SAFETY CASE ASSESSMENT GUIDE

Jointly developed by:

MINISTRY OF MANPOWER

National Environment Agency
Safeguard • Nurture • Cherish

SCDF
The Life Saving Force

SCIC
SINGAPORE CHEMICAL INDUSTRY COUNCIL

1 August 2017

Table of Contents

Chapter 1: Introduction to Safety Case Assessment Guide

1. Purpose of Safety Case Assessment Guide

1.1. This is an internal guide used by the Major Hazards Department (MHD) for the assessment of safety cases submitted by MHIs.

1.2. The Safety Case Assessment Guide provides guidance on principles and the approach for using the respective assessment criteria. The assessment criteria are detailed from Chapter 2 to 10 of this guide and are used by MHD to reach conclusions on the extent to which safety cases meet their purposes under the WSH (MHI) Regulations.

1.3. The assessment criteria provide a framework to achieve a consistent and proportionate consideration of matters that may be examined during the assessment. As the proportionality principle is a cornerstone of the safety case regime, MHD focuses on where it matters most in the prevention of major accidents and is not obligated to address every criterion, nor to the same depth of detail. The criteria reflect the range of hazards expected and encountered by MHIs, which come under the scope stipulated in the WSH (MHI) Regulations.

2. Definitions and Abbreviations

2.1. For the purposes of this assessment guide, the definitions and abbreviations given in Chapter 1.3 and List of Abbreviations of the Safety Case Technical Guide apply.

3. Assessment Criteria Scope

3.1. The assessment guide will focus on the following areas during the assessment of safety cases:

a)	Descriptive aspects	[Chapter 2]
b)	MAPP and SHMS	[Chapter 3]
c)	Predictive aspects	[Chapter 4]
d)	Technical aspects	
	(i) Process safety (PS)	[Chapter 5]
	(ii) Mechanical engineering (Mech)	[Chapter 6]
	(iii) Electrical, control and instrumentation (EC&I)	[Chapter 7]
	(iv) Human factors (HF)	[Chapter 8]
e)	Emergency response	[Chapter 9]
f)	Assessment of ALARP	[Chapter 10]

3.2. The criteria in the assessment guide will be marked as follows:

a) Criteria will be "**met**" when all relevant items are included in descriptions and the necessary supporting information has been provided;
b) Criteria will be "**not met**" when relevant items are not included in the descriptions or the necessary supporting information has not been provided;
c) Criteria will be "**not relevant**" when they are not relevant to the MHI;
d) Criteria will be "**previously met**" when the previous assessor recoded the criterion as "met".

4. Demonstration

4.1 The WSH (MHI) Regulations require MHIs to prepare safety cases for the purposes of making a series of demonstrations. In this context, to demonstrate means to 'show' or 'justify' by the information given which should be taken at face value unless there is clear evidence to the contrary (e.g. conflicting statements in the safety case or local knowledge of the assessment team). It does NOT mean 'pursue by extensive in-depth scrutiny' or 'exhaustive examination to prove beyond reasonable doubt' whether the relevant criteria have been met and the demonstrations achieved.

4.2 MHIs are required by the WSH (MHI) Regulations to ensure that the data and information contained within the safety case adequately reflects the conditions in the installation. Verification of this can only be achieved by conducting inspections at the installation which can then feed back into the safety case assessment.

4.3 It is often helpful for MHIs to provide a matrix which links the content of the safety case to the requirements of the Safety Case Assessment Guide.

4.4 There is no specific requirement for MHIs to include copies of operating procedures and/or associated documentation in their safety case. MHIs should determine the level of information to be provided in support of a given demonstration or requirement in the WSH (MHI) Regulations. MHIs may choose to assist their demonstrations where necessary, by summarising a given procedure and providing an example of related documentation in support of it (e.g. a summary of the key points of a permit-to-work procedure alongside a completed permit-to-work record).

4.5 Where relevant, site records shall be used as examples to validate descriptions or where demonstrations are required by the WSH (MHI) Regulations, primarily relating to design, construction, operation, maintenance and modification.

5. Proportionality of Assessment

Factors Affecting Proportionality

5.1. A key principle of the safety case assessment process is that it is proportionate to the hazards and levels of risks associated with the MHI. The proportionality of assessment of a safety case should broadly match the proportionality required of the MHI's risk assessment i.e. an MHI with higher risks of major accidents will undergo greater rigour and depth in the assessment process.

5.2. The proportionality of assessment is essentially determined by:

a) the severity of the worst possible consequences should the worst case scenario occur;
b) the levels of risk that remain after taking into account the prevention and mitigation measures that the MHI has put in place; and
c) other considering factors such as:
   (i) The scale (inventory, vessel sizes, etc.) and nature of the hazards (hazardous properties, toxicity, flammability, etc.);
   (ii) The location of the MHI in relation to external populations (e.g. population density) and sensitive receptors (e.g. hospitals, schools);
   (iii) The number of people in the MHI;
   (iv) The variation of residual individual risk with distance;
   (v) Escalation potential (e.g. domino effects in relation to neighbouring MHIs); and
   (vi) The criticality of applied measures to achieving the claimed level of residual risk.

The Decision-Making Process

5.3. The level of risk posed by the MHI should have an influence on the areas in which MHD focus their attention. Information in the safety case should enable MHD to understand site specific circumstances (on-site and off-site), so that a view on proportionality can be reached. Where an early predictive screen has been completed, this will provide information towards MHD's decision-making process until a full predictive assessment has been carried out.

5.4. In the context of the Safety Case Assessment Guide, decisions about proportionality of assessment mean considering both the **breadth** and **depth** of assessment.

Breadth of Assessment

5.5. The nature and spread of the hazards present at an MHI determines the breadth of assessment. The assessment needs to consider a representative sample of the types of hazards found. It will therefore need to have covered different facilities, units and activities sufficient to reflect the varying nature of the hazards present, and the different nature of the measures taken to control them.

Depth of Assessment

5.6. The depth of assessment depends on the risk and one approach is to use the consequence extent and severity information relating to a scenario to make judgments about the required depth of assessment.

5.7. In considering the extent of a potential major accident, MHD will be looking at the range over which the effects extend on-site and off-site to both people and the vicinity.

5.8. In considering the severity of a potential major accident, MHD will be looking at how severe the consequences of the accident might be. This might be expressed in terms of numbers of fatalities, serious injuries, or hospitalisation, etc. Such matters depend on the surrounding population and the vicinity.

It follows that the safety case for higher risk MHIs should, in principle, be assessed to a greater depth than those for MHIs presenting lower risk.

Chapter 2: Descriptive Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the descriptive aspects of the assessment.

1.2. This chapter is linked to **Chapter 2** of the Safety Case Technical Guide.

1.3. All descriptive assessment must use the criteria and guidance set out in **Appendix A – 'Descriptive Assessment Criteria and Guidance'.**

Appendix A – 'Descriptive Assessment Criteria and Guidance'

Technical Criterion	Guidance
Overview of MHI	
2.1 The safety case shall give general information to the MHD and identify the organisations involved in preparing it.	**To meet this criterion**, the safety case shall include the following information: a) name, workplace number and address of MHI; b) mailing address of MHI [if different from (a)]; c) details of whether the MHI is part of a larger group of companies, and other subsidiary office in Singapore, as well as a brief description of the activities at each location; d) name(s), designation(s), telephone and/or fax number(s), and email address(es) for contact(s) within the MHI for communication about the safety case; and e) names of the external organisation involved in preparing the safety case and their area of contribution (e.g. QRA consultant, competent person involved in implementing risk-based inspection). This is high level information, for example, "Consultant X was used for risk assessment review work". In circumstances where no other organisations have been involved, MHIs should confirm this in the safety case.
2.2 The safety case shall provide a general outline of the installation, its activities, processes and products.	**To meet this criterion**, the safety case shall provide a general outline, without extensive detail, to set the context for the reader and the outline shall include: a) purpose of the installation; b) main activities and production which include an overall process flow diagram or block flow diagram; c) general statements characterising the main hazards of the MHI with respect to its dangerous substances and processes; d) types of MASs; e) historical development of activities and production, where relevant to MAS or SCE; f) the number of persons working at the installation and their working hours (including internal and contractors' personnel); and g) name and job scope of contractor companies engaged.

Description of Installation and its Activities/Processes Relevant to Major Accidents	
2.3 The safety case shall identify units and other activities of the installation which could present a MAH on adequately scaled plan.	**To meet this criterion**, the safety case shall contain plans, maps or diagrams with descriptions which clearly set out detailed information about the installations which could present a MAH. The layout of the installation shall be clearly presented on adequately scaled plan (i.e. usually at least 1: 10 000) which includes: a) main storage facilities (e.g. tank farms, storage vessels, warehouses); b) process sections (e.g. reaction, purification, recovery); c) location of dangerous substances; d) relevant equipment linked to MASs; e) location of essential utilities, services and internal infrastructure equipment which may be relevant to the prevention or containment of a major accident (e.g. instrument air, steam, or electrical networks); f) location of key abatement system preventing or containing major accidents, such as drainage and firewater retention, gas cleaning or liquid treatment works important for the protection of people and the vicinity; and g) location of occupied building such as control rooms, offices, workshops and canteens that could be vulnerable in a major accident (with an indication of the numbers of people likely to be present during peak and non-peak hours). For (c), MHI could provide a map containing individually labelled tanks and major process vessels and then supplemented by a table in the safety case showing what substances are stored and/or processed in each tank and major process vessel, their states and their quantities.
Information on Dangerous Substances	
2.4 The safety case shall identify the maximum quantities of every dangerous substance present, or likely to be present, at the installation.	**To meet this criterion**, the safety case shall identify and tabulate a list of all dangerous substances and their respective maximum quantities present or likely to be present in the installations as per the WSH (MHI) Regulations. MHIs shall attach relevant current licences issued by NEA (hazardous substance licence) and SCDF (petroleum & flammable materials storage licence) in the safety case.

2.5 For each dangerous substance identified, the safety case shall describe its classification under GHS, its chemical name and CAS number, according to IUPAC nomenclature.	**<u>To meet this criterion</u>**, for each dangerous substance identified, the safety case shall include: a) its chemical name and where appropriate its common chemical name; b) identification of the substance or class of substance under the International Union of Pure and Applied Chemistry (IUPAC) system of nomenclature; c) the Chemical Abstract Service (CAS) number for the substance or class of substance; d) classification under the Globally Harmonised System of Classification and Labelling of Chemicals (GHS) based on its hazards (health, physical, environmental and others) and properties as per WSH (MHI) Regulations Second Schedule Part 2 (e.g. P1, P2, H2); and e) proportion of each constituent in a mixture, where applicable. MHI shall present all information which is relevant to the various demonstrations of safety contained in the safety case.
2.6 The safety case shall describe the physical, chemical and toxicological characteristics of each dangerous substance identified, relevant to normal operating conditions and foreseeable accident conditions.	**<u>To meet this criterion</u>**, the safety case would typically include: a) SDSs of respective dangerous substances identified. The SDS should, where relevant, contain the following information: (i) flash point (by an identified method); (ii) auto-ignition temperatures; (iii) flammable limits; (iv) vapour pressure; (v) density; (vi) boiling point; (vii) data on reactions; (viii) miscibility; (ix) partition coefficient; (x) rate of decomposition; (xi) data on sensitiveness of explosives and the behaviour of explosives on accidental initiation; and

	(xii) appropriate data on toxicology. b) relevant physical and chemical data shall be presented in a clear and concise form using appropriate and consistent unit of measurement, preferably following the SI system (e.g. in kilogram, metres).
2.7 The safety case shall indicate the hazards, both immediate and delayed, for human health on-site and off-site, for the dangerous substances identified.	**<u>To meet this criterion</u>**, the information presented shall relate to the physical, chemical and toxicological characteristics of the dangerous substances and should address both the short-term and long-term effects. Examples could include: a) health hazard such as irritation, asphyxiation, cancer or mutagenic damage; b) toxicity data (e.g. PEL, LC50, LD50, IDLH, AEGL-3, ERPG-2); c) potential to cause fire and/or explosion; and d) effects on the vicinities (e.g. building damages or impacts on sensitive receptors). Appropriate references shall be provided: a) for recognised acceptable limits, in terms of concentration, distance from source, exposure time and other relevant parameters; and b) for justification of the harmful effects, hazardous concentrations and acceptable limits presented in the safety case. If there is little knowledge of the effects, MHIs should outline in the safety case the approach towards evaluating the significance of that lack of knowledge and the policy for dealing with it.

Information on the Vicinity	
2.8 The safety case shall describe the vicinity of the installation in sufficient detail to allow the consequences of a major accident to be assessed.	**To meet this criterion**, the safety case shall provide information as follows: A map of a suitable resolution should be used when describing the vicinities (outside MHI boundary limit). Separate maps of different scale may be required when considering different consequence impacts (e.g. toxic effects) • On the maps, MHIs should clearly indicate, where applicable: a) sensitive receptors (e.g. schools, hospitals, residential areas or worker dormitories); and b) access routes and escape routes from the installation and other traffic routes significant for rescue or emergency operations. • Information on the installation's vicinity that may influence the impact of a major accident, such as: a) the surrounding water courses including controlled water (if any), and any catchment area in relation to the dispersion of liquid contaminants; b) sewage and rainwater systems, if they could be involved in the dispersal of liquid contaminants off-site; c) features of the vicinity that may hinder emergency response or containment measures. • Information on external factors which may lead to or exacerbate major accidents such as: a) the topography, if it could have an effect on the dispersion of toxic or flammable gases or combustion products. This should include buildings or other structures where appropriate; b) local weather records, including wind speed, wind direction and atmospheric stability and the relevance of this information to the behaviour of releases of dangerous substances; c) history of the land on which the installation is located, together with its vicinities, may be significant when considering major accident causes. For example, land subsidence could be considered in

	reclaimed industrial land like Jurong Island as this is a threat to equipment integrity (i.e. contributing to stress and strain on piping and equipment); d) historical evidence of other external events that might cause accidents such as flooding, extreme weather conditions including temperature, rain, wind and lightning; and e) transport activities that may have an impact, including shipping, major transport routes and dangerous substance movements. • Information on structure which may be impacted by the effects of an MHI's major accident, such as any section of key infrastructure, including major land, sea or air transport routes or hubs and utilities. • Description of protected parts of the vicinities such as: a) nature reserves; b) reservoirs; and c) marine reserves. • Identification of neighbouring MHIs, pipelines and piperacks in the area. **[Description of the vicinity and surrounding populations should reflect expected conditions once the MHI becomes operational. The safety case shall describe circumstances (including temporary arrangements such as use of temporary offices and buildings and inclusion of on-site populations) as they apply to each phase (e.g. various construction phases, commissioning, start-up and shutdown).]**
2.9 On the basis of available information, the safety case should identify its neighbours.	**<u>To meet this criterion</u>**, the safety case should: a) give the name, address, and type of business for the neighbouring industrial installations; and b) describe for example the nearby housing and other buildings where there might be large numbers of people, or people who might be particularly vulnerable to a major accident.

Chapter 3: Major Accident Prevention Policy (MAPP) and Safety & Health Management System (SHMS) Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the MAPP and SHMS aspects of the assessment.

1.2. This chapter is linked to **Chapter 3** of the Safety Case Technical Guide.

1.3. All MAPP and SHMS assessments shall use the criteria and guidance set out in **Appendix B – 'MAPP and SHMS Assessment Criteria and Guidance'.**

2. The General Approach to MAPP and SHMS Assessment

2.1. The assessment will focus on the individual elements contained SS506 Part 3: Requirements for the chemical industry (2013) and on the extent to which the safety case is able to show how those elements work together to create an appropriate SHMS for the MHI concerned.

2.2. The assessment criteria and guidance which follow in this chapter are set out under headings taken from the Plan, Do, Check and Act approach of SS506: Part 3.

2.3. It shall be noted that some aspects of the SHMS are subject to assessment via the Human Factors assessment criteria and guidance (e.g. resources, personal performance, internal communication, investigation and corrective action).

2.4. It shall also be noted that this assessment criteria and guidance only outlined the salient points that MHD would be looking at in greater detail. Nonetheless under the WSH (Safety and Health Management System and Auditing) Regulations, MHIs have the ultimate responsibility to ensure that all other parts that were not mentioned in this assessment criteria and guidance but mentioned in SS506: Part 3 are duly complied.

Appendix B – 'MAPP and SHMS Assessment Criteria and Guidance'

Technical Criterion	Guidance
MAPP – 'Plan'	
3.1 ***MAPP Aims and Principles*** **The MAPP shall include a commitment to achieve a high standard of protection for people and the vicinity.**	**<u>To meet this criterion, the MAPP shall:</u>** a) specifically address MAHs and the protection of people and the vicinity in relation to the installation; and b) contain a suitable statement of the MHI's aims and principles of action and its commitment towards continuous improvement in aspects relating to the control of MAHs at the installation.
3.2 ***MAPP and SHMS Objectives*** **The MAPP shall include a commitment to provide and maintain a SHMS.**	**<u>To meet this criterion</u>**, the MAPP shall: a) a recognition that the nature of the MHI's activities could give rise to MASs potentially impacting employees, contractors, visitors, members of the public, and the natural and built environment as appropriate, and therefore that the MHI has obligations to employees, neighbours and the vicinity; b) statements explaining the company's overall aims and principles of action in relation to the systematic control of major accidents; and c) a commitment to provide and maintain a management system which addresses the issues described under Section 3.3.1 of the Safety Case Technical Guide. **[Note that for this criteria, the MHD is only looking for the policy statements; subsequent criteria will look at the detail under each heading to demonstrate that there is the SHMS to implement the MAPP.]** The MAPP shall be made available to employees and others in the MHI (e.g. contractors).

