experienced during normal operation of the plant and all foreseeable operational extremes during its expected lifetime

a) Mechanical safety

The safety report should have demonstrated the following:

- how the operator monitors and ensures that plant and equipment continues to operate within the design envelope and defined safe operating limits (for example, process control systems, alarms, trips);
- excursion relief is provided (for example, pressure / vacuum relief devices) where appropriate;
- testing regimes are in place to ensure that protection systems remain operable (for example, relief valve testing);
- that foreseeable extreme conditions (for example, during start-up, shutdown, process upsets and so on) have been accounted for in the design of plant and equipment;
- suitable margins exist between design and operating conditions;
- how fouling and other factors are managed.

The normal operating conditions of the plant and any foreseen operational extremes such as external loads, ambient temperatures and the full range of process variations (for example, normal operation, start-up and shutdown, turndown, process upset, emergencies) should have been described.

It should have been explained how safety margins are determined such that the safe working limits of the plant (pressures, temperatures, flow rates, liquid levels, and so on) are compatible with all expected operating extremes. Specific details should have been given where actual applied margins differ significantly from industry practice and the safety implications arising from the variation should have been described and justified.

8) The materials of construction used in the plant are suitable for the application

a) Mechanical safety

The safety report should have described the following:

- the approach taken to material selection, demonstrating that materials of construction are suitable for the substances being handled and the expected process conditions (temperature, flow and so on) noting that;
  - operator experience of material performance should not be solely relied on;
  - more expensive materials of construction are not universally better or more appropriate for aggressive environments;
- positive material identification procedures for materials of construction where uncontrolled variations would be critical;
- material of construction and coating system selection processes for plant and equipment operating in corrosive environments.

The safety report should have demonstrated:

- the compatibility between operating conditions and the material of the containment systems (for example, for known corrosive agents). The aggressive nature of the operating environment and operating conditions should have been linked to the material selection process for specified equipment;
- a consistent approach in the choice of materials rather than just a catalogue of materials specification for the whole plant.

The safety report should have described the parent metal inspection regime for verification of bought-in raw materials or equipment.

Corrosion and the products of corrosion can impact on the reliability of safety instrumented systems. The safety report should have demonstrated that corrosion / erosion potential has been taken into account in material selection and has affected the selection of equipment, for example:

- high / low pressure let-down;
- entrained solids;
- use of protective barriers for transmitters.

An awareness that products of corrosion may appear at locations remote from the affected instrumentation should also have been demonstrated.

9) Adequate safeguards have been provided to protect the plant against excursion beyond design conditions

a) Mechanical safety

The safety report should provide:

- a description of mechanical measures in place to prevent excursion conditions;
- demonstration that appropriate provision has been made for excursion relief by:
    - pressure or vacuum relief devices, or other pressure protection arrangements;
    - description where the nature of the process fluid may compromise effective operation of the relief devices (for example, fouling);
    - description of relief system testing regimes;
    - description of potential excursions (for example, overfill / underfill, starvation, cavitation, deadheading of pumps, and so on);
    - reverse rotation / overspeed of compressors or turbines;
    - provision of suitable measures within packaged units (proprietary packaged equipment may not meet the same standards adopted elsewhere in the overall design philosophy for the site).

b) Electrical, control and instrumentation safety

This criterion is generally more relevant to chemical processing establishments. For example, the description of a warehouse might be limited to environmental monitoring whereas the description for a chemicals processing establishment would provide an overview of the process control and safety strategy and key proves control and safety systems.

The safety report should have described the overall process strategy (for example, automatic control, manual control, automatic safety systems and alarm and operator action) and the types of installed control and safety systems, for example:

- distributed control systems;
- panel-mounted controllers;
- standalone control systems such as burner management systems;
- PLC-based packaged units;
- safety PLCs;
- individual hardwired instrument safety loops;
- alarm annunciators.

The safety report should also have described:

- how independence and separation between control and safety systems has been achieved;
- a system for determining, recording and reviewing safe operating limits and how these relate to control alarm and trip settings;

- how safety system settings are reviewed based on operating history and accounting for any modifications;
- the standards applied to alarm management.

c) Process safety

The safety report should have provided information on:

- the safety related controls and alarms designed to prevent or warn of excursions beyond safe operating limits and upon which the safety of the plant is based;
- how chemical reaction hazards are evaluated and a justification of the sufficiency of the control measures to prevent thermal runaway, over-pressurisation and loss of containment. This includes chemical manufacturing processes as designed and also accidental mixing of incompatible chemicals on site and the treatment of waste streams.

The safety report should also have included:

- details of the physical parameters of possible conditions: flows, temperatures and pressures with respect to excursions, runaway, worst case scenarios and so on;
- demonstration that the design standards and other applied codes of practice are appropriate to the conditions under which the design must work;
- demonstration that hazard identification has covered the possibility of beyond design conditions;
- demonstration that accident history for a type of plant has been considered where relevant.

A description of emergency prevention and protection measures should have been provided including:

- safety related controls and alarms designed to prevent or warn of excursion beyond safe operating limits and upon which the safety of the plant is based;
- the pressure relief and emergency venting arrangements - the method for the sizing of the pressure relief and emergency venting should have been specified;
- explosion relief;
- active and passive fire protection;
- occupied building risk assessment;
- interfaces with other measures designed to limit excursions beyond safe operating limits such as:
    - shutting-off feed streams;
    - shutting down of heat sources;
    - adding inhibitors to the reagent;
    - dump systems;
    - inerting;
    - flushing through of continuous processes;
    - application of process cooling;
    - shut-down of equipment;
    - sprinklers / water deluge;

- whether interventions are automatic or manual. For safety critical interventions, the safety report should have shown that the operator has examined the costs and benefits of automating the system and justified the suitability of the adopted approach.

10) Safety-related control systems have been designed to ensure safety and reliability

Electrical, control and instrumentation safety

This criterion is only relevant to establishments that manage functional safety. For example, it would not be relevant to warehousing unless environmental control measures such as temperature or humidity alarms are relevant to major accident scenarios.

The safety report should have described the following:

- the standards applied to the design of instrumented safety systems including process safety systems and machinery safety systems (for example, where machines are used in the manufacture of chemicals or explosives);
- the general approach to functional safety management;
- how it has been assured that persons involved in the design of safety instrumented systems are competent to carry out the activities for which they are accountable;
- how current relevant good practice (for example, EN 61508) has been applied as far as reasonably practicable to systems designed before its publication;
- how instrumented safety systems with a required integrity of less than SIL 1 are managed;
- the design of alarm systems including how the reliability of the operator is taken into account;
- the extent to which fire and gas detection systems are used to initiate executive action (for example, deluge systems, inerting systems, automatic dump systems and so on).

Where applicable, the safety report should have contained the following records or equivalent:

- sample safety requirements specification;
- sample SIL assessment record (for example, PFD calculation and fault tolerance assessment);
- sample record of competence for an individual involved in the design of safety instrumented systems or in the review of safety instrumented systems against relevant good practice.

Human factors

The safety report should have described how the potential for human failure is acknowledged and systematically treated in the design of safety instrumented systems.

Tasks should have been identified where:

- human failure could lead to a demand on the safety function (for example, errors in setting process parameters, conflicting responsibilities that may distract the operator's attention, unauthorised use of system overrides, and so on);
- human action could reduce the demand rate on the safety function (for example, responding to alarms);
- failure of the safety function requires actions to mitigate the consequences of the event.

The levels of risk reduction claimed for alarm systems should have been realistic and should have considered:

- availability of the operator to respond;
- adequacy of time to respond;
- the potential for alarm flooding;
- whether the operator knows how to respond (for example, a clear, documented response for each critical alarm, supported by training).

Assumptions about human performance in the control system are documented and an example could be included in the safety report.

The safety report should have identified and addressed human failures that increase the likelihood of the safety function failing to work on demand (inspection, testing, maintenance, calibration and so on).

The safety report should have described how the potential for operatives to override safety functions has been identified and assessed.

The availability of human control systems during upset and emergencies (for example, can operatives reach shut off valves) should have been considered (where appropriate).

11) Systems which require human interaction have been designed to take into account the needs of the user and to be reliable

The safety report should have identified safety critical operations carried out by operatives and how they know when to intervene to carry out such operations.

The operator should have justified the assumptions regarding the availability and integrity of required human response during foreseeable normal and emergency operating states. In particular, the following should have been addressed:

- important process safety critical control actions would not be jeopardised by changes in staff arrangements;
- the time to achieve operations has been taken into account;
- the safety of the design will otherwise not be critically compromised by failure of required operative response due to foreseeable causes (for example, lack of training, human response under high stress, exposure to hazards preventing required action and so on);
- suitable performance standards have been developed and are monitored for safety critical operator functions;
- an adequate response will be achievable where operative intervention is a safeguard (for example, for detection and correction of deviations);
- for batch plant operations, consideration of possibility of steps being omitted / repeated / carried out in the wrong order.

If human response is safety critical, evidence that the operator has examined the costs and benefits of having an automated system should have been provided and the suitability of the adopted approach justified.

It should have been shown in the safety report that over-reliance on operatives to prevent, control or mitigate hazardous events has been avoided.

Process control systems which are highly reliant on human intervention to keep the process within safe operating envelopes should have suitable independent safety layers of protection to prevent or mitigate hazardous events. For such arrangements, the assessment should examine the potential for high demand rates on the safety related layers of protection.

Where the operative is part of a safety related control loop, and so has a performance function, the reliability with which the operative performs the function should have been realistically assessed.

Information should have been provided in the safety report to describe how the effects of alarms experienced by operatives in normal operation have been assessed, including the potential for alarm flood situations in the event of an emergency or shutdown.

Where the reliability of human action is critical, the safety report should have included:

- references to design standards;
- usability assessments;
- indications of operative involvement in setting reliability criteria;
- compatibilities with other systems;
- consideration of teams for dealing with continuous improvement;
- appropriate standards for ergonomic design that include control and alarm display interfaces;
- workspace design considerations (such as heat, light, noise, interface, physical access);
- alarm handling design and procedures (form, numbers, priorities, actions required, management of overrides);
- evidence of correct allocation of function, especially of new plant and for emergency shutdown arrangements;
- avoidance of undue reliance on special or rarely used automation or procedures or unusual or rare judgement.

It should have been shown in the safety report that the design process for manually operated equipment and controls ensures that the needs of users are fully taken into account including:

- usability and maintainability assessments;
- the participation of operatives from an early stage;
- identification of training needs;
- where reliable response to alarms forms part of the demonstration, effective action has been taken to ensure usability and compatibility with suitable standards.