3.3 ***Senior Level Endorsement*** **The MAPP shall be set at a senior level in the MHI's organisation and be established in writing.**	**<u>To meet this criterion</u>**, the copy of the MHI's MAPP included in the safety case shall be signed and dated by an appropriate director or senior executive to demonstrate that it is truly the policy of the organisation's leadership.
SHMS – 'Do'	
3.4 ***Roles and Responsibilities*** **The safety case shall show that all necessary roles and responsibilities in the management of MAHs have been clearly allocated and defined.**	**<u>To meet this criterion</u>**, within the safety case, typically an organogram, table or similar is shown, which highlights the roles, responsibilities, accountabilities and authorities across the organisation, for all staff who have duties to manage MAHs. Additional information shall support the high level view and would usually include job descriptions or details of individual responsibilities in relation to the management of MAHs.
3.5 ***Resources*** **The safety case shall show how MHI allocates resources to implement the MAPP.**	**<u>To meet this criterion</u>**, the safety case shall show: a) who has overall responsibilities for the safe operation of the MHI; b) how key roles are identified; c) details of any qualifications, skills or experience require for key roles; d) how training for those key roles are delivered, verified and assessed; e) describing the philosophy for deputising arrangements for key functions to cover absences; f) an overview of any key roles contractors may have on-site and how training is carried out and verified for those workers.
3.6 ***Personal Performance*** **The safety case shall show that the performance of people having a role to play in the management of MAHs is measured and that they are held accountable for their performance.**	This concerns the people having a role to play in the management of MAHs and **<u>to meet this criterion</u>**, the safety case shall provide a brief outline of: a) how the responsibilities for the management of MAHs are made clear to the appointment holder (e.g. job descriptions); b) how the performance review is conducted with respect to the above requirement (a);

	c) how compliance is checked (e.g. on-site compliance checks). The safety case shall also provide: a) information about the process for identifying and taking action on failures to achieve satisfactory performance; b) reference to incentive and reward schemes; c) summaries of arrangements for setting performance standards and targets for line managers.
3.7 ***Worker Participation*** **The safety case shall show that the MHI has systems for ensuring that those working in the installation are actively involved in the control of MAHs, where relevant.**	**<u>To meet this criterion</u>**, the safety case shall typically include: a) a brief summary of how consultations are carried out with the workforce (e.g. toolbox meetings); b) an outline of the arrangements for upward reporting of information relevant to the control of MAHs; and c) how employees involvement is secured in relation to: (i) hazard studies (e.g. HAZOP) and risk assessments; (ii) devising, reviewing and revising operating and emergency systems, procedures and instructions for the control of MAHs; (iii) performance measuring activities including accident, incident and near miss investigations; and (iv) audit and review activities.
3.8 ***External Organisations*** **The safety case shall show that the MHI has in place arrangements for cooperating with, communicating information to and securing the cooperation of, external organisations.**	**<u>To meet this criterion</u>**, a brief overview shall outline the MHI's arrangements for communicating and cooperating with external organisations. This includes: a) other workplaces which might be affected by the MASs; b) contractors and their employees; c) the emergency services (e.g. SCDF); d) other relevant bodies (e.g. media, clean-up contractors).

3.9 ***Information Gathering*** **The safety case shall show that the MHI has arrangements for gathering information from external sources relevant for the control of MAHs.**	A MHI's management of MASs requires them to keep up-to-date with legal and technical developments that are relevant to their installation. The WSH (MHI) Regulations requires MHIs to review the safety case when it is necessary to do so to take account of new technical knowledge and developments in knowledge concerning the assessment of MAHs. **To meet this criterion**, the safety case shall provide a description of the MHI's arrangements for ensuring they are aware of important safety information such as changes in legislation, developments in technical standards and management practices. MHIs often describe receiving information from, for example: MHD; professional bodies; industry associations; emergency services; other companies. The focus here is on the arrangements made by the MHI to obtain and review relevant information (i.e. how they approach the task; experience or competence of those involved; how the findings have been used in the installation, etc.).
3.10 ***Internal Communication*** **The safety case shall show that the MHI has arrangements for communicating information important for the control of MASs within the MHI's organisation.**	**To meet this criterion**, a brief description of how the information pertinent to the control of major accidents is disseminated throughout the organisation, this shall include: a) information relating to the aims and purpose of the MAPP; b) information relating to the relevant risk control systems in place (e.g. management of change, permit-to-work, inspection and maintenance); c) how suggestions for improvements can be made; d) the purpose of monitoring and auditing activities; e) how lessons learned are acted upon.

3.11 ***Priorities for Improvement*** **The safety case shall show that the MHI has systems for:** **a) determining priorities to achieve the objectives of the MAPP;** **b) identifying areas for necessary improvement in relation to the control of MAHs; and** **c) scheduling the identified improvement work.**	**<u>To meet this criterion</u>**, the safety case shall typically provide: a) a brief outline of the arrangements for improvement planning, in relation to the control of MAHs; b) an explanation of how work identified as part of improvement planning process is prioritised, resourced, scheduled and how timescales for completion are set; and c) information relating to current backlogs of improvement work with a brief explanation regarding how these are being progressed. MHIs shall provide a copy of their current improvement plan in the safety case to support their demonstration (e.g. referencing to current improvement plans with a suitable explanation of the basis on which priorities have been decided, referencing to current improvement plans to illustrate how work has been scheduled).
3.12 ***Procedures*** **The safety case shall show that the MHI has adopted procedures and instructions for safe operation and maintenance.**	This criterion is about describing the risk control systems which the MHI has in place for controlling the risks which arise at each stage of the life cycle of the plant, processes or storage facilities in question. **<u>To meet this criterion</u>**, the safety case shall describe the systems for controlling risks at each of the following stages as appropriate: a) **Construction and commissioning** of plant, processes, equipment and facilities; • Including details of how the organisational readiness of the operating functions and/or the technical safety and integrity of the new facility under construction are ascertained prior to the introduction of dangerous substances. b) **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; c) **Safe operation under maintenance conditions** • Including carrying out risk assessment for decontamination and maintenance work, generating safe methods of working for maintenance (e.g. hot tap, isolation, depressurising, deenergising) and using permit-to-work systems to control it;

	d) **Selection and management of contractors** • How contractors are selected, managed, inducted and trained; e) **Decommissioning** of plant, processes, equipment and installation. MHIs may support their demonstration by providing copies of, for example, their contractor management procedure, operating procedure and permit to work procedure (or summarised versions) in the safety case.
3.13 ***Management of Change*** **The safety case shall show that the MHI has adopted procedures for addressing possible hazards and associated risk that may be introduced as a result of new dangerous substances, change in dangerous substances inventories, change in process technology, in facilities or in organisation.**	**To meet this criterion**, the safety case shall describe the 'management of change' processes used. The procedure shall follow the requirement as stipulated in SS506: Part 3. MHIs may provide a copy of their management of change procedure (or a summarised version) to support the demonstration along with a completed example of a recent change in the safety case.
SHMS – 'Check'	
3.14 ***Active Monitoring*** **The safety case shall show that the MHI has devised proactive means of performance measurement, which provide information on whether the control measures taken to guard against MASs are operating as intended.**	This criterion recognises that in the case of MASs, a low incident rate is no guarantee that risks are being effectively controlled. **To meet this criterion**, the safety case shall: a) provide information relating to a set of leading Process Safety Performance Indicators (PSPIs) which follow suitable standards such as API 754, HSG 254 or similar; b) key risk control systems, necessary for the control of major accidents have been identified and that there is a process for gathering data on the performance of the risk control systems; c) performance standards have been set for each performance indicators; d) senior management are actively involved in setting performance indicators and standards.

3.15 ***Reactive Monitoring*** **The safety case shall show that the MHI has adopted a system for reporting incidents and near misses, relating to failure of the protective measures for control of MASs.**	Following on from criterion 3.14, the safety case shall show that there is an established set of lagging PSPIs which follow suitable standards such as API 754 or HSG 254 or similar. **<u>To meet this criterion</u>**, it shall be shown that senior management receive relevant information on: a) dangerous occurrences as defined in the Workplace Safety and Health Act relevant to major accidents; b) major accidents as defined in the WSH (MHI) Regulations; c) injuries and cases of ill-health related to major accidents; d) incidents with the potential to escalate into major accidents (i.e. near misses); and e) hazardous conditions, including losses of containment or process deviations exceeding safe or design limits.
3.16 ***Investigation and Corrective Action*** **The safety case shall show that the MHI has adopted mechanisms for investigating and taking corrective action:** **a) in cases of the proactive performance standards showing a deterioration in risk control measures; and** **b) in relation to any incident or event with potential to cause a MAS.**	Within the safety case, information shall be provided on the actions taken by the MHI in response to data received through monitoring arrangements. That would typically be: a) a description of the arrangements in place for carrying out investigations, including how the type and level of investigation is determined and what outputs are expected (e.g. underlying and immediate causes); b) a clear link between the MHI's monitoring arrangements (both active and reactive) and any initiation of corrective action taken by the company to remedy any lapses found; c) how the MHI respond to necessary corrective action work identified by investigation reports or similar, and how these are prioritised.

3.17 ***Audit*** **The safety case shall show that the MHI has adopted a procedure for systematic assessment of the MAPP and the effectiveness and suitability of the SHMS.**	**To meet this criterion**, the safety case shall provide a description of auditing activities carried out on-site, which is expected to contain the following: a) the resources and personnel required for each audit, bearing in mind the need for expertise, operational independence and technical support; b) the audit plan indicating how it has been prioritised; c) the audit protocols to be adopted (which might include use of questionnaires, checklists, open and structured interviews as well as checking documents and measurements and observations); d) the procedures for reporting the audit findings; and e) the procedures for following up the recommendations shown to be necessary by audits. Typically the safety case may include a copy of an audit plan and an example of a completed audit.
SHMS – 'Act'	
3.18 ***Review*** **The safety case shall show that the MHI has adopted a review process which uses information from performance measurement and audit to facilitate the update of the MAPP and SHMS.**	**To meet this criterion**, the safety case shall describe how information collected from performance measurements and audits are reviewed (e.g. management review), and as a minimum, show: a) how the results are considered and by whom; b) how they are used by senior management to carry out necessary updates of the MAPP and SHMS; and c) how the suitability and adequacy of the current arrangements for performance standards and audits are assessed.
3.19 ***Documenting the Review*** **The safety case shall show that results of review are documented and communicated within the organisation.**	**To meet this criterion**, the safety case shall include a description of the MHI's arrangements for documenting and publishing the results of the review within the organisation.

Chapter 4: Predictive Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the predictive aspects of the assessment.

1.2. This chapter is linked to **Chapter 4** of the Safety Case Technical Guide.

1.3. All predictive assessment must use the criteria and guidance set out in **Appendix C – 'Predictive Assessment Criteria and Guidance'.**

1.4. Experience has shown that it is essential for MHIs to identify all MAHs, their likelihood, and consequences before going on to perform a sufficient and suitable risk assessment and identify risk reduction measures.

1.5. Any subsequent risk assessment may be qualitative, semi-quantitative, quantitative, or a combination of these. MHIs will need to decide the scope and nature of their risk assessment based on proportionality in relation to their site-specific circumstances and the demonstration required.

2. Risk Assessment

2.1. Risk assessment steps that shall be demonstrated in the safety case are:

a) understand the site operations, the materials involved and the process conditions;
b) identify the hazards with potential effect on people on-site and off-site;
c) analyse the different ways the hazards can be eliminated or reduced in scale.
d) analyse the risks associated with the remaining hazards and the options for reducing them. Risk reduction cannot be looked at without first doing a risk analysis;
e) for these hazards, predict the likelihood of the hazards being realised taking into account of the chance of success and failure of possible preventive measures;
f) predict the corresponding consequences considering failure of measures;
g) decide which measures need to be implemented to make the risks to people ALARP; and
h) present the results of the risk assessment in sufficient detail to demonstrate that the necessary measures have been taken to prevent and mitigate major accidents.

2.2. The risk assessment needs to address:

a) risks to people on-site; and
b) risks to people off-site.

2.3. For new MHIs and modifications to existing MHIs, the risk assessment needs to include:

a) consideration of the elimination of hazards;
b) inherently safe approaches to reduce the scale of hazards; and
c) prevention and mitigation measures to prevent and limit risk.

Appendix C – 'Predictive Assessment Criteria and Guidance'

Technical Criterion	Guidance
Overview of MHI Installations and Activities and/or Processes Relevant to Major Accidents	
4.1 The safety case shall describe the sections of the installation that could give rise to major accidents.	**To meet this criterion**, the safety case shall contain plans, maps or diagrams with descriptions which clearly set out detailed information about the installations with potential for major accidents. The safety case should contain detailed process descriptions of the relevant sections by providing information such as: a) block flow diagram or process flow diagram; b) the operating parameters and envelopes of the plant during: (i) normal operations; (ii) normal non-routine operations (e.g. regeneration); (iii) commissioning and start-up; (iv) shutdown; and (v) decommissioning. c) the designed minimum and maximum parameters, such as capacities, temperatures, pressures and inventories; d) relevant qualitative and quantitative information on mass and energy transport in the process (e.g. material and energy balance) during: (i) normal operation; and (ii) non-routine operations (e.g. regenerations), if available; e) information on what happens to the dangerous substances (physical and chemical changes) at designed operating conditions or foreseeable deviations from design operating conditions. The range of conditions considered could include: (i) operating pressures and temperatures during start-up, regeneration, normal operation, turndown or other designed mode; (ii) production of products, by-products, residues or intermediates as a result of normal operations or through foreseeable accidental conditions;

	(iii) process upset conditions; (iv) storage of materials under normal operation and following loss of utility, for example, refrigerated storage or heated storage; (v) contamination of products; and (vi) loss of containment. f) the discharge, retention, reuse, recycling or disposal of residues, waste liquids and solids, and the discharge and treatment of waste gases; g) sufficiently scaled plot plan which clearly identifies the location of processes and/or activities where a major accident could happen; h) dangerous substance locations and at each location, an indication of the chemical and physical state and quantity of the dangerous substance in major process vessels or storage tanks; and i) plant diagram which clearly identifies key control and safety systems, reaction vessels, storage vessels, piping systems, valves and significant connections (e.g. process flow diagrams and/or piping & instrumentation diagrams).
Identification of Representative Set of MASs	
4.2 The safety case shall identify and describe in detail all potential MASs.	The safety case's description of the MAS identification exercise needs to demonstrate to the MHD that all MAHs are taken into account. As such it shall be extensive, inclusive, and transparent, and **to meet this criterion**, the safety case shall: a) demonstrate that a systematic process has been used to first identify all possible MAHs and then its associated potential MASs; b) describe the relevant expertise of the hazard identification team involved. The safety case shall also show that multi-disciplinary team composed of persons with appropriate competency (e.g. personnel trained in specific hazard identification methodologies, personnel with relevant experience in design, operation, maintenance, process safety, or human factors) were used to conduct or inform the analysis. c) identify and describe the range of hazard identification methods used in the safety case. All hazards identified shall initially be considered as if no measures were in place.