The operator should have shown in the safety report that the usability and error potential of existing safety-critical manual tasks or interventions (for example, critical connections or disconnections, critical alarms and controls) are understood and action has been taken to minimise potential hazards that may arise.

i. Manual control of systems

Where there is a reliance on human performance to keep a system within design parameters manually, the safety report should have described those measures taken to ensure human reliability. For example:

- plant (for example, valves, flow direction and contents of pipework) and materials (for example, chemicals added manually to batch processes) are clearly labelled;
- information about the status of the process is available to the operative (for example, pressure gauges, sight glasses) and appropriately located;
- procedure design has been optimised to support the operative in the field;

Process control systems are designed to inform the operative if unsafe parameters are entered into the system.

ii. Control room and interface design

A description of the control room environment (where relevant) and associated process control systems should have been provided. The following should have been demonstrated:

- relevant standards and recognised good practice are applied during upgrades and modifications of existing control room interfaces, as well as the design of new control systems;
- design criteria encompass control room arrangements and layout, panel workstations, displays and controls, environmental conditions (lighting, acoustics, ventilation, temperature and so on);
- the experience of operators and engineering / maintenance personnel is captured and fed back into the upgrade process;
- DCS and SIS training / assessment covers specific, local operational issues as well as generic functionality of the interface and familiarisation with system operating manuals.

iii. Alarm handling

The safety report should have outlined the philosophy with regard to the design and management of alarms and described how:

- alarm handling is fully integrated into the design process;
- the design process acknowledges and accommodates human capabilities and limitations (including operative availability to respond, time to respond, the potential for alarm flooding and so on);
- alarms will be justified and prioritised;
- alarm systems are subject to continuous improvement (for example, there is a clear link between process change and alarm system upgrade);
- relevant performance measures are defined and monitored (average alarm rate, upset alarm rate, average number of standing alarms and so on);
- bulk tank capacities and alarm set points are clearly defined to ensure there is sufficient time for detection, diagnosis, planning and action;
- alarm systems alert, inform and guide required operative action (including a defined, documented response for each safety critical alarm, supported by training and assessment.

12) Systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk have been described

a) Mechanical safety

The safety report should have demonstrated that:

- mechanical equipment used in potentially explosive atmospheres is designed to be safe;
- suitable international standards have been used to identify potential ignitions sources from mechanical equipment including:
  - heat energy (hot surfaces, hot work, heating installations);
  - mechanical energy (overheating, friction, impact, grinding, compression);
- suitable inspection, testing, cleaning and maintenance regimes have been implemented (to minimise ignition sources occurring as a result of overheating or fault conditions).

b) Electrical, control and instrumentation safety

This criterion is equally relevant to all establishments where potentially explosive atmospheres might exist.

The safety report should have described:

- the standards applied to:
  - the design and selection of explosion protected equipment;
  - the design of lightning protection systems;
  - the management of hazards due to static electricity;
  - control of ignition of flammable atmospheres by radio-frequency radiation;
  - the management of cathodic protection in explosive atmospheres;
  - the management of lift trucks in potentially explosive atmospheres;
- how the requirements for lightning protection and surge suppression systems were established and an overview of the systems;
- how it has been assured that persons involved in the design of explosive atmosphere installations are competent.

Where applicable, the safety report should have contained records of sample initial radio frequency assessment or equivalent.

c) Process safety

The following should have been addressed in the safety report:

- that the operator has an explosion protection document that complies with *Part 8: Explosive Atmospheres at Places of Work of the General Application Regulations*;
- that the procedures and policies for identifying hazardous areas are based on established codes and standards and are applied consistently;
- that releases of flammables through vents, from leaks from gaskets and when equipment is opened have been considered (that is, where the leaks are likely to occur and what the release parameters and flammable properties of release materials are likely to be);

- that the hazardous area classification data is used in the selection and location of equipment and its maintenance and in considering plant and process changes;
- the location of ignition sources in relation to loss of containment events have been identified. The major accident hazard risk assessment may indicate that further risk reduction measures are required such as removal of ignition sources or provision of protected electrical equipment in other areas, for example, closure of adjacent roadways during tanker loading / offloading, provision of protected lighting.

A map showing areas with explosive atmospheres (ATEX zones) should have been included (see also criterion 1.4).

4.2 * It has been demonstrated that safety and reliability to prevent major accidents and reduce loss of containment have been considered during construction

This criterion applies to the construction of **new** and **recent** plant (for example, as part of a modification) so as to gain assurance that the construction phase will be effectively managed. The assessment of the criterion in existing establishments is likely to be associated with modifications involving new plant integrated with old systems. The safety report should have provided information such as:

- reference to international codes and standards;
- reference to a category of construction (if applicable);
- explanation of the relevance and applicability of codes and standards.

Mechanical safety

The safety report should have provided evidence to demonstrate that the initial inspection, testing and commissioning of the plant have been documented and the information is retrievable (particularly for plant / equipment forming the primary containment boundary). Where this information is not be available (for example, for older or second-hand plant), the safety report should have described how major accidents are prevented / plant integrity is demonstrated, by discussing, for example:

- inspection history (older plant);
- post-installation baseline inspection data (second-hand plant);
- any operating restrictions.

Electrical, control and instrumentation safety

This criterion is generally relevant to the construction of all establishments. However, functional safety assessment will only be relevant to chemicals processing establishments where functional safety is a consideration.

The safety report should have described:

- the standards applied to the construction verification of:
    - safety instrumented systems;

  - explosion protected (Ex) equipment;
  - electrical power systems;
- the process for ensuring that the electrical, control and instrumentation equipment and systems are verified against the appropriate standards to ensure adequate safety prior to the major accident hazards being present.