	Examples of risk studies that MHIs may use (but not limited to) to identify all possible MAHs and potential MASs include: (i) QRA studies; (ii) PHA studies such as HAZOP, failure mode and effects analysis (FMEA), process hazards review (PHR); (iii) safety reviews and studies of the causes of past major accidents and incidents; (iv) industry standards or checklists; (v) job safety analysis (e.g. task analysis); (vi) human error identification method.
4.2.1 The safety case shall demonstrate that a systematic process has been used to identify events and events combinations which could cause MAHs to be realised.	**<u>To meet this criterion</u>**, the following should be considered when determining the causes or initiators of potential major accident during the identification process: a) **operational causes** are determined according to the methodology chosen; where relevant, the following should be considered: (i) physical and chemical process parameters limits; (ii) hazards during specific operation modes (e.g. start-up and shut down); (iii) malfunctions and technical failures of equipment and systems; (iv) utilities supply failures; (v) human factors involving operation, testing and maintenance (e.g. loading wrong reactants into a batch reactor); (vi) chemical incompatibility and contamination; and (vii) ignition sources (e.g. electrostatic charge); b) **internal causes**, where relevant**,** may be related to fires, explosions or releases of dangerous substances at a certain section within the installation which the safety case covers and affecting other section leading to a disruption of normal operations (e.g. the failure of a water pipe in a cooling tower, thus leading to a disruption in the cooling capacity on-site); and c) **external causes**, where relevant, may include: (i) impacts of accidents (e.g. fires, explosions, toxic releases) from neighbouring installations (domino effects);

	(ii) impact of accidents arising from transportation of dangerous substances off-site (e.g. roads, pipelines); (iii) functional interdependence with other installations; (iv) land slips, subsidence; (v) aircraft impact (for installations near airports); (vi) extreme environmental conditions (e.g. abnormal rain, temperature, wind, floods, lightning); and (vii) pipelines or other common utilities (e.g. disruptions of steam, power or cooling water from external providers). Scenarios influenced by emergency action or adverse operating conditions should also be taken into consideration during the hazard identification process.
4.2.2 There shall be a suitable review of past accidents and incidents relevant to the site.	A review of past accidents and incidents with the same substances and processes used, consideration of lessons learned from these and explicit reference to specific measures taken to prevent such accidents is required by the WSH (MHI) Regulations and **is a minimum requirement**. This should also look beyond the MHI to the wider industry relevant to the site. Insights gained from the review of past accidents and incidents relevant to the site shall form part of the input used by MHIs when generating MAS.
4.3 The safety case shall describe a representative and sufficient set of MASs for the purpose of detailed assessment.	**To meet this criterion**, the safety case shall consider in detail the risks associated with a subset of all MASs considered for the site, which is known as the representative set of MASs. This makes the subsequent risk assessment more manageable. The representative set of MASs must be sufficient and should include: a) range of accidents for the site, taking account of different hazards, substances, processes, geographical spread, etc. leading to fatalities or serious harm injuries on-site and/or off-site; b) worst case scenarios (consideration of worst case scenarios is particularly important when assessing the adequacy of the emergency response arrangements);

	c) events which in themselves might be low severity or risk, but which could escalate to give a more serious event; and d) MASs with lesser consequences at higher frequency.
4.3.1 Any criteria for eliminating possible MASs from further consideration shall be clearly presented and well argued in the safety case.	The intent of this criterion is to ensure that no important MASs go unconsidered. **To meet this criterion**, any key assumptions made during the hazard identification stage shall be described in the safety case, especially if such assumptions lead to the elimination of significant scenarios from the eventual representative list of MASs.
4.4 The safety case shall justify on the risk assessment methodologies used when conducting detailed assessment on the representative set of MASs.	MHIs shall justify their risk assessment methodology based on: a) expertise and competence of those identifying and analysing hazards; b) methods used in the risk analysis; c) data and assumptions; and d) how the significance of the risk was assessed. In general, MASs deemed to have a higher level of risk, consequences impact or potential for escalation to a more serious event shall be conferred with a greater degree of rigour during the assessment process. **To meet this criterion**, MHIs shall justify in the safety case on the depth of analysis and degree of rigour required for each representative set of MASs prior to the detailed assessment. It should be noted that subsequently on detailed assessment, the actual risks might be shown to be significantly reduced either by revised frequencies, which are demonstrated to be lower than was initially judged, or by accounting for systems which reduce the consequence.

4.5 It should be clear that human factors have been taken into account in the risk assessment.	**<u>To meet this criterion</u>**, the safety case should: a) describe a process for identification of human failures, actions or other involvement as contributor to major accident which is systematic and integrated with the overall risk assessment; b) show how human failure contributes to major accident initiation or escalation; c) where quantitative assessments are used: (i) address the probabilities of human actions and omissions contributing to major accidents; (ii) address the reliability of measures which is dependent upon human action; and (iii) show that all assumptions made in the determination of human failure probabilities are appropriate or based on a thorough and systematic assessment.
Detailed Assessment – Consequences Assessment and Likelihood Estimation of Representative Set of MAS	
4.6 The safety case shall produce an adequate assessment of the extent and severity of the consequences for representative set of identified MASs.	**This is the most important predictive part of the safety case and must be included. Without it, it is impossible to come to an appropriate view on proportionality and where a company should put effort into risk reduction measures.** The safety case shall contain the results of calculations showing suitable estimates of the extent and severity of the consequences for each representative set of MAS. Extent and severity is concerned with who (people) might be harmed, how badly, and how many people are affected by major accidents. The safety case shall provide details to demonstrate that suitable and sufficient consequence assessment for each representative set of MAS has been carried out with respect to people. The safety case shall: a) Present **extent** information: • Effects distances on maps and/or images of the site and the vicinity showing areas likely to be affected by representative set of major accidents (with identified estimations of numbers, centres and types of populations both on-site and estimated off-site).

	b) Presents **severity** information in a suitable form, e.g.: • Numbers of fatalities, serious injuries, hospitalisations, • Banding in terms of consequences to people (e.g. 1-5, 5-20, 20-100). • Where major accidents have been put into example groups, then it is acceptable to present extent and severity for each group. • Occupancy based population data MHIs shall either describe or reference any consequence assessment model used in the safety case. MHIs shall also take into account the limits of applicability of the model used and justify all assumptions made and the values used in the key variables of the method or model (e.g. wind speed, atmospheric conditions and ground roughness in gas dispersion models). Different levels of harm need to be considered. Any harm footprints, levels or vulnerability models used, in predicting the extent of areas where people or the vicinities may be affected shall be aligned to the Revised QRA Guidelines.
4.7 The safety case shall contain estimates of the probability, in qualitative or quantitative terms, of each MAS analysed. **This shall include a summary of the initiating events and event sequences (operational, internal or external) which may play a role in triggering each MAS.**	**To meet this criterion**, the likely frequency or probability of MASs shall be considered. The depth of the analysis of scenario likelihood shall be proportionate to the scale and nature of the hazard. If judgmental words such as 'likely' or 'non-credible' are used in qualitative estimation of likelihood, then the significance of these words shall be clearly explained. For failure rates, the safety case should: a) ensure that failure rate data used are aligned to the Revised QRA Guidelines; or b) include the references and methods of derivation (where appropriate) for using failure rate data not in accordance with the Revised QRA Guidelines.

	It is not sufficient to adopt data from published sources without justifying its suitability to the installation, unless the MHI shows that the conclusions of the risk assessment are not affected by such data (e.g. through a sensitivity analysis). If the estimations of the likelihoods of the representative MASs are sensitive to the data and assumptions used, suitable and sufficient justification is needed. MHIs should assess the sensitivity of the conclusions to the assumptions and other uncertainties. For example, in situations where there are not much data on event probabilities for certain processes, which causes uncertainty in the estimation process. The significance of this uncertainty should be discussed in the safety case and sufficient detail will have to be provided to allow the MHD to make a judgement on the quality of the risk assessment. Where uncertainties exist, **a conservative approach should be evident for arguments used.**
4.7.1 Methods used to generate event sequences, and to estimate the probabilities of potential major accidents, shall be appropriate and used correctly.	Appropriate methods to generate event sequences and estimates of major accidents probabilities include: a) relevant operational and historical failure data; b) fault tree analysis (FTA); c) event tree analysis (ETA); or d) other relevant methodologies. The methods employed shall be fit for purpose and used correctly. The process and methods adopted to generate any probabilities or event sequences, together with assumptions and data sources used, shall be described clearly. Checks against company benchmarks must be included if MHIs used them.

4.7.2 Estimates of, or assumptions made about, the reliability of protective systems and the times for operators to respond and isolate LOC accidents or others need to be realistic and adequately justified.	The qualitative or quantitative arguments presented in the safety case shall be realistic, well-reasoned and plausible. Where possible, arguments shall be backed-up by credible performance data. Any qualitative arguments made shall be: a) based on accepted good standards for engineering and safe systems of work; and/or b) supported by evidence on the likely demand on the various control measures and systems, and what the consequences might be if these fail. For example, if an operator has to intervene to close an isolation valve manually when automatic isolation fails, then the release duration will be determined by the time taken to intervene successfully. **In such cases, release durations of less than 20 minutes will require justification.**
Selection of SCEs for ALARP Demonstration	
4.8 The safety case shall describe how MHIs uses risk assessment to identify the SCEs from the representative set of MASs for the purpose of ALARP demonstration.	**The risk assessment shall show which events are critical from a safety point of view and this requires consideration of the likelihood and consequences of the various MASs.** The safety case shall identify SCE and the basis for the choice of the identification. The following should be considered when identifying SCEs: a) worst case scenarios in each frequency band; and b) the most likely scenarios in each consequence band. SCEs are those that dominate the contribution to risk *at different distances* and thus are key to identifying suitable control and protection measures for preventing MASs or limiting their consequences. However, the failure of these protection measures must also be considered in assessing whether the residual risks are ALARP or whether more needs to be done.

	One way that MHIs could demonstrate how SCEs are selected from a representative set of MASs is to plot the scenarios onto a risk matrix. From the risk matrix, it is then straightforward to identify the SCEs such as worst-case scenarios, high risk scenarios and other MASs of interest. • The risk matrix could also be used to inform of the proportionality of the installation as a whole. MASs approaching or in the red or uncomfortably high zone are considered to be of higher proportionality and therefore the level of ALARP demonstration would be greater.

Chapter 5: Process Safety Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the process safety assessment.

1.2. This chapter is linked to **Chapter 5** of the Safety Case Technical Guide.

1.3. All process safety assessment must use the criteria and guidance set out in **Appendix D – 'Process Safety Assessment Criteria and Guidance'.**

2. The General Approach to Process Safety Assessment

2.1. MHD is looking for a demonstration that adequate safety have been taken into consideration in the design, construction, operation, maintenance and modification of any plant, storage facility, equipment and infrastructure connected with the installation's operation, which are linked to MAHs inside the installation.

2.2. For new projects, design standard shall address ten design key issues in the safety cases. For existing facilities, the key issues in design shall be considered for control measures implemented for SCEs.

Appendix D – 'Process Safety Assessment Criteria and Guidance'

Technical Criterion	Guidance
Link with Predictive Criteria	
5.1 The safety case shall show a clear link between the measures taken and the SCEs described.	This is the core of the safety case from the technical point of view and provides the link between identification and analysis of hazards and the selection of measures. **This criterion can be regarded as a conclusion and the MHD would first consider criteria in Chapter 10 of the assessment guide.** **<u>To meet this criterion, the safety case shall:</u>** a) identify the hazards and the SCEs (covered under Chapter 4 of the assessment guide); b) describe the control measures and demonstrate clear links to the SCEs; c) explain the decision criteria for selecting the necessary measures to ensure risks are ALARP for SCEs i.e. the safety case demonstrates there are no further reasonably practicable measures the MHI could take; **[MHD would assess this particular criterion in tandem with Chapter 10 of the assessment guide.]** d) demonstrate adequate diversity and redundancy in the control measures (appropriate to the risk). The findings of the hazard identification process shall be presented to demonstrate that mechanical equipment has been considered. <u>There are two main functional categories:</u> a) Equipment containing dangerous substances which, on failure, have the potential to lead to a LOC. This could include but not limited to: • Pipework • Storage tanks • Pressure vessels • Rotating equipment

	b) Items which play a role in the prevention or mitigation of MAHs. This could include but not limited to: • Relief valves • Cooling pumps • Emergency isolation valves • Non-return and check valves • Excess flow valves • Support structures (including jibs and cranes) • Secondary containment • Tertiary containment • Fire suppression system **<u>In addition, the safety case shall describe:</u>** a) the link between the design stages and the associated hazard studies; b) how a suitable hierarchical approach (i.e. eliminate, prevent, mitigate) has been used and inherent safety designs have been introduced where reasonably practicable. **[Applying inherent safety designs may be difficult for existing MHIs but is relevant to the design of new plants and major modifications. It is specifically addressed in 5.2.1.2 below]** The Hazard Studies shall be: a) sufficient to identify the hazards arising from the processes and the dangerous substances involved; b) appropriate for the scale and nature of the hazards presented. Such studies could include HAZID, HAZOP, Fault Trees, FMEA, hazardous area classification, chemical reaction hazards assessment, SIL and LOPA assessments and where appropriate comparison with published standards; c) carried out by competent personnel with relevant discipline representation; d) used correctly to inform decision making.

General Principles	
5.2 The safety case shall demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents and limit their consequences.	**<u>The safety case shall describe:</u>** This is effectively a summary of criteria 5.2.1.1 to 5.2.3, the MHD would come back to this when criteria 5.2.1.1 to 5.2.3 have been assessed, and then conclude: a) whether all the assessed criteria have been met; b) how significant the failure to meet one or more criteria is to the overall safety demonstration; in particular: • identifying any failure to follow appropriate standards, codes of practices and guidance; and • any deviations shall be fully justified by the MHI and the risks shall be ALARP. c) the recommended actions for improving the safety case and suggested timescales; and d) the recommendations for follow-up inspection and verification, their priority and timescale.
Use of Industry Codes and Standards	
5.2.1.1 The safety case shall show that the installations have been designed to an appropriate standard.	The MHD will be looking at the overall design strategy and the justification for the design selected including the associated control measures. **<u>To meet this criterion, the safety case shall:</u>** a) give references to standards and codes of practice used as the basis for the design of the process and its application. These may be incorporated in the text or as a list; b) show that where such standards and codes of practice have been revised or new standards created, these have been considered (e.g. by gap analysis) and incorporated into installations, <u>where reasonably practicable,</u> for barriers identified for SCEs; c) show that global or company standards (where they are used) align with appropriate published standards and guidance. Where global or company standards are not aligned with published standards and guidance, MHIs shall justify how their own standards are appropriate and fit for purpose;

	d) identify where the design of equipment is not covered by published standards and codes and demonstrate that safety is not compromised. **[For common types of installation, reference to published standards or guidance within the safety case can be an effective way of showing that adequate measures have been taken.]** **[For older plants in particular, the safety case shall describe additional (if any) systems or control measures are in place to prevent an SCE or limit its consequence, to take account of plant built to standards that have since been superseded. The safety case shall also describe any additional systems or control measures that have been introduced as a result of long operational experience on-site.]**
Design Considerations	
5.2.1.2 The safety case shall show that a hierarchical approach to the selection of measures has been used.	The use of a hierarchical approach is mentioned in 5.1 and 5.2.1.5. The three stage hierarchy, in order of priority, is: a) Eliminate (inherent safety) b) Prevent c) Mitigate **For new and modified facilities, the safety case shall justify** the quantity and type of dangerous substance on-site by, for example, showing that appropriate consideration has been given to: a) reducing inventories of dangerous substances on-site; b) use of alternative less hazardous substances; c) use of inherently safer processes; d) use of intensified processes (e.g. use of smaller volume continuous processes rather than large batch processes); and e) other examples as provided in Chapter 5 Paragraph 148 of the Safety Case Technical Guide.

	<u>For existing MHIs</u>, they shall be alert to the possibility of taking advantage of technical advances in their industry to improve safety. **<u>The safety case shall also show that:</u>** a) processes are designed to eliminate or prevent unsafe conditions occurring and that the principles of redundancy, diversity, separation and segregation have been applied; b) priority is given to passive rather than active measures; c) safety critical control measures have been identified and alternatives considered. d) identify how the behaviour of equipment on failure has been addressed, including events which may cause a fault and disable protective systems; e) show that performance standards (reliability, availability, accuracy, etc.) are adequate (linked to Criterion 5.3 below).
5.2.1.3 The safety case shall show that the layout of the plant limits the risk during operations, inspection, testing, maintenance, modification, repair and replacement.	**This criterion is particularly relevant during the QRA approval stage where design of the layout of a plant can make a big contribution to reducing the likelihood and consequences of a major accident.** **<u>To meet this criterion, the safety case shall show that:</u>** Due attention has been given to ensuring safety in the design of the layout of the installation. In particular, it shall show how the layout prevents or reduces the development of MASs. Examples of how this might be achieved include the following: a) Separation of facilities with MAHs or dangerous substances from the site boundary to reduce off-site risk, and to reduce risk to the plant from off-site causes such as fires; b) Safe positioning of occupied buildings; c) Separation between facilities with MAHs or dangerous substances and storage areas to limit the spread of fire and other domino effects;

	d) Separation of facilities with MAHs or dangerous substances and processes from ignition sources, roadways or other activities which may impact on safety; e) Low congestion of structures, equipment, plant or any other obstacle to gas flow that could aggravate the pressure effects resulting from the ignition of a release of a flammable substance; f) Access for emergency services; g) Adequate safety refuge or in-place protection (IPP) facilities during any toxic release, and adequate means of escape during other emergencies; h) Access for inspection, testing, maintenance and repair, at all times throughout the life of the plant. **<u>The safety case shall contain the following relevant records, or equivalent such as:</u>** a) Maps of the site layout, identifying process and storage areas, occupied buildings, roadways, locations of dangerous substances; b) Hazardous Area Classification (HAC) drawings showing the locations of flammable substances and the associated hazardous areas (see also 5.2.1.8); c) Drainage diagrams, as appropriate to demonstrate routes to separators, etc.; d) Location of gas detectors, fire and smoke detectors; e) Loading and off-loading facilities, delivery arrangements particularly tanker movement; f) Vapour recycle and venting systems and emergency venting arrangements. (see also 5.2.1.5)