The safety report should have included the following records or equivalent (where applicable):

- sample functional safety assessment;
- sample initial Ex inspection record;
- record of competence of the persons who carried out the initial inspections;
- sample industrial low voltage fixed installation inspection and test (verification) record.

4.3 *** It has been demonstrated that safety and reliability have been considered during operation

a) Mechanical safety

The safety report should have demonstrated how the documented operating procedures assure that mechanical plant and equipment are always operated within safe limits (for example, procedures should prevent damage to plant or components from occurring during operational extremes such as start-up and shut-down - see also criterion 2.5).

The procedures in place to control temporary constraints during the operational life of the plant should have been addressed, for example:

- over-riding of safety devices to allow for maintenance work;
- running automated systems in a manual mode;
- emergency shutdown of equipment;
- isolation or part-isolation of manifolded systems.

b) Electrical, control and instrumentation safety

The safety report should have described the control of operation of electrical switchgear, including the control of switching by subcontractors and distribution network operators. The procedure for identifying, reporting and investigating the failure of electrical, control and instrumentation protective measures against major accidents (relevant to all establishments where such measures exist) should also have been described.

The control of overrides of safety instrumented systems is only relevant to establishments that manage functional safety (for example, it would not be relevant to warehousing unless environmental control is a major accident control measure).

In the context of major accident hazards, the safe operation of electrical switchgear and the authorisation of personnel to operate electrical low voltage (LV), high voltage (HV) and generation systems are only relevant to establishments that manage such equipment or systems. (It would not apply to a warehouse with a simple distribution network that complied with the National Rules for

Electrical Installations). A sample record of authorisation for person(s) authorised to operate such equipment should have been included in the safety report.

4.4 ** It has been demonstrated that safety and reliability have been considered for maintenance activities associated with major accident hazards

1) An appropriate maintenance scheme has been established for plant and systems to prevent major accidents or reduce the loss of containment in the event of such accidents

a) Mechanical safety

The safety report should have described:

- the maintenance administration system (relevant job descriptions, roles and responsibilities including an organogram if appropriate);
- the maintenance regime for safety critical plant;
- the systems for periodically reviewing the suitability of the maintenance regime (based on findings / failure history);
- the maintenance philosophy for mechanical plant and equipment (for example, based on time, condition, reliability);
- the systems for prioritisation of maintenance activity, especially relating to safety critical plant;

Examples of information that could be provided:

- details of the personnel (employees, external contractors) completing key mechanical maintenance activities and an overview of competency requirements;
- examples of safety critical maintenance activities completed on mechanical equipment (for example, bench testing of pressure relief devices);
- examples of relevant performance monitoring procedures such as process safety performance indicators) including confirmation that data is reviewed by senior management.

b) Electrical, control and instrumentation safety

This criterion applies equally to all establishments. However, maintenance standards on functional safety would be unlikely to apply to a flammable storage warehouse due to the absence of chemical processing but standards on explosion protected equipment and lightning protection would apply.

The safety report should have described:

- the maintenance management system including:
  - how scheduled work is planned and prioritised;
  - how defects are prioritised and repaired;
  - how reactive work is prioritised;

- the location and structure of the electrical, control and instrumentation safety critical elements inventories (for example, ex-rated equipment, SIS, electrical supplies);
- the strategy and methodology for monitoring and control of the condition of the equipment;
- the strategy for managing obsolescent electrical, control and instrumentation equipment;
- the standards applied to the maintenance and proof testing of safety instrumented systems and how this is managed;
- the standards applied to the maintenance and inspection of equipment (fixed and moveable) in explosive atmospheres and how this is managed;
- the standards applied to the maintenance and inspection of electrical power systems and how this is managed;
- how it has been assured that persons involved in the maintenance of electrical, control and instrumentation equipment and systems are competent.

The following records (or equivalent) should have been included (where applicable):

- sample SIS proof test procedure or sample record of completed SIS proof test (functional safety);
- equipment in explosive atmospheres:
    - representative sample of periodic explosion inspection records (or records of continuous supervision) including protection concepts Ex d, Ex e, EX N, Ex i and Ex tD where they exist on site;
    - record of competence of the persons who carried out the inspections (or continuous supervision);
    - sample tests and inspection records for:
        - lightning protection and static earthing systems;
        - detection systems for flammable and toxic gases, and fire;
- electrical power systems:
    - sample inspection and test records for:
        - HV / LV transformer and switchgear;
        - electrical power system earthing;
        - emergency generator periodic inspection, maintenance and test (no load and / or load).

c) Human factors

The operator should have shown in the safety report that there are measures in place to detect, monitor or avoid maintenance error. The following should have been described:

- how the operator's methodology for human failure analysis has been applied to safety critical maintenance tasks;
- the competence of maintenance personnel (for example, training using recognised schemes, ongoing refresher training);
- the maintenance activities that could lead to major accidents;
- the controls that are in place to ensure these accidents are very unlikely, including:

    - physical barriers and guards;
    - administrative controls (permits, procedures, checklists);
    - management controls (supervision and checking of tasks).
- confirmation that maintenance tasks are well-designed (for example, no time pressure, comfortable conditions) including:
    - how the maintenance programme is based on major accident risk assessment;
    - how communications are controlled during and between shifts;
    - arrangements for the care of temporary or inexperienced maintenance technicians and contractors;
    - inspections of maintenance tasks in progress;
    - identification of equipment that cannot be inspected under normal circumstances (for example, some tubes in steam boilers may not be accessible);
- how the ease of maintaining systems and continual improvement is achieved;
- how early signs of problems are monitored (for example, a large backlog of jobs / excessive repair times / adverse feedback from staff);
- how the investigation of near misses and accidents is used to learn from human failure in maintenance and to improve the systems;
- where activities are out-sourced, the arrangements to retain adequate technical competence to judge whether, and ensure that, work is done to the required quality and safety standards.

2) Maintenance procedures take account of any hazardous conditions within the working environment

The safety report should have included an overview of the mechanical isolation practices adopted on site, prior to completing intrusive activities on plant or equipment containing hazardous substances (as they relate to major accident hazards). A description of how the mechanical isolation procedures fit into the overall maintenance management procedures (for example, permit to work) should have been provided.

Similarly, the safety report should have described how safe systems of work are applied to electrical, control and instrumentation maintenance activities and how electrical safety rules, including isolation of electrical supplies, are applied to maintenance activities. While this criterion applies equally to all establishments, only safe systems of work that are specific to electrical, control and instrumentation maintenance activities and are not covered by safe systems of work defined by the site SMS need be described.

3) There is a system in place to ensure that safety critical plant and systems are examined at appropriate intervals by a competent person

Mechanical safety

This criterion is concerned with in-service integrity of safety critical plant. It does not apply to pre-construction safety reports. However, pre-construction and pre-operation safety reports should have demonstrated that a suitable Written Scheme of Examination is in place (and initial inspection by the competent person has been completed) prior to introducing pressurised hazardous substances on site.

The safety report should have described:

- the periodic in-service examination regimes adopted for all plant containing hazardous fluids (includes pressurised and atmospheric systems, pipework and so on);
- the procedures for analysing inspection findings and confirming that safety critical plant is endorsed for a period of operating service (before the next examination is required);
- the role of external accredited organisations (where applicable);
- how inspection regimes and schemes of examination are reviewed to ensure they remain suitable and sufficient.

Examples of information that could be included to assist demonstration. Information on:

- systems for the prioritisation of safety critical equipment;
- independence and competence of inspection staff;
- justification of inspection scope and frequencies by reference to relevant industry standards (where appropriate) and to analysis of inspection findings;
- appropriate systems for managing follow-up actions resulting from periodic inspection.

Where risk based inspection is carried out, the operator should have shown in the safety report that:

- the assessment team has the relevant experience and knowledge;
- a thorough and systematic process is used to identify all relevant degradation mechanisms and likely sites (relevant industry guidance should be referenced where appropriate);
- a suitably cautious approach is taken to changes in inspection frequency as shown by the risk based inspection process, with the competent person involved in any modifications to the schemes of examination.

Human factors

The safety report should have demonstrated that there are:

- suitable procedures for examination, inspection and proof testing, with clear pass / fail criteria;
- arrangements to ensure:
    - personnel / contractors who conduct such activities are competent to do so, and are fully aware of related major hazards and their consequences;
    - an intelligent customer capability is retained where activities are out-sourced.

4) There is a system in place to ensure the continued safety of the installations based on the results of periodic examinations and maintenance

This criterion applies equally to all establishments but only in relation to the extent of the installed electrical, control and instrumentation systems. For example, performance monitoring of safety instrumented systems would be unlikely to apply to a flammable storage warehouse due to the absence of chemical processing but performance monitoring of explosion rated equipment would be likely to apply due to the presence of potentially explosive atmospheres.

The safety report should have described:

- performance monitoring of electrical, control and instrumentation systems and equipment, including the use of safety performance indicators such as faults and failures found during operation, inspection and testing;
- how the results of performance monitoring are used to ensure the continued safety of the installations.

4.5 ** It has been demonstrated that there is a system for ensuring modifications are adequately conceived, designed, installed and tested

a) Mechanical safety

The safety report should have demonstrated:

- that changes to existing plant and mechanical equipment are included in the modification procedure;
- how the potential impact of new equipment is assessed;
- how technical approval is carried out (to show that the concept has been properly addressed for mechanical integrity);
- how post-construction / implementation review is carried out (to confirm that the design intent of the modification has been met);
- that there are procedures for integrating new plant and equipment within existing integrity management arrangements.

b) Electrical, control and instrumentation safety

This criterion applies equally to all establishments. However, the need is only to describe change management systems that are specific to electrical, control and instrumentation measures and that are not covered by change management systems defined by the site safety management system. The management of change to safety instrumented systems would be unlikely to apply to a flammable storage warehouse due to the absence of chemical processing.

The safety report should have described:

- how the impact of electrical, control and instrumentation safety systems, equipment, operation and maintenance are addressed when carrying out plant and process modifications;

- how management of change is applied to safety instrumented systems.

Where applicable, the safety report should have contained a sample record for management of change showing consideration of instrumented safety systems.

c) Process safety

The safety report should have described the management of change procedure including:

- the criteria for determining when a process change is sufficient to go through a formal management of change process;
- whether a process change needs a formal hazard study / risk assessment;
- whether the hierarchical approach is used where practicable in relation to process modifications and changes;
- the competence and independence of the personnel involved in the decision making;
- the method for ensuring that the modification is installed as specified in the change proposal;
- the system for dealing with changes, updates or modifications to:
    - plant and equipment;
    - process parameters (for example, temperature, pressure);
    - operating procedures and other documentation;
    - raw material specifications, suppliers and so on.

d) Human factors

The safety report should have demonstrated that human factors are integrated into major projects, for example, by:

- ensuring that specific human factor activities are built in to project plans and are sufficiently resourced;
- understanding and specifying the context of use:
    - who the users are;
    - what it is they will be doing;
    - assessing the impact of the change on workload and staffing levels;
- ensuring that descriptions of user characteristics and tasks analysis are considered as the basis for design;
- specifying the user and organisational requirements, and ensuring a balance between user-centred design options and relative cost;
- applying human factor expertise to generate design options which meet user requirements (planning in time for iterative design and relative cost);
- evaluating requirements by involving target users and human factor specialists, where this is appropriate.