5.2.1.4 The safety case shall show that utilities that are needed to implement any measure defined in the safety case shall have suitable reliability, availability and survivability.	**<u>To meet this criterion, the safety case shall show:</u>** a) that 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; b) the effect of the loss of key utilities has been considered as part of a structured hazard identification and analysis process. This shall ensure that control systems and safety systems fail to a safe state and that the consequence of utilities failure does not act as a major accident initiator; c) the reliability of utilities for safe shutdown and emergency response have been determined and independent back-up supplies provided where necessary; and d) those utilities that are essential for operation of key safety systems and its back-up system. Further justification that the utilities are suitable may include reference to: a) the routing of services; b) physical protection (e.g. barriers and fireproofing); c) the segregation of duplicated supplies; d) the means of managing changed demands (e.g. during start-up and shutdown) and abnormal operation; and e) the methodology adopted to allow continued availability of essential services while allowing maintenance activities or modifications to be carried out safely. Utilities to be considered, as appropriate, include: a) electrical power; b) steam and condensate; c) inerting gases (e.g. nitrogen); d) compressed air; e) vacuum systems; f) cooling water;

	g) process and service water; h) fuel (e.g. oil, gas); i) refrigeration; j) any other safety critical utility. **[Chapter 7 of the assessment guide will further assess the effect of loss of utilities on control systems.]**
5.2.1.5 The safety case shall show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances.	**<u>To meet this criterion, the safety case shall show:</u>** **<u>The process</u>** by which dangerous substances could be accidentally released from containment and **<u>the measures</u>** which have been provided to prevent or minimise releases. The safety case shall demonstrate the suitability of measures to prevent or minimise releases. Such measures may include: a) control measures used in the design to reduce potential sources of release which include, for example, the location, number and type of joints (e.g. threaded and screwed joints, flanged joints, socket-welded joints). Any joints used shall be suitable for the intended purpose considering the nature of the contained material, operating conditions and the degree of danger this represents; b) design requirements for temporary arrangements, taking into account possible movement (e.g. flexible connections between fixed storage or piping systems and isotankers or vessels); c) maintenance and inspection requirements addressed at the design stage; and d) process design and control for exothermic reactions. Details of system designed to control LOC and to manage unplanned releases shall be demonstrated and these could include: **i. Primary Containment** All process, storage and any other equipment containing dangerous substances shall be designed to appropriate standards. Where there are deviations from standards, these shall be documented and justified to demonstrate an equal level of safety.

	ii. Secondary and Tertiary Containment Measures Where LOCs of a significant quantity of dangerous substances is foreseeable, the safety case shall describe the measures to limit the consequences. These measures include secondary and tertiary containment (e.g. bunding, interceptors, catchment pits, dump tanks, diversion walls or grading of the ground). The safety case shall also identify such measures and demonstrate the adequacy of the design and the capacity in relation to the maximum expected spill. The possibility of bund overtopping shall be taken in account. **iii. Venting Systems** The safety case shall describe and justify the design basis for any venting system taking into account foreseeable hazards (including loss of utilities or the effects of fire) and the consequences of venting to the vicinity. **iv. Isolation Arrangements** The safety case shall describe and justify the emergency automatic and manual isolation arrangement to manage a release including consideration of the time required to isolate. Appropriate performance standards for emergency isolation shall be stated and justified in the safety case. **[Isolation may also be necessary for maintenance but the arrangements for this will be different from those required for emergency isolation where speed of response and accessibility may be important.]** **v. Other Prevention and Containment Measures** The safety case shall describe and justify the design basis for each of these measures taking into account the foreseeable hazards. **[In the case of some situations involving explosives, it may be more appropriate to limit the effects of an explosion through reducing the containment or confinement of the explosive.]**

	vi. Detection of Releases The safety case shall describe the measures to detect a LOC or other incident at an early stage. These measures include gas detection, level monitoring, loss of pressure, visual methods (e.g. operator rounds, cameras), etc.
5.2.1.6 The safety case shall show how the containment systems have been designed to withstand the loads experienced during normal operation of plant and all foreseeable operational extremes during its expected life.	**<u>To meet this criterion, the safety case shall describe:</u>** a) 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 (e.g. normal operation, start-up and shutdown, turnaround, regeneration, process upset and emergencies); b) how suitable safety margins are determined such that the safe working limits of the plant (pressures, temperatures, flow rates, liquid levels, etc.) are compatible with all expected operating extremes; • Specific details shall be given where actual margins differ significantly from industry practice and the safety implications arising from the variation shall be described and justified. c) the provision of excursion relief (e.g. pressure and/or vacuum relief devices), where appropriate. **<u>The safety case shall also demonstrate</u>** how foreseeable extreme conditions (e.g. during start-up, shutdown, process upsets) have been taken into consideration in the design of plant and equipment. To assist in the demonstration of this criterion, a table or list detailing the following information for the major equipment items featuring in SCEs selected could include: a) Expected minimum and maximum operating conditions (e.g. pressure and temperature) and design limits. b) Set pressures for associated relief devices (PRVs, rupture discs, etc.) where appropriate.

5.2.1.7 The safety case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions.	**<u>To meet this criterion, the safety case shall describe:</u>** a) how margin shall be set so that for foreseeable failures (e.g. equipment failure), appropriate corrective action can be taken before the safe operating limits are exceeded. The corrective action can be either automatic, manual, or a combination of both. b) how MHIs monitor and ensure that plant and equipment continues to operate within the design envelope and defined safe operating limits (e.g. process control systems, alarms, trips); c) how chemical reaction hazards are evaluated and justify the sufficiency of the control measures to prevent runaway reactions, overpressure and LOC. This description shall include chemical manufacturing processes as designed, and also accidental mixing of incompatible chemicals on-site and treatment of waste streams; <u>The safety case shall:</u> • give details of the physical parameters of possible conditions (i.e. flows, temperatures and pressures) with respect to excursions, runaway, worst case scenarios, etc.; • show that the design standards and other applied codes of practice are appropriate to the conditions under which the design must work; • show that hazard identification has covered the possibility of beyond design conditions; and • show that accident history for a type of plant has been considered where relevant. d) the emergency prevention and protection measures and show that these are fit for purpose. These measures include: • the safety-related controls and alarms designed to prevent or warn of excursion beyond safe operating limit 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 shall be specified; • explosion relief; • occupied building risk assessment (OBRA);

	• interfaces with other measure designed to limit excursions beyond safe operating limits such as: o shutting off feed streams; o shutting down of heat sources; o adding inhibitors to the reagent; o dump systems; o inerting; o flushing through of continuous processes; o application of process cooling; o operating vents; o shutdown of equipment; and o sprinklers or water deluge. e) whether interventions are automatic or manual. The safety case shall show that the MHIs have examined the costs and benefits of automating the system and justified the suitability of the adopted approach. **[Where examples of procedures or operating instructions have been included in the safety case, the MHD will examine them to see if these procedures and instructions could be helpful in clarifying on the process and the associated control measures.]**
5.2.1.8 The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk.	**<u>To meet this criterion, the safety case shall show:</u>** a) that, as part of the risk assessment, MHIs must assess whether potentially hazardous areas (flammable and explosive atmosphere) is likely to form; b) that all possible ignition sources (including electrostatic discharges) in areas where dangerous substances are present have been considered. <u>As a minimum</u>, the following form of energy shall be included when considering potential ignition sources: • heat (including possibility of radiofrequency energy leakage from semiconductor equipment); • electrical; • mechanical; and

	• chemical. c) that a hazardous area classification (HAC) study has been carried out and this shall be recorded in the form of drawing which: • identifies the hazardous areas and types (e.g. zone 0, 1, 2 or division 1, 2); • shows the extent of the zones in both plan and elevation (i.e. illustrates the 3D nature of the hazardous zone); • is supplemented by text, where applicable, giving information about: (i) the dangerous substances that will be present; (ii) the work activities that have been considered; (iii) other assumptions made by the study. • is considered whenever new equipment is to be introduced into a zoned area. d) the procedures and policies for identifying hazardous areas are based on established codes and standards; e) the procedures and policies for identifying hazardous areas are consistently applied; f) the HAC data is used in the selection and location of equipment and its maintenance and in considering plant and process changes; g) the location and likelihood of potential sources of ignition in relation to LOC events and MASs shall be considered. The MAH 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 (e.g. closure of adjacent roadways during tanker loading and offloading, provision of protected lighting).

Operation		
5.2.2	**The safety case shall show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions.**	**<u>The safety case shall describe</u>** how documented operating procedures assure that mechanical plant and equipment are always operated within safe limits (e.g. procedures shall prevent damage to plant or components from occurring during operational extremes such as start-up and shutdown). **[Process control systems (where installed) are covered under criterion 5.2.1.6 above.]**
Modification and Decommissioning		
5.2.3	**The safety case shall describe the system in place for ensuring modifications are adequately designed, installed and tested.**	Failure to properly manage change management is a common cause of accidents. **<u>To meet this criterion, the safety case shall describe:</u>** a) the system for dealing with changes, updates or modifications to: • plant and equipment; • process parameters such as temperature and pressure; • operating procedures and documentation; • raw material specifications, suppliers, etc. b) the management systems for change as described under SS506: Part 3 (Management of Change). The management of change procedure shall also include: • 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 or risk assessment; • whether the hierarchical approach is used where practicable in relation to process modifications and changes; • the competence and independence of the team or individuals involved in the decision making;

	• the arrangement for temporary modifications which shall be identified together with procedures for reinstatement as appropriate. MHIs shall also identify how risk is assessed and decisions are made on temporary modifications; • the method for ensuring that the modification is installed as specified in the change proposal (e.g. pre-start-up safety review).
Performance Standards and Indicators	
5.3 The safety case shall show that performance standards and indicators (including safety indicators covered under SS506: Part 3) are implemented to provide ongoing assurance that key systems relevant to major accidents are under control.	Performance standard is the acceptable level of response or the required performance for a control to be considered effective in managing the risk. Standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe. **<u>To meet this criterion, the safety case shall show that:</u>** a) performance indicators and related performance standards enabled MHIs to: • measure, monitor and test the effectiveness of each control measure; • take corrective action based on failure to meet the performance standard; and • generate performance management reports on the integrity of the MHI's control measures and how well they are being managed. b) there are performance indicators to measure not only how well the control measures are performing, but also how well the management system is monitoring and maintaining them.

Chapter 6: Mechanical Engineering Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the mechanical engineering assessment.

1.2. This chapter is linked to **Chapter 5** of the Safety Case Technical Guide.

1.3. All mechanical engineering assessment must use the criteria and guidance set out in **Appendix E – 'Mechanical Engineering Assessment Criteria and Guidance'.**

2. The General Approach to Mechanical Assessment

2.1. MHD is looking for a demonstration that adequate safety have been taken into account in the design, construction, operation, maintenance and modification of any plant, storage facility, equipment and infrastructure connected with the installation's operation, which are linked to MAHs inside the installation.

2.2. In relation to 'any installation and equipment and infrastructure connected with its operation which are linked to MAHs within the installation', the MHD assessor is looking for:

a) <u>Adequate Initial Mechanical Integrity</u>

Demonstrated by:

(i) adherence to suitable design principles, often embodied in international codes and standards; and

(ii) suitable controls on manufacturing and construction for the delivery of design intent.

b) <u>Adequate Continuing Mechanical Integrity</u>

Demonstrated by:

(i) suitable procedures and hardware controls (e.g. trips, relief devices) to ensure that the facilities are operated within the limits for which it was designed;

(ii) appropriate maintenance and periodic examination regimes; and

(iii) suitable procedures to ensure modifications to facilities will not compromise mechanical integrity.

2.3. For new projects, design standard shall address the ten key design issues (see Safety Case Technical Guide 5.3.2.2) in the safety cases. For existing facilities, the key issues in design shall be considered for control measures implemented for SCEs.

a) Design Criteria

(i) Design and construction to an appropriate standard;
(ii) Identification of direct causes of LOC (e.g. corrosion, erosion, vibration);
(iii) Mechanical measures to prevent LOC;
(iv) Suitable materials of construction; and
(v) Selection and design of mechanical equipment for use in hazardous-classified areas.

b) Construction Criteria

(i) Construction against appropriate standards;
(ii) Controls over manufacture (e.g. welding procedures and welder competency);
(iii) Inspection and testing of initial integrity (e.g. Non-destructive testing (NDT) requirements embodied in design and construction standards);
(iv) Management of design changes during construction including mechanical integrity assessment.

c) In-Service Criteria

(i) Assuring mechanical facilities are always operated within safe limits;
(ii) Management of change to ensure that mechanical integrity is not compromised by equipment, process, or operating and maintenance system changes.

d) Maintenance and Inspection Criteria

(i) Prioritisation of safety critical equipment;
(ii) The specified design basis for major equipment items and how the impact of the selected design (e.g. pressure and temperature rating, material, corrosion allowance) on inspection, testing and maintenance requirements is assessed;
(iii) Appropriate maintenance or inspection regimes and philosophies including procedures for periodic review;
(iv) Identified degradation (damage or deterioration) mechanisms;
(v) Procedures for identifying ageing and determining the condition of mechanical facilities (e.g. from comprehensive inspection or maintenance history, measured corrosion rates, operational performance);
(vi) Assessment procedures or justifications required prior to operating facilities beyond its expected life (rather than repairing or replacing on breakdown). Requirements for increased inspection (to inform the assessment or to monitor ongoing condition of plant) shall also be described, where appropriate;
(vii) Any requirement for fitness-for-service or remnant life assessment techniques (e.g. API 579-1, ASME FFS-1) to be employed, to enable major equipment items to be returned to service following inspection;
(viii) Competence of maintenance and inspection personnel;
(ix) Analysis of maintenance and inspection findings by a competent person;
(x) Performance monitoring of integrity assurance systems.

Appendix E – 'Mechanical Engineering Assessment Criteria and Guidance'

Technical Criterion	Guidance
General Principles	
6.1 The safety case shall demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents and limit their consequences.	This is effectively a summary of criteria 6.1.1.1 to 6.1.4. MHD would come back to this when criteria 6.1.1.1 to 6.1.4 have been assessed, and then conclude: a) whether all the assessed criteria have been met; b) how significant the failure to meet one or more criteria is to the overall safety justification; c) the recommended actions for improving the safety case and suggested timescales; and d) the recommendations for follow-up inspection and verification, their priority and timescale.
Use of Industry Codes and Standards	
6.1.1.1 The safety case shall show that the installations have been designed to an appropriate standard. **The safety case shall also show how the installations have been constructed to appropriate standards to prevent major accidents and reduce LOC.**	This criterion applies to all major vessels, pipework, rotating equipment (e.g. pumps, compressors) and structures (e.g. pipe racks), relevant to MASs. **<u>The safety case shall describe adequate initial integrity of facilities by:</u>** a) reference to design codes and standards (including justification of any deviations or exceptions adopted) according to the hierarchy of preference: (i) Singapore Standard; (ii) Commonly used international standards (e.g. EN, BS, API, ISO, IEC); (iii) Other national standards (e.g. GB, DIN, JIS); (iv) Industry standards; (v) Company standards. b) reference to principal design parameters (e.g. design pressure and/or temperature) and construction as per applicable standards and code.

	Where in-house design codes and standards have been adopted, the safety case shall demonstrate: a) their relevance; and b) how the company has validated them. Where no standards have been used, the safety case shall: a) demonstrate how fitness for purpose of such facilities is assured; and b) include a description of design reviews conducted (e.g. where novel designs are employed). A table or list detailing the design codes, standards and principal design parameters for the equipment featuring in the representative MASs selected could be provided in the report to assist the demonstration. In assessing the demonstration that the mechanical design has been considered and the risk reduced to ALARP, the MHD shall consider the applicability of codes and standards in each case and adopt an approach proportionate to the overall risk. **<u>In addition, the safety case shall also:</u>** a) show that construction of plant and associated equipment is managed to ensure that it is built in accordance with the design intent; b) show, wherever available, that the manufacture and construction of facilities have employed appropriate materials and construction methods; c) show that construction work has been carried out by suitable personnel in accordance with appropriate procedures; d) provide evidence on the adequacy of procedures adopted if codes or standards have not been used or do not exist; and

	e) describe the arrangements for controlling and recording changes to the original design made during construction. Any deviations from the original that may affect safety shall be identified, and the effect on safety demonstrated to be acceptable. **[Information in the safety case shall show that the construction of the plant, including deviations from the original design, has been documented to give an assurance of conformity.]** **[For common types of installation, reference to published standards or guidance within the safety case can be an effective way of showing that adequate measures have been taken.]** **[For older plants in particular, the safety case shall describe additional (if any) systems or control measures are in place to prevent an SCE or limit its consequence, to take account of plant built to standards that have since been superseded. The safety case shall also describe any additional systems or control measures that have been introduced as a result of long operational experience on-site.]**
Design Considerations	
6.1.1.2 The safety case shall show that the layout of the plant limits the risk during operations, inspection, testing, maintenance, modification, repair and replacement.	**To assist demonstration of this criterion, the safety case shall discuss how the following were considered ,where applicable, during design of the plant layout:** **This criterion is particularly relevant during the QRA approval stage where design of the layout of a plant can make a big contribution to reducing the likelihood and consequences of a major accident.** a) Access requirements for periodic maintenance and inspection; b) Lifting provision (i.e. requirements to facilitate the removal of equipment for periodic maintenance or replacement); c) Construction and maintenance activities (e.g. to minimise the risks from dropped objects, eliminating the need to lift over live plant as far as possible).

	[MHD will be assessing the as-built layout plans against previously submitted design layout plans for any significant deviations. Justifications shall be provided to demonstrate that any significant deviation made does not result in additional risk. MHIs shall demonstrate that additional risk, if any, has been mitigated.]
6.1.1.3 The safety case shall show that utilities that are needed to implement any measure defined in the safety case shall have suitable reliability, availability and survivability.	**The safety case shall describe** the likely impact of utility failure on safety critical mechanical equipment (e.g. primary containment system). **Content provided in the safety case to assist demonstration could include:** a) the design standards for equipment incorporated within safety critical utility supplies; b) details of the monitoring, testing, maintenance and inspection regimes employed for equipment incorporated within safety critical utilities including backup system;
6.1.1.4 The safety case shall show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances.	**The safety case shall describe:** a) the mechanical measures in place to prevent and contain releases; b) the integrity (i.e. function, reliability) of such measures; and c) the availability of emergency systems (i.e. in the event of a fire or major accident). **Content provided in the safety case to assist demonstration could include discussion of** the integrity of mechanical measures such as: • emergency shutdown 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 (e.g. protection from reverse rotation and over-speed, cavitation, dry running, deadhead conditions, seal failure); • joints (e.g. suitability for intended duty of flanged and screwed joints, couplings);

	• bellows and flexible joints; • temporary repairs (e.g. clamps, wraps); • dry break couplings; • secondary containment.
6.1.1.5 The safety case shall show that all foreseeable direct causes of major accidents have been taken into account in the design of the installation.	**<u>The safety case shall describe</u>** how the following direct causes of LOC, where applicable, have been considered in the design of the installation and the selection of measures: a) **Corrosion (internal and external):** • Variations in process conditions have been considered – the equipment design and materials of construction shall accommodate foreseeable changes to the process conditions, such as variations in temperature and corrosive species (e.g. during cleaning). • Consideration of inspection requirements during design (e.g. to facilitate the detection and monitoring of corrosion under insulation). • The potential for corrosion has been eliminated or reduced (e.g. 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:** • Consideration shall be given to the effect of solids, abrasion, phase changes and cavitation. c) **External Loading:** • Consideration shall be given to the suitability of facilities to survive anticipated loadings from external sources, such as wind and rain, as well as process and dynamic loadings. The construction phase shall also be considered in addition to normal operation. d) **Impact:** • During operation (e.g. isotankers or forklift truck impact). • During construction and maintenance activities (e.g. from swinging loads, dropped objects).

	• On buildings from blast loadings. e) **Pressure:** • The installations are protected from the effects of excessive pressure and vacuum. • Pressure fluctuations are recognised as inducing fatigue failures. f) **Temperature:** • High temperatures are accommodated in the design (e.g. creep resistance) and protective systems are in place to prevent damage from excessive temperature. • Low temperature effects are avoided or controlled (e.g. brittle failure, freezing effects). • Temperature fluctuations are recognised as inducing fatigue failures (i.e. thermal fatigue). g) **Vibration:** • Consideration of both machine induced and process induced vibration (e.g. high and low frequency, water hammer). • Show elimination by design, prevention or control of vibration where possible. • Vibration induced fatigue is recognised (e.g. provision of suitable supports for small-bore connections). h) **Inappropriate Equipment and Material:** • Controls exist for the specification and supply of safety critical equipment and spares. i) **Defective Equipment:** Identification and monitoring of pre-existing flaws introduced during design and construction. **It is unacceptable for the safety case to have no explanation of how foreseeable direct causes of LOC have been taken into account in the design of the installation.**
6.1.1.6 The safety case shall show that materials of construction used in the plant are suitable for the application.	**<u>The safety case shall describe:</u>** a) the approach taken for selection of materials, demonstrating that materials of construction are suitable based on the substances being handled, expected process conditions (e.g. temperature, flow) and external environment conditions;

	• MHIs' or personnel experience of material performance may inform the selection process but should not be solely relied on. Additional assurance (e.g. worldwide performance data) shall be obtained for safety critical applications. • More expensive materials of construction (e.g. stainless steel or hastelloy) are not universally better or more appropriate for aggressive environments. Justification of their suitability for the intended use shall still be made. b) how effects of impurities on the containment materials have been taken into consideration based on impurities likely to be present under normal and abnormal conditions; c) Positive Material Identification (PMI) procedures for materials of construction where uncontrolled variations would be critical (e.g. certain high hazard applications in refining); and d) material of construction and coating system selection processes for facilities operating in corrosive environments. Example(s) detailing and justifying the materials of construction selected for particular major plant items (subject to aggressive operating environments, where appropriate) could be included into the safety case to assist the demonstration.
6.1.1.7 The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk.	**<u>The safety case shall demonstrate that:</u>** a) where mechanical equipment is to be used in potentially explosive and/or flammable atmospheres, the equipment selected is designed to be safe in hazardous areas; b) suitable international standards have been employed to identify potential ignition sources from mechanical equipment including: • heat energy (e.g. hot surfaces, hot work such as welding spatter, heating installations); and • mechanical energy from overheating or friction due to rotating equipment, impact, grinding, adiabatic compression and shockwaves, etc. c) suitable inspection, testing, cleaning and maintenance regimes have been implemented to minimise presence of flammable substances and ignition sources occurring as a result of for example overheating or fault conditions.

Construction	
6.1.2 The safety case shall show how construction of all facilities is assessed and verified against the appropriate standards to ensure adequate safety.	**<u>The safety case shall demonstrate that</u>** initial inspection, testing and commissioning of the plant has been documented and the information is retrievable (particularly for equipment forming the primary containment boundary). Where the above information is not available (e.g. for older, existing or second-hand MHIs), the safety case shall describe how major accidents are prevented or how plant integrity is demonstrated, by discussing for example: a) For older plant: inspection history; b) For second-hand plant: post-installation baseline inspection data obtained; c) operating restrictions applied, where appropriate.
Maintenance	
6.1.3.1 The safety case shall show that an appropriate maintenance regime is established for plant and systems to prevent major accidents or reduce the LOC in the event of such accidents.	**<u>The safety case shall describe:</u>** a) the maintenance administration system. Relevant job descriptions, roles and responsibilities. A department organisation chart such as organogram could be used to demonstrate, if appropriate; b) the maintenance regime adopted for equipment of high safety concern (i.e. evidence of a suitable planned and preventative maintenance regime; c) systems for periodically reviewing the suitability of the maintenance regime adopted for equipment of high safety concern (e.g. based on findings and/or failure history); d) the maintenance philosophy adopted for mechanical facilities (e.g. time, condition and/or reliability-based); and e) systems for prioritising maintenance activities (particularly in relation to safety critical equipment). **<u>Content provided in the safety case to assist demonstration could include:</u>**

	a) an overview of competency requirements of the personnel completing key mechanical maintenance activities relating to MASs on-site (e.g. company employees, external specialist contractors); b) example(s) of safety critical maintenance activities completed on mechanical equipment (e.g. bench testing of pressure relief devices); and c) examples illustrating the performance monitoring procedures applicable to the maintenance system (e.g. process safety performance indicators) including confirmation that data is periodically reviewed by senior management.
6.1.3.2 The safety case shall show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment.	**<u>The safety case shall include:</u>** a) an overview of the mechanical isolation practices adopted on-site, prior to completing intrusive activities on equipment; and **[MHD will focus on potential MAHs. Concerns relating to particular hazardous activities may be addressed within the intervention plan.]** b) a description of how the mechanical isolation procedures fit into the overall maintenance management procedures (e.g. permit-to-work system) adopted on-site.
6.1.3.3 The safety case shall show that systems are in place to ensure that safety critical equipment and systems are examined at appropriate intervals by a competent person. **The safety case shall also show that there is a system in place to ensure the continued safety of the**	**This criterion is concerned with in-service integrity of safety critical equipment and statutory equipment.** **[The safety case shall include a demonstration that suitable inspection regimes are in place and required pre-checks have been completed by competent person.]** **<u>The safety case shall describe:</u>** a) the periodic in-service examination regimes adopted; b) the procedures for analysing inspection findings and confirming that the relevant equipment is endorsed for a period of operating service before the next examination is required. The role of external accredited organisations shall also be described, where employed; and

installations based on the results of periodic examinations and maintenance.	c) how inspection regimes are reviewed to ensure that they remain suitable and relevant. Typical contents of an inspection regime for the relevant equipment include: (i) identifications of the equipment and machineries within the MHI; (ii) those parts of the system which are to be examined; (iii) the nature of the examination required, including the inspection and testing to be carried out on any protective devices; (iv) where appropriate, the nature of any examination needed before the system is first used; (v) the maximum interval between examinations; (vi) the critical parts of the system which, if modified or repaired, should be examined by a competent person before the system is used again; (vii) the name and position, where applicable, of the competent person approving the inspection regime; and (viii) the date of the inspection. **<u>Content provided in the safety case to assist demonstration could include:</u>** a) systems for the prioritisation of safety critical systems; b) independence and competence of inspection staff; c) justification of inspection scope and frequencies by reference to relevant industry standards, where appropriate, and to analysis of inspection findings; and d) appropriate systems for managing follow-up actions resulting from periodic inspection. Where Risk-Based Inspection (RBI) is employed, the safety case shall show: a) that the RBI assessment team contains the experience and knowledge required for a suitable and sufficient analysis; b) that a thorough and systematic process is employed for identifying all relevant damage mechanisms and likely locations including referencing to relevant industry guidance, where appropriate; and

	c) that a suitably cautious approach is taken to changes in inspection frequency indicated by the RBI process, with the competent person involved in any modification to the inspection regime. **[The approach to integrity management adopted shall reflect the complexity of the plant and the potential severity of the consequences of failure.]**
Modification and Decommissioning	
6.1.4 The safety case shall describe the system in place for ensuring modifications are adequately designed, installed and tested.	**For new or major plant modification projects, the safety case shall describe** the system in place for identifying and managing modifications during the design and construction phases. **[The above process may be implemented by the principal design and/or construction contractor and may differ from the change management procedure ultimately adopted by the MHIs, following project 'handover'.]** **In addition, the safety case shall demonstrate:** a) how MHIs' modification procedure covers changes to existing facilities b) how the potential impact of new equipment on existing systems is assessed; c) technical approval processes for proposed modifications (e.g. demonstrations that the concept has been properly addressed for mechanical integrity); d) pre-start-up safety review to confirm that the construction and equipment is in accordance with specifications; and e) procedures for integrating new facilities within existing integrity management arrangements. **[Where arrangements exist for temporary modifications, they shall be identified in the safety case, together with procedures for reinstatement as appropriate. MHIs shall identify how risk is assessed and decisions made for temporary modifications.]**

	<u>For decommissioning or mothballing projects, the safety case shall describe:</u> a) the system in place for identifying decommissioned or mothballed facilities; and b) the arrangement in place to ensure that the removal or mothballing of such facilities shall not lead to an increased risk associated with the use of the remaining facilities.
Performance Standards and Indicators	
6.2 The safety case shall show that performance standards and indicators (including safety indicators covered under SS506: Part 3) are implemented to provide ongoing assurance that key systems relevant to major accidents are under control.	Performance standard is the acceptable level of response or the required performance for a control to be considered effective in managing the risk. Standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe. **<u>To meet this criterion, the safety case shall show that:</u>** a) performance indicators and related performance standards enabled MHIs to: • measure, monitor and test the effectiveness of each control measure; • take corrective action based on failure to meet the performance standard; and • generate performance management reports on the integrity of the MHI's control measures and how well they are being managed. b) there are performance indicators to measure not only how well the control measures are performing, but also how well the management system is monitoring and maintaining them.

Chapter 7: Electrical, Control & Instrumentation Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the electrical, control and instrumentation (EC&I) assessment.

1.2. This chapter is linked to **Chapter 5** of the Safety Case Technical Guide.

1.3. All EC&I assessment must use the criteria and guidance set out in **Appendix F – 'Electrical, Control & Instrumentation Assessment Criteria and Guidance'.**

2. The General Approach to EC&I Assessment

2.1. MHD is looking for a demonstration that adequate safety have been taken into account in the design, construction, operation, maintenance and modification of any plant, storage facility, equipment and infrastructure connected with the installation's operation, which are linked to MAHs inside the installation.

2.2. For the assessment of EC&I, the MHD would be covering on three priority topics:

a) Functional safety;
b) Explosive and/or flammable atmospheres; and
c) Electrical power systems.

Functional Safety

2.3. Functional safety is concerned with the management, design, installation, operation, maintenance and modification of instrumented process safety systems that reduce the risk of a major accident. Such systems include:

- process control systems;
- safety instrumented systems;
- alarm systems.

Explosive and/or Flammable Atmospheres

2.4. In the context of EC&I inspection, explosive and/or flammable atmospheres are concerned with the management, design, installation, operation, maintenance and modification of systems that reduce the risk of electrical sources of ignition arising from:

- electrical and instrumentation equipment;
- lightning;
- static;

and the mitigation of releases using:

- flammable gas detection;
- fire detection.

Electrical Power Systems

2.5. In the context of MAHs, electrical power systems are concerned with:

a) the management , design, installation, operation, maintenance and modification of electrical power systems so that they provide the necessary reliability and availability to prevent or mitigate major accidents and prevent danger to personnel; and
b) the initiation of major accidents by electrical equipment through fire and explosion.

2.6. MHD is also looking for an adequate description of the following aspects of the safety and health management system, so far as they apply to the EC&I discipline:

a) structure, responsibility and authority;
b) operational control;
c) management of change; and
d) performance standards and indicators.

Appendix F – 'Electrical, Control & Instrumentation Assessment Criteria and Guidance'

Technical Criterion	Guidance
Link with Predictive Criteria (Chapter 4)	
7.1 The safety case shall show a clear link between the measures taken and the SCEs described.	**<u>To meet this criterion, the safety case shall describe:</u>** a) how necessary instrumented safety functions are identified for SCEs; b) how the required integrity of instrumented safety functions is determined and competency of team determining the SIL levels, if relevant; c) how, in general terms, other EC&I measures such as fire and gas detection systems are applied to MASs (e.g. by reference to process risk assessments). **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample SIL determination record (e.g. LOPA, risk graph output)
Use of Industry Codes and Standards	
7.1.1.1 The safety case shall show that the installations have been designed to an appropriate standard.	**<u>To meet this criterion, the safety case shall describe</u>** the general approach to the application of EC&I design standards for example: a) Singapore Standard; b) Commonly used international standards (e.g. EN, BS, API, ISO, IEC); c) Other national standards (e.g. GB, DIN, JIS); d) Industry standards; e) Company standards and how it has been established that they align with relevant good practice. **[For common types of installation, reference to published standards or guidance within the safety case can be an effective way of showing that adequate measures have been taken.]**

	[For older plants in particular, the safety case shall describe additional (if any) systems or control measures are in place to prevent an SCE or limit its consequence, to take account of plant built to standards that have since been superseded. The safety case shall also describe any additional systems or control measures that have been introduced as a result of long operational experience on-site.]
Design Considerations	
7.1.1.2 The safety case shall show that utilities that are needed to implement any measure defined in the safety case shall have suitable reliability, availability and survivability.	**<u>To meet this criterion, the safety case shall describe</u>** how electrical and instrument air supplies (and any other fluid used to provide motive force to instrumentation and control such as nitrogen) have been designed to have suitable reliability, availability and survivability, including: a) the standards applied to the design of supplies; b) the sources of supply; c) the supplies that are essential for the operation of safety systems; d) the integrity requirements for supplies; e) any instrumentation employed to maintain the integrity of supplies (e.g. level alarms on cooling water vessels); f) the use of diverse and/or back-up supplies; g) how partial and total loss of supplies has been considered (e.g. as part of a structured hazard identification and analyses process); h) the effect of the partial and total loss of supplies; i) means of ensuring that power supply to human-operated control systems survives during a major accident such as via an uninterruptible power supply (UPS); j) UPS systems support all necessary instrumentation and equipment to address emergency situations: (i) control room interfaces; Supervisory Control and Data Acquisition (SCADA) systems; local panels; (ii) level monitoring and gauging equipment; (iii) process alarms; site-wide evacuation alarms; (iv) radio base stations; land-line communication systems; (v) other remotely operated shutdown equipment.

	k) how it has been determined that electrical distribution equipment is not overstressed; l) the standards applied to the design of electrical power system earthing; m) how the ignition risk from excessive stress voltages in LV (low voltage) distribution systems is managed; n) how high energy electrical equipment that poses a risk to major hazard plant has been identified and managed. **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample of a current electrical signal line diagram demonstrating diversity and/or redundancy of electrical supply; b) sample fault energy level calculation for a typical HV (high voltage) and a typical LV switchboard; c) sample protection coordination study for a typical HV and a typical LV substation and switchroom showing that adequate selectivity and protection has been achieved.
7.1.1.3 The safety case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions	**<u>To meet this criterion, the safety case shall describe:</u>** a) the overall process control strategy, for example: • automatic control; • manual control; • automatic safety systems; • alarm and operator action. b) the types of installed control and safety systems, for example: • distributed control systems; • panel-mounted controllers; • standalone control systems such as burner management systems (BMS); • Programmable Logic Controller (PLC)-based packaged units; • safety PLCs; • individual hardwired instrument safety loops; • alarm annunciators.

	c) how independence and separation between control and safety systems has been achieved; d) the system for determining, recording and reviewing safe operating limits and how these relate to control alarm and trip settings; e) how control & safety system settings are reviewed based on operating history and accounting for any modifications; and f) the standards applied to alarm management.
7.1.1.4 The safety case shall show how safety-related control systems have been designed to ensure safety and reliability.	**<u>To meet this criterion, the safety case shall describe:</u>** a) the standards applied to the design of instrumented safety systems, including: (i) process safety systems; (ii) machinery safety systems (e.g. where machines are used in the manufacture of chemicals or explosives); b) the general approach to functional safety management; c) how it has been assured that persons involved in the design of safety instrumented systems (SIS) are competent to carry out the activities for which they are accountable; d) how current relevant good practice (e.g. IEC 61511) has been applied as far as reasonably practicable to systems designed before its publication; e) how instrumented safety systems with a required integrity of less than SIL 1 are managed; f) the design of alarm systems, including how the reliability of the operator is taken into account; and g) the extent to which fire and gas detection systems are used to initiate executive action (e.g. deluge systems, inerting systems, automatic dump systems). **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample safety requirements specification (SRS); b) sample SIL assessment record (e.g. PFD calculation and fault tolerance assessment); c) sample record of competence for an individual involved in the design of SIS or in the review of SIS against relevant good practice.