The safety report should have described how:

- the design considerations outlined above have been addressed;
- the management of organisational change procedure has been applied;

- human reliability has been robustly addressed in the new design;
- procedures have been updated to reflect change;
- additional training and assessment have been provided.

5. Assessment of the Emergency Planning Elements

Pre-construction and pre-operation safety reports

Pre-construction safety reports should have described emergency response arrangements to the extent that information is available and in relation to the major accident hazards at the establishment. Relevant content may include but is not limited to:

- control and limitation of escalation of major accidents, including isolation and removal of inventories;
- communication during emergency response;
- emergency control centres;
- access routes;
- design and construction of moveable response resources, particularly nearer pre-operation stage;
- arrangements during phased commissioning of plant.

Training in emergency response, testing of emergency plans, and provision of information for the EEP is more relevant to pre-operation safety reports.

While there may be gaps relating to emergency response content in a pre-construction safety report, the pre-operation safety report should have demonstrated that the emergency response arrangements meet the requirements of the COMAH Regulations.

Emergency Planning - Significant Omissions and Serious Deficiencies

Examples of significant omissions:

- the arrangements for training staff in the duties they will be expected to perform in implementing the internal emergency response have not been described;
- the arrangements for providing early warning of an incident to the local authority responsible for setting the EEP in motion have not been described;
- adequate information has not been provided on the intervention arrangements in an emergency;
- it has not been demonstrated that possible loss of essential services or other utilities has been considered;
- the arrangements to terminate a release or mitigate the consequences of a major accident are inadequate;
- the LCAs have not been consulted;
- the system for alerting persons to the hazardous situation is not appropriate (for example, in the absence of an alarm, the operator proposes to telephone persons in the public information zone);
- it has not been demonstrated that equipment is compatible with that provided by the LCAs.

Examples of serious deficiencies:

- the internal emergency plan (IEP) arrangements have not been linked to the foreseeable major accident scenarios which could occur at the establishment;
- the description of the key elements for internal emergency response taken as a whole (that is, preparation, testing, review, training and mobilization) is inadequate;
- the public have not been informed of the action to take;
- arrangements have not been described for unstaffed sites, out of hours;
- the IEP has not been tested or inadequately tested.

5.1 *** The organisation of the alert and intervention in the event of a major accident has been described

The safety report should have described the following:

Basic operational issues necessary for emergency response including:

- the provisions for establishing and maintaining communications during the emergency response;
- the nature and location of areas such as:
  - emergency control centres;
  - first aid centres;
  - emergency refuges;
  - muster points;
  - pre-defined forward control points;
  - any identified secondary, back up locations .

Arrangements for raising the alert to the hazardous situation:

- to cover persons on site, the general public, neighbouring establishments, local authorities, Irish Water, persons with a private well (where relevant);
- description of the nature of the alarms and the plant conditions required to activate them;
- the roll call and search and rescue arrangements.

Arrangements for intervention in an emergency situation:

- the initial actions required both on-site and off-site in response to alarms / warnings and the prevention of domino effects;
- the arrangements for controlling and limiting the escalation of accidents on-site, including:
  - the isolation of hazardous inventories and the removal of inventories (where appropriate);
  - the use of fire fighting and other mitigatory measures;
- the nature and location of any pollution control devices and materials, and the arrangements for subsequent environmental clean-up and restoration;

- details of how wind speed and direction, and other environmental conditions will be monitored.

Where relevant, or where more rigorous or detailed demonstrations are required, the safety report should have considered the following:

- how the effects of emergency response actions, including fire-fighting activities, will minimise the overall impact on human health and the environment (for example, due to contaminated firewater) - this should include short term and long term effects and alternative options for disposal or discharge together with the least damage solutions and the circumstances in which they apply;
- the nature of, and arrangements for maintaining, any mutual aid agreements with nearby establishments;
- the nature and location of any installations which may require special protection, or rescue intervention;
- the arrangements for unmanned sites and sites that are not continuously manned, and sites with varying manning levels at different times;
- the evacuation arrangements and any transport requirements;
- the location of:
    - access routes for emergency services;
    - rescue routes;
    - escape routes;
    - any restricted areas;
- the arrangements and conditions for alerting and mobilising:
    - persons (on-site and off-site) with defined responsibilities under the IEP;
    - the emergency services (including arrangements for briefing them and of any special problems they might face);
    - neighbouring establishments (where mutual aid agreements exist);
    - relevant off-site agencies.