7.1.1.5 The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk.	**<u>To meet this criterion, the safety case shall describe:</u>** a) the standards applied to: • the design and selection of explosion protected (Ex) equipment; • the design of lightning protection systems; • the management of hazards due to static electricity; • the management of cathodic protection in explosive and/or flammable atmospheres; • the management of lift trucks in potentially flammable atmospheres. b) how the requirements for lightning protection and surge suppression systems were established, wherever relevant; c) in overview, the installed lightning protection and surge suppression systems including lightning protection levels where relevant; and d) how it has been assured that competent persons are involved in the selection and installation of equipment and protective systems designed to be safe in explosive and/or flammable atmosphere.

Construction		
7.1.2	**The safety case shall show how construction of all plant and systems is assessed and verified against the appropriate standards to ensure adequate safety.**	**<u>To meet this criterion, the safety case shall describe:</u>** the standards applied to the construction verification of: a) safety instrumented systems (SIS); b) explosion protected (Ex) equipment; c) electrical power systems; and d) the process for ensuring that the EC&I equipment and systems are verified against the appropriate standards to ensure adequate safety prior to the MAHs being present. **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample functional safety assessment; b) sample Ex inspection record; c) record of competence (e.g. certificate of core competence) of the persons who carried out the initial inspections; d) sample industrial LV fixed installation inspection & test (verification) record.
Operation		
7.1.3	**The safety case shall show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions.**	**<u>To meet this criterion, the safety case shall describe:</u>** a) the control of operation of electrical switchgear, including the control of switching by subcontractors and distribution network operators; and b) the procedure for identifying, reporting and investigating the failure of EC&I protective measures against major accidents. **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample record of authorisation for person(s) authorised to operate electrical LV, HV and generation systems.

Maintenance	
7.1.4.1 The safety case shall show that an appropriate maintenance regime is established for plant and systems to prevent major accidents or reduce the LOC in the event of such accidents.	**<u>To meet this criterion, the safety case shall describe:</u>** a) the MHIs' maintenance management system, including: • how scheduled work is planned and prioritised; • how the repair work is prioritised (e.g. defects). b) the location and structure of the MHIs' EC&I safety critical elements inventories (e.g. Ex equipment, temperature and pressure sensors, PLCs, emergency block valves, SIS, electrical supplies); c) the strategy and methodology for monitoring and control of the condition of the equipment; d) the strategy for managing obsolescent EC&I equipment; e) the standards applied to the maintenance and proof testing of SIS; f) how the maintenance and testing of SIS is managed; g) the standards applied to the maintenance and inspection of equipment in explosive and/or flammable atmospheres, including fixed and mobile equipment; h) how the maintenance and inspection of equipment in explosive and/or flammable atmospheres, including fixed and mobile equipment, is managed; i) the standards applied to the maintenance and inspection of electrical power systems; j) how the maintenance and inspection of electrical power systems is managed; and k) how it has been assured that persons involved in the maintenance of EC&I equipment and systems are competent. **<u>Content provided in the safety case to assist demonstration could include</u>:** a) functional safety: • Sample SIS proof test procedure; • Sample record of completed SIS proof test. b) Equipment in explosive and/or flammable atmospheres:

	• Representative sample of periodic Ex inspection records (or records of continuous supervision), including protection concepts (e.g. d, e, N, I and tD from IEC 60079/61241) where they exist on-site; • Record of competence (e.g. Licenced Electrical Worker) of the persons who carried out the inspections (or continuous supervision); • Sample lightning protection system test and inspection record; • Sample static earthing system test and inspection record; • Sample flammable gas detector test and inspection record; • Sample fire detector test and inspection record; • Sample toxic gas detector test and inspection record. c) Electrical power systems: • Sample HV and LV transformer periodic inspection and test record; • Sample HV and LV switchgear inspection and test record; • Sample electrical power system earthing inspection and test record; • Sample emergency generator periodic inspection, maintenance and test (no load and/or load) record.
7.1.4.2 The safety case shall show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment.	**<u>To meet this criterion, the safety case shall describe:</u>** a) how safe work practices are applied to EC&I maintenance activities; and b) how electrical safety rules, including isolation of electrical supplies, are applied to maintenance activities, wherever applicable.

7.1.4.3 The safety case shall show that there is a system in place to ensure the continued safety of the installations based on the results of periodic examinations and maintenance.	**<u>To meet this criterion, the safety case shall describe:</u>** a) performance monitoring of EC&I systems and equipment, including the use of performance standards and indicators such as faults and failures found during operation, inspection and testing; and b) how the results of performance monitoring are used to ensure the continued safety of the installations.
Modification and Decommissioning	
7.1.5 The safety case shall describe the system in place for ensuring modifications are adequately designed, installed and tested.	**<u>To meet this criterion, the safety case shall describe:</u>** a) how the impact on EC&I systems, equipment, operation and maintenance are addressed when carrying out plant and process modifications; b) how management of change is applied to SIS. **<u>Content provided in the safety case to assist demonstration could include</u>:** a) sample record for management of change showing consideration of instrumented safety systems.

Performance Standards and Indicators	
7.2 The safety case shall show that performance standards and indicators (including safety indicators covered under SS506: Part 3) are implemented to provide ongoing assurance that key systems relevant to major accidents are under control.	Performance standard is the acceptable level of response or the required performance for a control to be considered effective in managing the risk. Standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe. **<u>To meet this criterion, the safety case shall show that:</u>** a) performance indicators and related performance standards enabled MHIs to: • measure, monitor and test the effectiveness of each control measure; • take corrective action based on failure to meet the performance standard; and • generate performance management reports on the integrity of the MHI's control measures and how well they are being managed. b) there are performance indicators to measure not only how well the control measures are performing, but also how well the management system is monitoring and maintaining them.

Chapter 8: Human Factors Aspects of Safety Case Assessment

1. Introduction

1.1. This guide is for MHD assessors completing the human factors assessment.

1.2. This chapter is linked to **Chapter 3, 4, 5, 6, and 7** of the Safety Case Technical Guide.

1.3. All human factors assessment must use the criteria and guidance set out in **Appendix G – 'Human Factors Assessment Criteria and Guidance'.**

1.4. MHIs are allowed the flexibility to take a phased implementation approach towards human factors in the safety case. The MHD will carry out the human factors assessment in three submission cycles with the first cycle starting with the MHIs' first safety case submission. Subsequent cycles (i.e. 2nd and 3rd) will take place during the 5-yearly submission of the reviewed safety case. Starting from the third cycle, the human factors criteria outlined in this assessment guide will be fully applied by the MHD during the assessment of the safety case.

2. The General Approach to Human Factors Assessment

2.1. The safety case shall demonstrate how measures taken will prevent foreseeable human failures that could lead to major accidents. MHIs should have a systematic approach to managing human performance based on a thorough understanding of human reliability and where the site is vulnerable to human failure. There should be a system in place to:

a) identify all safety critical tasks at the site, and those which could initiate, prevent or mitigate the representative set of MASs;
b) analyse the tasks for the potential for human failure (task analysis and human failure analysis);
c) identify appropriate risk control measures matched to the type of human failure and implement them; and
d) identify any performance influencing factors (PIF) and introduces measures to optimise performance.

2.2. The human factors discipline covers a range of topics including:

a) Human Reliability

(i) A structured and systematic approach to identify and manage human failure is evident for both operation and maintenance functions;
(ii) Human factors are integrated into accident, incident and near-miss investigations as per SS506 Part 3: Section 4.5.3(c).

b) Ergonomics Design of Facilities, Equipment, Working Environment and Tasks

(i) Human factors are integrated into the MHI's management of change and design processes and the MHI has arrangements to integrate human factors into all major modifications and new projects;

(ii) A hierarchical approach to the selection of risk control measures has been adopted and there is a clear justification for the allocation of functions[1] to humans or to automation;

(iii) Human failure is systematically addressed during the design of safety instrumented systems;

(iv) Facilities, equipment, workstations, etc. are designed with user capability in mind, considering construction, operation, maintenance and decommissioning tasks;

(v) The design (and upgrade) of control rooms and interfaces is user-centric;

(vi) Alarm systems are designed and managed to take account of limitations in human performance;

(vii) Environmental effects such as working space, temperature, lighting, etc., and their effects on human performance are considered in the design process.

c) Optimisation of Organisational Performance Influencing Factors

(i) Robust and systematic arrangements for the management of organisational change related to major accidents. Organisational changes include examples such as:

- downsizing with a reduction in staffing levels;
- a move to multi-skilling;
- de-layering and changes in supervision such as introducing self-managed teams;
- outsourcing of key functions to contractors;
- centralisation or dispersal of functions;
- mergers and/or acquisitions;
- changes to roles or position related to risk management of major accidents.

(ii) A structured framework to ensure that there are adequate numbers of competent people with realistic workloads to prevent and mitigate major hazards in MHIs – especially during abnormal and/or upset conditions;

(iii) Suitable arrangements are in place to manage shift work and fatigue;

(iv) Effective arrangements for safety critical communications including shift handover system;

(v) A description of supervisory arrangements.

Use of Examples in the Safety Case

2.3. Where appropriate, MHIs should consider providing examples of:

a) Task analysis and human failure analysis;

b) Documented assumptions underpinning assessment of human performance in SIL and LOPAs;

c) Consideration of how equipment design and the associated operating environment minimise Human failure or improving equipment design to provide a more error tolerant system

[1] The UK HSE website provides further explanation on allocation of function and this can be found under http://www.hse.gov.uk/humanfactors/resources/safety-report-assessment-guide.pdf

d) Where a measure relies on human intervention, an explanation as to why human intervention has been selected in preference to an automated system;

e) Management of organisational PIFs (e.g. shift work and overtime arrangements to minimise fatigue, staffing levels and supervisions).

Appendix G – 'Human Factors Assessment Criteria and Guidance'

Technical Criterion	Guidance
MAPP and SHMS Aspects	
8.1.1 ***Resources*** **The safety case shall show how MHI allocates resources to implement the MAPP.** *(Same as criterion 3.5 of Safety Case Assessment Guide Chapter 3)*	**i. STAFFING LEVELS** The safety case shall explain how senior management provide sufficient human resources to maintain adequate staffing levels for the full range of safety-critical tasks at the installation. **<u>To meet this criterion, the safety case should describe:</u>** a) the methodology by which appropriate staffing levels have been set for: (i) the full range of normal operations including (e.g. start-up of continuous processes); (ii) especially during abnormal or upset conditions (i.e. how staffing arrangement are set not to affect the reliability and timeliness of detecting, diagnosing and recovering from MASs); and (iii) the full range of maintenance activities including turnarounds where relevant. b) arrangements for ensuring that the identified staffing levels are maintained; c) arrangements for detecting, assessing and addressing workloads which are either too high or too low. **ii. MANAGEMENT OF SHIFT WORK** Fatigue may result in slower reactions, reduced ability to process information, memory lapses, absent-minded slips, lack of attention, etc. **<u>To meet this criterion, the safety case should describe:</u>** a) the methodology by which appropriate staffing levels have been set for:

	(i) the full range of normal operations including start-up, shutdown and non-routine activities (i.e. how staffing arrangement affect the reliability and timeliness of detecting, diagnosing and recovering from MASs); (ii) maintenance shift activities including turnarounds where relevant; and b) the framework for managing fatigue using appropriate standards and good practice including: (i) a policy that specifically guards against fatigue by addressing shift patterns, working hours, overtime, etc.; (ii) guidance on shift roster design that takes account of shift types, shift lengths, rest periods, rotation and social factors, etc.; (iii) consideration of environmental factors (e.g. temperature, noise levels, ventilation, lighting); (iv) systematic arrangement of changes to working hours and shift patterns; (v) arrangements to set, record, monitor and enforce limits and standards for working hours, overtime, on-call duties, shift swapping, etc.; (vi) arrangements to educate personnel in fatigue risks; (vii) arrangements for personnel and contractors to report fatigue problems.
8.1.2 ***Personal Performance*** **The safety case shall show that the performance of people having a role to play in the management of MAHs is measured and that they are held accountable for their performance.** *(Same as criterion 3.6 of Safety Case Assessment Guide Chapter 3)*	**i. SUPERVISION** The safety case explains the on-site arrangements for supervision of operational and maintenance teams. **<u>To meet this criterion, the safety case should describe:</u>** a) competence standards have been established for supervisory personnel which include: (i) non-technical skills (e.g. leadership, managing poor performance, communicating effectively); (ii) technical skills (relevant to the facility and process); and (iii) management of organisational PIFs within their control (competence assurance, workload, staffing levels, shift work, fatigue, etc.). b) supervisory roles and responsibilities are clearly defined in the context of MAHs (this would have been assessed under the MAPP and SHMS assessment portion);

	c) supervisory role in managing compliance with safety-critical rules and procedures. **ii. PROCEDURES COMPLIANCE** **<u>To meet this criterion, the safety case should describe</u>** the arrangements developed to ensure day-to-day compliance with safety-critical procedures, including effective supervision (e.g. there are enough supervisors, with sufficient time, to carry out their supervisory responsibilities; those responsibilities are clearly defined; supervisors display a good understanding of MAHs and control measures).
8.1.3 ***Internal Communication*** **The safety case shall show that the MHI has arrangements for communicating information important for the control of MASs within the MHI's organisation.** *(Same as criterion 3.10 of Safety Case Assessment Guide Chapter 3)*	**<u>To meet this criterion, the safety case should describe:</u>** **i. SHIFT HANDOVER** Arrangements for shift handover: a) The standards and/or procedures for shift handover which has been implemented; b) Support equipment which is provided (structured written or electronic logs); c) Allocation of time for incoming and outgoing shifts to discuss plant status face-to-face; d) Arrangements to schedule maintenance within shifts, or arrangements to control maintenance work that crosses shifts. **ii. REMOTE COMMUNICATIONS** Arrangements for remote communications and the measures taken to ensure: a) remote communication equipment (e.g. radios, intercoms, public announcement systems, telephones) is suitable and reliable; b) users are competent in the use of equipment and associated radio protocols.

8.1.4 ***Investigation and Corrective Action*** **The safety case shall show that the MHI has adopted mechanisms for investigating and taking corrective action:** **a) in cases of the proactive performance standards showing a deterioration in risk control measures; and** **b) in relation to any incident or event with potential to cause a MAS.** *(Same as criterion 3.16 of Safety Case Assessment Guide Chapter 3)*	SS506: Part 3 stated investigation shall consider human factors. **<u>To meet this criterion, the safety case shall describe how:</u>** a) the investigation process is clearly defined via procedures and checklists, encouraging investigators to determine why human failures occur; b) a systematic approach is adopted (e.g. investigations follow a path similar to human failure analysis); c) immediate human failures as well as latent human failures (e.g. decisions remote in time and place from the incident) are addressed; d) contributing factors (e.g. PIFs) are identified at job, individual and organisational levels. The demonstration could include the documented findings of an accident investigation.
Predictive Aspects	
8.2 The safety case shall demonstrate that a systematic process has been used to identify events and events combinations which could cause MAHs to be realised. *(Same as criterion 4.2.1 of Safety Case Assessment Guide Chapter 4)*	MAH risk assessment process needs to consider human factors. Supporting documents (e.g. LOPA, bowtie diagrams) should clearly illustrate the part played by people in initiating, preventing and mitigating the consequences of MAHs. The potential for dependency between successive human task has been recognised and accounted e.g.: a) the human failure probabilities for one task may be significantly influenced by an error in previous related step or task; b) the same person may make the same or similar failure during a number of tasks; c) a staff responsible for cross-checking may fail to detect an error. **<u>To meet this criterion, the safety case should describe:</u>**

	a) the methodology for identifying safety critical tasks in the MHI (including e.g. routine; non-routine; abnormal and upset; first line emergency response; safety critical maintenance, inspection and testing activities); b) the methodology used for task and human failure analysis – an appropriate system could include: (i) structured task analysis, to gain a thorough understanding of the task and identify safety critical steps (the latter being the focus for in-depth analysis); (ii) systematic identification of the different types of human failure (slips, lapses, mistakes and violations, etc.) using a recognised methodology; (iii) active involvement of front-line personnel who currently perform the task being analysed (with support from competent facilitators). c) a suitably prioritised programme of task and human failure analysis that accounts for the full range of safety critical tasks related to representative MASs in the MHI. A typical programme may run over a number of years. d) arrangement to ensure that those who undertake or facilitate task and human failure analysis are knowledgeable to do so.
General Principles	
8.3 The safety case shall demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents and limit their consequences.	**<u>This criterion is to be completed last.</u>** This is effectively a summary of criteria 8.3.1.1 to 8.3.2, the MHD would come back to this when criteria 8.3.1.1 to 8.3.2 have been assessed, and then conclude that the safety case has demonstrated that: a) a structured and systematic approach to managing human performance in the context of MAHs; and b) risk control measures, and the supporting MAPP and SHMS, are built upon a sound understanding of how human failure plays a part in initiating, escalating, and failing to mitigate the consequences of major accidents. Overall, where reliance is placed on people as part of the package of necessary measures, the safety case demonstrates that human factors issues (such as human reliability) are being addressed with the same rigour as technical and engineering measures.