5.2 *** It has been demonstrated that suitable and sufficient on-site and off-site resources can be mobilised to limit the consequences of a major accident to human health and the environment

This criterion is considering the adequacy of the equipment selected to limit the consequences of the foreseeable major accident scenarios identified in the safety report. Sufficient detail should have been provided to show that the mobilizable resources which may be relied upon are fit for purpose. The safety report may show the following where applicable:

- an example of an emergency pre-plan which has been drawn up in accordance with the Energy Institute (EI) Part 19 – 'Fire Precautions at Petroleum Refineries and Bulk Storage Installations', or similar;
- the estimated amount of water or foam needed to mitigate the consequences of a major accident scenario and confirmation that this can be achieved in practice;
- the timescale in which the equipment will be available for use;

- that the equipment can function effectively in all expected environmental conditions and if there is a loss or utilities or similar;
- the use of personal protective equipment (PPE) (for example, breathing apparatus, respirators, chemical suits and so on), has been identified and the amount of each has been determined and is available;
- that the fire fighting roles of the on-site personnel are complementary to the role of the off-site emergency services;
- adequate consideration has been given in the design (for example, the positioning of walls, fire screens) to assist the positioning and protection of fire fighting equipment and personnel;
- the reach of the fire protection and extinguishing equipment is appropriate;
- adequate consideration has been given to flammable substances being carried with fire water and spreading the fire other areas, including details of any potentially incompatible substances and any additional mitigatory measures in place to limit the consequences of a major accident hazard;
- suitable and sufficient portable and mobile fire fighting equipment (for example, mobile monitors, mobile pumps, hand / portable extinguishers, foam generation equipment, hoses and hydrants) have been located at appropriate points throughout the establishment according to the hazard.

1) Personnel

The safety report should have demonstrated that sufficient personnel can be made available within appropriate timescales to carry out the mitigatory actions required by the IEP taking account of the following:

- the posts required to implement the IEP have been identified:
- the numbers of personnel, with the appropriate expertise and training, required to achieve the necessary level of response have been determined and they can be assembled within the necessary response time;
- the mitigatory actions are achievable in practice, particularly in the early stages of the incident, given the rate at which the incident could escalate (for example, plant in the vicinity of a major fire may not receive water spray protection from external responders for at least 20 minutes);
- the potential incapacity of personnel (for example, due to sheltering from the incident, casualty of the incident, absence from site and so on), where they have a key role in the IEP.

Where applicable, the report should have described:

- how the number of people and the functions required have been determined;
- how deputising arrangements for key roles have been assigned and how it can be assured that required staff are available;
- key functions / roles fulfilled by third parties and how their skills or competence are assured;
- information taken from analysis of the general suitability of mitigatory actions.

2) Provisions to minimise the release of, and mitigate the consequences of, airborne toxic and / or flammable substances

The safety report should have considered:

- measures to terminate or reduce the leak at source (for example, patching or plugging of leaks, isolation by valve closure or other means);
- measures to reduce the evolution of fumes from hazardous materials that have already been spilled (for example, foam cover, surface cooling of the spilled material);
- measures to reduce the effects of airborne substances (for example, water sprays to absorb soluble fumes and / or to promote dilution by mixing with air);
- the practicability of carrying out such actions in the foreseeable accident conditions;
- the equipment, tools and PPE that would be required to carry out these tasks.

3) First aid provisions / medical treatment

The safety report should have demonstrated that suitable consideration has been given to the first aid / medical provisions required in the event of a major accident and how the on-site provisions dovetail with the provisions in the EEP.

Examples of information that could be included:

- reference to the number / availability of trained first aiders;
- a description of the facilities available at the establishment;
- confirmation of both the expectations and limits of the first aiders training;
- a description of how the liaison with the local health authority and ambulance services has been carried out, making reference to how the operator's casualty control or decontamination strategies have been determined.

4) Provisions for any ancillary equipment, which may be required during the emergency response

An outline of the equipment which is intended for use should be provided. If there is a reliance upon a third party to supply plant or services, the safety report should have described the equipment needed and explained how this will be sourced, including estimated timescales for its arrival on site.

Examples of ancillary equipment:

- vehicles to transport emergency equipment to and from the site of the accident;
- heavy lifting equipment;
- earth moving equipment;
- emergency lighting,
- special tools, parts, and so on, required to carry out emergency repairs and actions.

5) Provisions for the restoration and clean-up of the environment following a major accident

The safety report should have identified the potential need for restoration and clean up measures including:

- the envisaged timescale over which temporary containment may be required;
- the arrangements made to ensure that such facilities would not pose an unacceptable threat to human health and the environment;
- suitable disposal arrangements;
- whether it is anticipated that the environment can be restored and the measures and timescale of restoration.

Examples of measures to be taken:

- monitoring / sampling arrangements (air, water, groundwater and land);
- equipment to contain toxic substances;
- agents to soak up and / or neutralise contaminants;
- earth moving equipment for the removal of contaminated soil and other material;
- booms and skimmers for spillages to water;
- temporary storage arrangements (for example, portable storage tanks for the contaminated material, detection / protection systems);
- measures for groundwater remediation.

Where an external company is responsible for delivering these measures, the safety report should have provided evidence that they are appropriate. For example:

- the operator has a contract with an external contractor;
- the contractor can deliver the necessary measures within the required time frame.

The safety report should have demonstrated that sufficient financial resources will be available to deliver the measures identified above in relation to major accidents to the environment (useful guidance on this issue has been provided by the Environmental Protection Agency[9])

[9] Guidance on Financial Provision for Environmental Liabilities. Environmental Protection Agency 2015.

5.3 *** The arrangements for the maintenance, inspection, examination and testing of the mobilizable resources and other equipment to be used during the emergency response have been described

The safety report should have provided evidence that suitable arrangements have been made for the maintenance (planned and breakdown), inspection, examination and testing of emergency response equipment and provisions for which the operator has responsibility.

In the case of equipment which the operator may rely upon but does not have responsibility for, the following information should have been provided:

- confirmation of the operator's arrangements to ensure that the equipment is maintained in an efficient working order such that it would be available for use and provide the necessary function when called upon;
- details of type of equipment covered;
- information on the scheduling of maintenance activities on such equipment.