Design Considerations	
8.3.1.1 The safety case shall show that the installations have been designed to an appropriate standard.	**HUMAN FACTORS IN DESIGN** **This criterion is particularly relevant for new projects. However for existing MHIs, this criterion should be raised for on-site verification.** **<u>To meet this criterion, the safety case should show:</u>** a) 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; b) that the MHI applies a hierarchy of control measures, which aims to remove reliance on humans, or improve system design, where human performance has a higher probability of failure; c) recognition that training should not be solely relied upon as a control measure to tackle human factors problem and should prioritises automation and user-centred design over procedures and training; d) the implications of human failure in automated systems (via design, inspection, testing, maintenance, etc.) are acknowledged and addressed; e) the need for manual intervention in higher risk processes or activities (e.g. manual emergency shutdown of a continuous process) is clearly justified **(this is a priority for verification by inspection)**; f) where possible, human performance is further assured by mechanical or electrical means (e.g. sequentially interlocked valves; interlocked earth-proving for isotanker operation); g) **where procedures and training are solely relied upon as a risk control measures**, the safety case should show that: (i) the relevant scenarios have been identified and analysed; (ii) the analysis supports the development of the procedures and training; (iii) the competence management system is in place which includes procedures and training; and (iv) the procedures and training manage risk to an acceptable level. h) facilities, equipment, workstations and control systems are designed with human performance in mind; and

	i) how the company integrate human factors in the design and commissioning process for all new and major modification projects: (i) Human factors principles are integrated into design; (ii) Human factors are considered throughout the project development lifecycle; (iii) Relevant front-line personnel including both operations and maintenance personnel are involved in the design process, where relevant; (iv) Usability or operability and maintainability are based on a user-centric design as far as applicable; (v) The design process contributes to the identification of procedural and training needs of relevant users; and (vi) Relevant general design standards have been applied on-site. **The demonstration could include a worked example.** **[For common types of installation, reference to published standards or guidance within the safety case can be an effective way of showing that adequate measures have been taken.]** **[For older plants in particular, the safety case shall describe additional (if any) systems or control measures are in place to prevent an SCE or limit its consequence, to take account of plant built to standards that have since been superseded. The safety case shall also describe any additional systems or control measures that have been introduced as a result of long operational experience on-site.]**
8.3.1.2 The safety case shall show that the layout of the plant limits the risk during operations, inspection, testing, maintenance, modification, repair and replacement.	**This criterion is relevant for new or modification projects. However for existing MHIs, this criterion should be raised for on-site verification.** **<u>To meet this criterion, the safety case should describe:</u>** How systems are designed for operability and maintainability:

	a) Facilities and equipment, including layout on-site, are designed with human performance in mind (e.g. accessibility for inspection, testing and maintenance); b) The working environment (noise; temperature; lighting, etc., e.g. in control rooms) has been considered; c) Facilities and equipment are clearly identified and labelled so as to reduce the likelihood of error; d) Up-to-date P&IDs, schematics, line diagrams, job-aids and other diagnostic tools are available for operation and maintenance.
8.3.1.3 The safety case shall show that utilities that are needed to implement any measure defined in the safety case shall have suitable reliability, availability and survivability.	**<u>To meet this criterion, the safety case report should describe</u>** where appropriate, the availability of system required for human invention following utility failure: a) UPS systems provide sufficient time to enable orderly shutdown and/or evacuation; b) there is adequate emergency lighting to carry out relevant shutdown tasks; where appropriate, hand-held torches are available.
8.3.1.4 The safety case shall show how safety-related control systems have been designed to ensure safety and reliability.	**This criterion is relevant for new or modification projects. However for existing MHIs, this criterion should be raised for on-site verification.** **<u>To meet this criterion, the safety case should describe</u>** how the potential for human failure is identified and systematically treated in the design of safety-related control systems (e.g. safety instrumented systems). The design process prompts a multi-discipline, team approach (including input from operators and human factors specialists, where applicable). <u>The MHI has identified tasks where:</u> a) human failure could lead to a demand on the safety function (e.g. errors in setting process parameters, conflicting responsibilities that may distract the operator's attention; unauthorised use of system overrides); b) human action could reduce the demand rate on the safety function (e.g. responding to alarms); c) failure of the safety function requires actions to mitigate the consequences of the event.

	<u>The safety case is realistic about levels of risk reduction claimed for alarm systems and considers:</u> a) availability of the operator to respond; b) adequacy of time to respond; c) the potential for alarm flooding; d) whether the operator knows how to respond (i.e. there is a clear, documented response for each critical alarm, supported by training). **<u>In addition, the safety case should:</u>** a) show that assumptions about human performance in the control system (relating to representative MASs) are documented; an example could be included in the safety case; b) identify and address human failures that increase the likelihood of the safety function failing to work on demand (inspection, testing, maintenance, calibration, etc.); c) describe how MHI identifies and addresses the potential for operators to override safety functions; and d) where appropriate, consider the availability of human-operated control systems during upset and emergencies (e.g. is control room toxic refuge, can operator reach shut-off valves).
8.3.1.5 The safety case shall show how systems which require human interactions have been designed to take into account the needs of the user and be reliable.	**<u>To meet this criterion, the safety case should describe:</u>** **i. MANUAL CONTROL OF SYSTEMS** Where relevant to representative MASs, the measures taken to ensure human reliability, where there is a reliance on human performance to keep a system within safe operating limits manually. This include examples such as: a) Facilities (e.g. valves, flow direction and contents of pipework) and materials (e.g. chemicals added manually to batch processes) are clearly labelled; b) Information about the status of the process is available to the operator (e.g. pressure gauges, sight glasses are appropriately located);

	c) Procedure has been optimised to support the operator in the field; d) Where applicable, process control systems inform the operators if unsafe set points or parameters are entered into the system. **ii. CONTROL ROOM AND INTERFACE DESIGN** **This criterion is relevant for new or modification projects. However for existing MHIs, this criterion should be raised for on-site verification.** Where there is a control room: a) the safety case contains a clear description of the control room environment and associated process control systems and interfaces; b) 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; c) design criteria encompass control room arrangements and layout; panel workstations; displays and controls; environmental conditions (lighting; acoustics; ventilation, temperature, etc.); d) the experience of operators and engineering and maintenance personnel is captured and fed back into the upgrade process; e) training for DCS and SIS covers specific, local operational issues as well as generic functionality of the interface and familiarisation with system operating manuals. **iii. ALARM HANDLING** How MHI has set out their philosophy with regard to the design and management of alarms. This includes description on how: a) alarm handling is fully integrated into the design process;

	b) the design process acknowledges and accommodates human capabilities and limitations (including operator availability to respond; time to respond; the potential for alarm flooding etc.); c) alarms will be justified and prioritised; d) relevant performance indicators are defined and monitored (e.g. average alarm rate; upset alarm rate; average number of standing alarms; bad actors); e) alarm systems are subject to continuous improvement (e.g. based on performance indicators). In particular: a) maximum tank levels and level alarm settings are clearly defined to ensure there is sufficient time for detection, diagnosis, planning and action; b) the safety case describes how alarm systems alert, inform and guide operator action (including a defined, documented response for each safety critical alarm, supported by training and assessment); c) specific examples could be included within the safety case to show how relevant standards and good practice have been applied on-site.
Modification and Decommissioning	
8.3.2 The safety case shall describe the system in place for ensuring modifications are adequately designed, installed and tested.	The MHI should demonstrate that human factors are considered in major projects. **<u>To meet this criterion, the safety case should describe how:</u>** a) ensuring that specific human factors activities are built into project plans and are sufficiently resourced; b) understanding and specifying the context of use of the proposed modifications, identifying who the users are, what they will be doing, including assessing the impact of the change on workload and staffing levels; c) ensuring that user characteristics and tasks analysis are considered as the basis for design; d) specifying the user and organisational requirements, and ensuring a balance between user-centred design options and relative cost; e) applying human factors expertise to generate design options which meet user requirements (planning in time for iterative design and using prototypes to evaluate user experience); f) evaluating requirements by involving target users and human factors specialists.

	g) the management of organisational change procedure has been applied related to major accidents; h) procedures have been updated to reflect the change; and i) training has been provided. **The demonstration could include a specific example.**
Risk Assessment and Risk Reduction Measures	
8.4 The safety case shall clearly describe how MHIs use risk assessment to help make decisions about the measures necessary to prevent major accidents or to mitigate their consequences. *(Same as criterion 10.1 of Safety Case Assessment Guide Chapter 10)*	**<u>To meet this criterion, the safety case shall show that</u>** risk reduction measures implemented to reduce or remove the likelihood of human failure are: a) matched to the human failure types identified; and b) where necessary, optimise the local performance influencing factors that make the error more likely. **Training and procedures are not viewed as the sole defence against human failure** – they form an integral part of a broader range of measures to reduce the potential for human failure. The risk assessment methodology should make it clear that: a) where appropriate, the human contribution to failure is removed (e.g. by a more reliable, automated system); b) automation is selected for the right reasons – there is consideration of involving the operators in the process and maintaining their situation awareness, and of the potential for alarm overload.

Chapter 9: Emergency Response Aspects of Safety Case Assessment

1. Introduction

1.1 This guidance is for MHD assessors completing the Emergency Response assessment.

1.2 This chapter is linked to **Chapter 6** of the Safety Case Technical Guide.

1.3 All emergency Response assessments must use the criteria and guidance set out in **Appendix H – 'Emergency Response Assessment Criteria and Guidance'.**

1.4 The aim shall be to demonstrate that MHIs have taken the measures necessary to limit the consequences of a major accident, and an emergency response plan has been developed to take these into account. The measures should be related, and preferably cross-referenced, to the MASs described elsewhere in the safety case.

2. The General Approach to Emergency Response Assessment

2.1 The main focus of the assessment is on the extent to which the safety case is able to show that an emergency response plan has been prepared that is proportionate to the possible MASs for the MHI concerned and for which the necessary measures have been taken to limit their consequences.

2.2 The MHIs shall develop scenario-specific emergency plans based on SCEs identified in the safety case and domino impacts from neighbouring MHIs to form part of Chapter 3.2.3.2 of the SCDF Emergency Response Plan template and include all relevant information outlined in chapter 6 of the Safety Case Technical Guide. MHIs can submit their scenario-specific emergency plans to MHD during their 1st safety case submission if available, otherwise, MHI shall submit latest by the 2nd safety case submission. While preparing these plans, MHIs are still required to submit their emergency response plans to NEA or SCDF annually as part of their licensing requirements.

Appendix H – 'Emergency Response Assessment Criteria and Guidance'

Technical Criterion	Guidance
Equipment and Systems Installed to Limit Consequence of Major Accidents	
9.1 The safety case shall describe the fixed equipment and systems installed on plant that limit or mitigate the consequences of major accidents and how these equipment or systems affect how an emergency is mitigated.	**To meet this criterion**, the safety case shall show basic information, which should include: a) the fixed equipment or systems available; b) a description of such equipment and systems; c) how these equipment or systems affect how a major accident is mitigated; d) list of relevant regulations, standards and codes of practices have been followed; and e) the manual intervention required.
Organisation, Arrangements and Provisions for the Alerting and Intervening in the Event of a Major Accident	
9.2 The safety case shall describe the organisation, arrangements and provisions for the alerting and intervening in the event of a major accident to provide evidence that the necessary control measures have been taken on-site.	**To meet this criterion**, the safety case shall show basic organisational information, which should include the functions of key posts and groups with duties in the emergency response. The following information on the organisation for alerting and intervening in the event of a major accident should be included: a) the arrangements for informing individuals on-site, neighbouring installations, where relevant: (i) to the nature of the alarms and the plant conditions required to activate them; and (ii) the initial actions required both on-site and off-site in response to alarm warnings. b) the arrangements and conditions for alerting and mobilising: (i) individuals or groups with defined responsibilities under the emergency response plans, including essential personnel on-site and off-site; (ii) the emergency services (e.g. SCDF); (iii) neighbouring installations, which may be affected by the off-site effects from the major accident or where mutual aid agreements exist; and (iv) external agencies. c) the arrangements for controlling and limiting the escalation of accidents on-site, including:

	(i) isolation of hazardous inventories and the removal of inventories where appropriate; (ii) use of fire-fighting and other mitigation measures; and (iii) prevention of domino effects. d) provision for monitoring of wind speed and direction and other environmental conditions, where applicable; e) a description of how communications will be established and maintained during the emergency response; f) the nature of, and arrangements for maintaining, any mutual aid agreements with nearby installations; g) the nature and location of any facilities which may require special protection and h) the nature and location of any facilities which require special rescue operation (e.g. confined space). i) the nature and location of: (i) emergency control centres and fire command centres – integrity maintained in the event of a major accident or, if not, a reserve facility available; (ii) medical and first aid points; (iii) in-place protection (IPP) facilities; (iv) sheltering buildings; (v) evacuation assembly areas; (vi) pre-defined control points, along with any identified secondary, back up locations; and (vii) any other relevant items. j) the location of access routes for emergency services, rescue routes, escape routes, and any restricted areas; k) occupancy load of occupied areas at peak and non-peak periods; l) the evacuation arrangements and any transport requirements, with considerations given to persons with disability; m) the headcount roll call and search and rescue arrangements; n) the communication means to signal occupants to initiate IPP. The roles of the coordinators and fire wardens to assist in setting up of IPP and the arrangements to isolate mechanical ventilation systems; o) the nature and location of any pollution control devices and materials; and

	p) consideration of the effects of emergency response actions, including fire-fighting activities, to minimise the overall impact on people and the environment. This should include short-term and long-term effects, and alternative options for disposal or discharge of released chemicals.
Description of Mobilisable Resources	
9.3.1 The safety case shall provide evidence that sufficient personnel can be made available within appropriate timescales to carry out the mitigation actions required by the emergency response plan.	**To meet this criterion**, the safety case shall confirm that the following factors have been taken into account: a) various functions which are required to implement the emergency response plan and supporting procedures have been identified; b) the number of personnel (including third parties) with appropriate skills and competencies required to implement the emergency response plan; c) staff required to implement the plan can be assembled in the required response time; d) mitigation actions are appropriate and achievable; e) how deputising arrangements for key roles have been assigned and how it can be assured that required staff are available; f) contingencies if the 'decision makers' such as key appointment holders are incapacitated; and g) information taken from analysis of the testing of plans which could show detailed assembly times and arrangements and how these relate to overall response times and the analysis of the general suitability of mitigation actions.

9.3.2 The safety case shall provide evidence that suitable and sufficient arrangements are in place to ensure that the equipment to be mobilised for mitigating the consequences of major accidents will be fit for purpose when called upon for use.	**To meet this criterion**, the safety case shall describe what provisions are in place to minimise the release or mitigate the consequences of major accidents. The following information shall be included: a) sufficient quantities of appropriately specified equipment can be made available within the required timescale, and the relevant containing action sustained for the necessary length of time; b) that the equipment can function effectively in all expected environmental conditions and if there is a loss of utilities or similar; c) emergency equipment is stored in an appropriate manner and location, it is accessible at all relevant times and it is suitably protected from the consequences of a major accident (e.g. fire); d) emergency equipment should be compatible, where necessary with that of SCDF (e.g. SCDF mobile water monitors, foam concentrate) and other organisations where mutual aid agreement exist; and e) electrical equipment used in emergency response should be suitably protected for the foreseeable environmental conditions during a major accident.
9.3.3 The safety case shall provide evidence that suitable and sufficient personal protective equipment (PPE) will be available in the event of a major accident.	**To fulfil this criterion**, the safety case shall include the suitability and accessibility of PPE such as breathing apparatus (BA) sets, respirators, chemical suits, personal detectors and other protective clothing have been described for the types of major accidents identified for both responders and other individuals not directly involved in dealing with the emergency response.
9.3.4 The safety case shall provide evidence that suitable and sufficient on-site firefighting and fire protection provisions can be mobilised in the event of a major accident.	**To fulfil this criterion**, the safety case shall include the following to demonstrate the MHI's ability to limit the consequences of a major accident, where applicable: a) MHIs should take account of resources available from other organisations with mutual aid agreements, where applicable; b) that the fire-fighting roles of CERT are complementary to the role of SCDF; c) that the quantity and specification of on–site fire-fighting equipment are sufficient; d) that the water requirements for fire-fighting and fire protection (e.g. cooling, have been predetermined, and that the capacity and reliability of the water supply are adequate, taking into account the various sources which may be available and the time required to establish back-up supplies);

	e) that suitable and sufficient portable and mobile fire-fighting equipment, such as mobile monitors, mobile pumps, portable extinguishers, foam generation equipment, hoses and hydrants, have been located at appropriate points throughout the installation according to the hazard; f) that suitable and sufficient stocks of foam compound are available when and where necessary; g) adequate consideration has been given in the design (e.g. the positioning of fire walls, to assist the positioning and protection of fire-fighting equipment and personnel, and that the reach of fire protection and extinguishing equipment are appropriate); h) adequate consideration (e.g. mitigation plans) has been given to flammable substances being carried by firewater and spreading the fire to other areas; and i) details of any potentially incompatible substances which may require additional mitigation measures in place to limit the consequences of a MAH.
9.3.5 The safety case shall show that suitable and sufficient provisions can be mobilised to minimise the release of, and mitigate the consequences of dangerous substances in the event of a major accident.	**To meet this criterion**, provisions to minimise the release and mitigate the consequences of major accidents related to toxic or flammable substances shall be included in the safety case: a) measures to reduce the evolution of toxic or flammable vapours from material that has already been spilled and to reduce the effects of its vapours (e.g. water curtains); b) equipment that will be used to terminate or reduce any leak at source (e.g. patching, plugging, valve closure and the isolation of sections of plant by blinding or blanking off); c) earth-moving equipment, sandbags, drain seals, pipe-blockers and absorbents for spillages on the ground and in drainage systems, as well as penstocks in drainage systems; d) floating booms for immiscible lighter-than-water products that have entered the water, including controlled waters, where applicable; and e) provisions for treating and removing spilled material (e.g. mobile pumps, special chemicals and other materials for neutralising or absorbing the spillage).
9.3.6 The safety case shall provide evidence that suitable and sufficient provisions for monitoring	**To meet this criterion**, the safety case shall show that suitable and sufficient provisions for monitoring and/or sampling, wherever necessary, which can be mobilised in the event of a major accident. Some examples of such information are:

	and/or sampling can be mobilised in the event of a major accident.	a) details of sampling and monitoring equipment; b) identify the purpose of the monitoring and sampling provisions and explain how the results might influence decisions concerning the emergency response; and c) any special technical expertise and other provisions required for analysing or interpreting the monitoring and/or sampling results.
9.3.7	**The safety case shall provide evidence that suitable and sufficient provisions have been made for the clean-up of the environment following a major accident.**	**<u>To meet this criterion</u>**, the safety case shall provide an outline of the provisions that are available for clean-up of the environment and which are suitable and sufficient for the MASs identified. The safety case should therefore outline what is available for use and who is trained to use it, such as: a) equipment to contain toxic substances; b) agents to soak up and/or neutralise contaminants; c) earth-moving equipment for the removal of contaminated soil and other material; d) booms and skimmers for spillages to water; and e) any temporary storage arrangements (e.g. portable storage tanks for the contaminated material). Other points to consider include the expected timescale over which any temporary containment may be required, the arrangements made to ensure that such facilities would not pose an unacceptable threat to health and the vicinity, and suitable disposal arrangements are made (e.g. engagement of toxic industrial waste collectors).