5.4 ** It has been demonstrated that emergency response training is carried out

The safety report should have demonstrated that emergency response training is carried out for all members of staff with a specific role in the event of a major accident, as well as the training / information needs of other employees, contractors and visitors to the site. The training should be kept up to date.

The safety report should have indicated that the training includes the following where relevant:

- information on the major accident scenarios which may trigger the IEP and the EEP;
- the nature of major accidents posing a threat to the environment and the particular steps to take in the event of such accidents;
- knowledge of the alarm systems and the required response to each alarm;
- the procedures for reporting and responding to incidents on site which have the potential to escalate into a major accident;
- the use of the resources which may be mobilised in the event of a major accident;
- the use of PPE and any limitations on its use;
- the evacuation and mustering procedures;
- the actions required by staff with key roles in the implementation of the IEP;
- the training of individuals from organisations with which a mutual aid agreement exists.

- **Examples of information that could be included:**
- a brief outline of training given to contractors, visitors and employees;
- a summary of the nature of the training or exercises carried out (for example, table top exercise, scenario specific tests, fire drills, fire and rescue training, along with information on who would be expected to undergo this training);
- details on how often training is carried out;
- an explanation on how gaps in competence are identified along with details on how training is verified.

5.5 *** An IEP has been prepared for the measures to be taken inside the establishment in the event of a major accident

The safety report should have demonstrated the following:

- an IEP has been prepared in consultation with:
  - personnel working inside the establishment including long-term relevant subcontracted personnel;
  - relevant LCAs in whose functional area the establishment is situated (Health Service Executive, An Garda Síochána, Local Authority (Fire Service), Port Authority (where applicable) - this may be co-ordinated at a regional Inter-Agency Emergency Management Office level);
  - other persons as appropriate (for example, neighbouring industrial establishments; sensitive developments (hospitals, nursing homes, schools); Environmental Protection Agency);
- the means and nature of the consultation including details of any impact that this may have had on the emergency planning arrangements have been described;
- the IEP contains the information specified in Schedule 4 of the COMAH Regulations (a copy of the IEP should be included in the safety report);
- LCAs have provided information (if requested) on the EEP to enable the IEP to be prepared.

Testing and review of the IEP

The safety report should have demonstrated that:

- a suitable programme of emergency exercises has been drawn up and emergency arrangements are tested at all levels within the establishment including the local plant response, the site-wide response and the interface with the off-site response;
- lessons learned from emergency exercises are reviewed and emergency arrangements are revised where necessary.

- **Examples of information that could be included:** details on the dates of previous exercises or tests including information relating to which scenario or element of the plan was tested (including both on and off site exercises and live or table top exercises);
- information on how tests or exercises are carried out to ensure all shift patterns are included;
- details on any debrief / analysis activities relating to how testing of the plan was carried out;
- information relating to how any actions arising as a result of any analysis or debrief are actioned and incorporated into any review process.

The safety report should have demonstrated that:

- the IEP is reviewed and updated where necessary, and tested at least every 3 years;

- any review of the IEP takes account of changes in the establishment or within the emergency services, new technical knowledge and knowledge concerning the response to major accidents;

5.6 *** It has been demonstrated that the necessary information has been supplied to the LCAs for the preparation of the EEP

The safety report should have described the arrangements for:

- supplying the necessary information to the LCAs and the most recent date this was done;
- ensuring any information supplied to the LCAs is updated as necessary and in the light of any changes;
- co-operating with other establishments identified by the CCA as being part of a domino group in supplying information to the LCAs;
- ensuring any information requested by a LCA is provided no later than one month after the request or within such longer period as the LCA may specify in writing.

5.7 *** It has been demonstrated that relevant information has been communicated to all persons likely to be affected by a major accident at the establishment

The safety report should have provided evidence that the following information is communicated to all persons likely to be affected by a major accident at the establishment:

- name or trade name of the operator;
- address of the establishment;
- confirmation that the establishment is subject to the COMAH Regulations;
- confirmation that the notification (Regulation 11) or safety report has been submitted to the CCA;
- an explanation in simple terms of the activity or activities undertaken at the establishment;
- the common names or, in the case of dangerous substances covered by Part 1 of Schedule 1, the generic names or the hazard classification of the dangerous substances at the establishment which could give rise to a major accident, with an indication of their principal dangerous characteristics in simple terms;
- general information on how the public concerned will be warned in the event of a major accident (for example, siren, megaphone or other system, which must be fit-for purpose),
- adequate information on the appropriate behaviour to be taken in the event of a major accident (for example, means of sheltering in the home or workplace, use of radio / telephone / television for further instructions from the emergency services) or where this information can be accessed electronically;
- the date of the last site visit or reference to where that information can be accessed electronically (for example, the HSA website);
- details of where further relevant information can be obtained (subject to the requirements of Regulation 26);

- general information relating to the nature of the major accident hazards, including their potential effects on human health and the environment and summary details of the main types of major accident scenarios and the control measures to address them;
- confirmation that the operator is required to make adequate arrangements on site, in particular liaison with the emergency services, to deal with major accidents and to minimise their effects;
- appropriate information from the EEP, including advice to cooperate with any instructions or requests from the emergency services at the time of the accident.

The safety report should have indicated the following:

- the means by which the information is communicated to all persons likely to be affected by a major accident (for example, leaflets, videos, meetings, media, web);
- that the information is supplied at least every 5 years and periodically reviewed and where necessary updated and supplied (including in the event of modifications covered by Regulation 12);
- that the LCAs have been consulted on the content of the information.