9.3.8 The safety case shall show that suitable and sufficient provisions have been made to mobilise first aid/medical treatment and decontamination functions during the emergency response.	**To meet this criterion**, the safety case shall show there are suitable and sufficient provisions made to mobilise first aid and medical treatment during the emergency response for the MASs identified in the safety case. For medical treatment, it is sufficient to describe the arrangements for providing first aid and/or transferring employees, such as those who have been exposed to toxic substances, to hospital as quickly as possible. In this part of the safety case, MHIs will need to show how the on-site first-aid provisions align with the provisions of emergency response plan. This can be achieved by: a) making reference to the number and availability of trained first aiders; b) describing the facilities available at the MHI; c) confirming both the expectations and limits of the first aiders training; and d) including relevant information any hazard-specific medical treatment that the MHI has catered for and describing the liaison with SCDF by making references to how the casualty control or decontamination strategies that have been determined.
9.3.9 The safety case shall show that suitable and sufficient provisions have been made to mobilise any ancillary equipment which may be required during the emergency response.	**To meet this criterion**, the safety case shall show that there are suitable and sufficient provisions to mobilise any ancillary equipment which may be required during the emergency response for the major accidents identified in the safety case. This could include equipment such as: a) fork lift; b) heavy lifting gear c) earth moving equipment; d) emergency lighting; and e) special tools and parts required to carry out emergency repairs and actions. If there is a reliance upon a third party to supply equipment or services, the safety case should describe the equipment needed and explain how this will be sourced, including estimated timescales for its arrival on-site.

Maintenance and Inspection of Emergency Response Equipment	
9.4 The safety case shall provide evidence that suitable arrangements have been made for the maintenance, inspection and testing of the mobilisable resources and other equipment to be used during the emergency response.	Maintenance activities should already be described elsewhere in the safety case, so a brief summary should meet the requirements of show that suitable arrangements have been made **to fulfil this criterion**. Typically, this would include: a) a description of arrangements used, for example: if using third party organizations, then details of the service level agreement in place should be provided (it is not necessary to include detailed arrangements in place with the emergency services); b) confirmation that suitable arrangements have been made for the maintenance, inspection and testing of emergency equipment for which the MHI has responsibility; and for equipment for which the MHI may rely upon but not have responsibility for; c) confirmation of the MHI's arrangements to ensure that the equipment is maintained in an efficient working order so that it would be available for use and provide the necessary function when called upon; d) details of type of equipment covered (e.g. fire-fighting equipment, breathing apparatus sets, personal monitors); and e) information on the scheduling of maintenance, inspection and testing activities on such equipment.
Training for Emergency Response	
9.5 The safety case shall provide evidence that suitable arrangements have been made in the SHMS for training of individuals on-site in the emergency response.	**To meet this criterion**, the safety case shall show that the safety and health management system has accounted for the need to train individuals in the emergency response and ensured that the training is kept up to date and refreshed. The training should be given to: a) employees with a specific role in the event of a major accident; b) information for other employees who may not have a specific role; and c) contractors and visitors to the site. Where applicable, the training shall include:

	a) information on the MASs and the emergency response procedures to take in the event of such accidents; b) specific training requirements for all staff; this may involve: (i) knowledge of the alarm systems and the required response to each alarm; (ii) procedures for reporting/responding to incidents on-site which have the potential to escalate into a major accident; (iii) the use of the resources which may be mobilised in the event of a major accident; (iv) use of protective equipment and any limitations on their use; (v) evacuation and mustering procedures; and c) actions required by staff with key roles in the implementation on the emergency response plans.
Testing of Emergency Response Plan	
9.6 The safety case shall provide evidence that procedures have been made and adopted to test and review emergency response plans, and to revise the emergency arrangements in the light of the lessons learned.	**<u>To meet this criterion</u>**, the safety case shall provide confidence that a suitable programme of emergency exercises has been drawn up. It should show that the programme has been implemented to test the emergency arrangements at all levels (i.e. the plant response and the site-wide response, and the interface with the external response by SCDF or third party emergency response teams). Confidence should be given that procedures exist to ensure that the lessons learned from these exercises are reviewed and the emergency arrangements are revised where necessary. Typical information included in a safety case to show these elements includes: a) Examples of frequency of live exercises, table-top exercises or tests, including information relating to which scenario or element of the plan to be tested (this should include both scenarios with on-site and with off-site impact); b) how tests or exercises are carried out to ensure that all personnel involved in the emergency response are included; c) approach on debrief and analysis activities relating to how the testing of the plan were carried out; and d) approach on how any lessons arising as a result of any debrief and analysis are effected into the review process.

Preparing the Emergency Response Plan	
9.7 Scenario-specific emergency plans shall be developed. These plans shall form part of Chapter 3.2.3.2 of the SCDF Emergency Response Plan template.	**To meet this criterion,** scenario-specific emergency plans based on SCEs identified in the safety case and domino impacts from neighbouring MHIs shall be developed. MHIs should include all relevant information outlined in Chapter 6 of the Safety Case Technical Guide. An example of a scenario-specific emergency plan is provided in Annex E1[2] of the SCDF Emergency Response Plan template.
Review of this Chapter and ERP	
9.8 MHIs shall review the contents of their emergency response plan to ensure they are current and relevant.	**To meet this criterion**, the MHIs shall review the contents of their emergency response plan annually.

[2] Annex E2 of the SCDF ERP template will be used for insertion of other premise-specific emergency plans (e.g. arson prevention plans) and standard operating procedures.

ANNEX E1

Scenario-Specific Emergency Plans

A MHI shall prepare a series of scenario-specific emergency plans that can be used by incident responders. They should cover, as a minimum, SCEs identified in the safety case and relevant off-site consequences from neighbouring MHIs encroaching into your premises (upon receipt of domino information).

The scenario-specific emergency plans should be:

- Site-specific and therefore relevant to the installation's systems and equipment;
- Fit-for-purpose;
- Easy to use; and
- Helpful to the end users.

Scenario specific emergency plans should preferably consist of only two pages. The first page is intended to provide guidance on the actions and resources required to deal with the incident during its first 20-30 minutes. Once this early stage has passed, a stable response should have been established. The scenario-specific emergency plans should combine operator and fire responder actions so that a coordinated approach is adopted for incident management. The plans may consist of a three-tiered response with:

1. First response by installation operators to verify incident and subsequent notification of SCDF, SPF and relevant parties;
2. Installation emergency responders (e.g. CERT or 3rd party fire brigades) as the second response; and
3. SCDF response and relevant parties as the third response.

On the reverse of the text page, a hazard effects map (based on existing QRA study or consequence contours developed for legacy sites) should be provided. This should indicate the potential toxic, overpressure, radiant heat hazard areas. In addition, nearby plant, tanks, vessels and associated equipment that could be affected by the incident should be indicated on the map. The hazard effects are produced from fire, toxic gas dispersion and explosion consequence-modelling programs. Hazard effects maps give an indication of the potential gas, fire or explosion area that may be involved during a major incident. They provide an appreciation of potential incidents for all responders.

An example of a scenario-specific emergency plan is provided in this Annex.

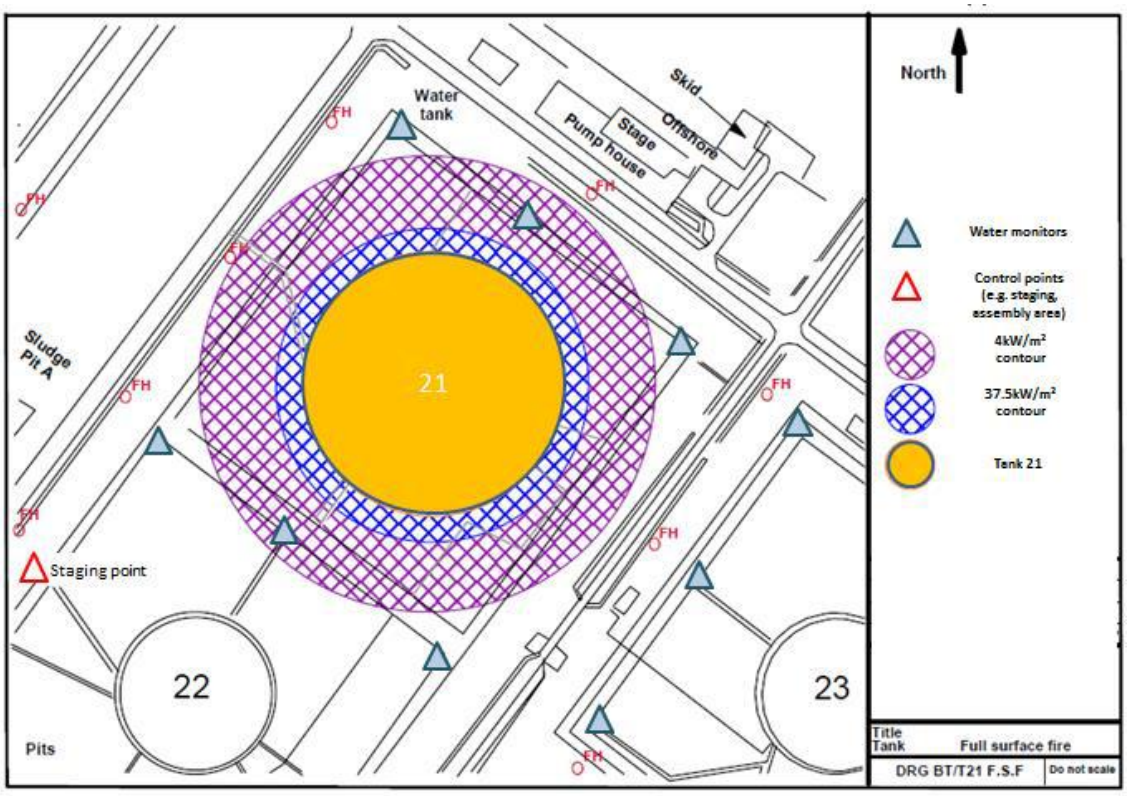
ANNEX E1

Example of Scenario-Specific Emergency Plans

Emergency plan for:		Description of the type of fire or emergency anticipated		
Strategy:		The major accident mitigation strategy which states the overall objectives to prevent escalation and bring the incident under control		
Immediately	**Actions**	**Equipment**	**Resources**	**Comments**
Usually control room or site personnel who will notify relevant authorities and companies, alert, shutdown and evacuate etc.	Logical step-by-step actions which are required according to the incident type and location. Typically, alarm, evacuation, isolation, shut down, informing etc.	What equipment are required to carry out the actions? Valves or devices to isolate.	Can be CERT, fire wardens, FSM etc.	As required.
1st response	**Actions**	**Equipment**	**Resources**	**Comments**
May be CERT and/or 3rd party fire brigade.	Sizing up of incident. Logical step-by-step actions necessary to isolate the fuel, or carry out initial incident control actions.	Fixed equipment systems installed on-site. Portable fire equipment for initial control. Any water or foam monitors required. Appropriate PPE etc.	Any foam concentrate required. The anticipated water demand for the incident. Fire hose/nozzles required. The number of hose will be based on the hydrant locations and fire vehicles used. The fire vehicles from CERT or 3rd party fire brigades.	As required.
2nd response	**Actions**	**Equipment**	**Resources**	**Comments**
Linking up with SCDF. Site personnel may be required to do other tasks at this stage.	Logical step-by-step actions necessary to control and mitigate the incident.	Fixed equipment systems installed on-site. Any water /foam monitors required.	Resources available to assist SCDF operations: e.g. foam concentrate and water supply	Foam applied at pertinent application rate etc.
Ongoing potential hazards Any known hazards that will be present because of the anticipated fire either from flame impingement or radiated or conducted heat. Also consider any explosion possibility.				
Other issues Any other issues, e.g. personnel safety, gas releases, public exposure.				

ANNEX E1

Example of Hazard Effects Map for Scenario-Specific Emergency Plans



Chapter 10: Assessment of ALARP in Safety Case

1. Introduction

1.1. This guide is for MHD assessors completing the ALARP aspects of the assessment.

1.2. This is linked to **Chapter 7** of the Safety Case Technical Guide.

1.3. All ALARP assessments must use the criteria and guidance set out in **Appendix I – 'ALARP Assessment Criteria and Guidance'.**

2. The General Approach to ALARP Assessment

2.1. ALARP demonstration for a SCE can be satisfied by MHIs by answering the following fundamental questions in relation to the identified SCEs:

a) What more can MHIs do to reduce the risks?

The answer to this question is **qualitative** in nature. MHIs should look systematically at each SCE and draw up, in a proportionate way, a list of control measures that have been implemented and which could be implemented to further reduce the risks of SCE. For few SCEs there will be nothing further that MHIs can do except shutting the plant down completely, for other SCEs there may be further risk reduction measures that can be possibly implemented. Having answered this question, the need to act is determined by answering the second question below in 2.1(b).

b) What further risk reduction measures are "reasonably practicable"?

The answer to this question may be **qualitative** or **quantitative** in nature. Whichever way the question is answered, if the control measure is "reasonably practicable", based on sound logical considerations, then MHIs are duty bound to implement that measure.

2.2. The MHD policy is that taking all necessary control measures (i.e. all "reasonably practicable" control measures) equate to reducing risks to ALARP.

2.3. In particular, the MHD needs to assess the analysis of possible further risk reduction measures. The information needed to determine if the necessary measures for risk reduction have been implemented must be either available or referenced and summarised, where appropriate in the safety case.

Appendix I – 'ALARP Assessment Criteria and Guidance'

Technical Criterion	Guidance
Risk Assessment and Risk Reduction Measures	
10.1 The safety case shall clearly describe how MHIs use risk assessment to help make decisions about the measures necessary to prevent major accidents or to mitigate their consequences.	This criterion is effectively a summary of the Predictive (Chapter 4), Technical (Chapters 5 to 8) and ALARP criteria (Chapter 10). The MHD would come back to this criterion when the criteria above has been addressed. **<u>To meet this criterion</u>,** the safety case shall pull together the information from the risk assessment such that it: a) draws together the likelihood and consequence assessments in an appropriate way to make estimates of the risks; b) identifies SCEs; c) recognises that high consequences events warrant attention for further risk reduction on a case by case basis; d) considers on-site risks and off-site risks; e) compares the risks against suitable MHIs' criteria and takes account of aversion to large scale MASs where necessary, in the selection of necessary control measures; f) considers sensitivity and uncertainty in the risk assessment; g) shows that risk assessment has been used in an appropriate way as part of the process to reduce risks on the installation to ALARP; h) includes a suitable and sufficient consideration of risk reduction options and describes the decision making process; i) comes to conclusion about what further risk reduction measures are reasonably practicable; j) demonstrate that the adopted control measures for any identified SCEs collectively eliminate or reduce the risk to health and safety to ALARP levels; and k) puts in place a programme for implementing further risk reduction measures with timescale.

Demonstration of ALARP	
10.2 The safety case shall show the approaches or methodologies used to support the MHIs' evidences and justifications for ALARP demonstration.	**To meet this criterion**, the safety case shall: a) describe the decision making process for control measures adopted and further risk reduction measures rejected for each SCE; b) define the underlying rationale, criteria and decision-making basis for ALARP demonstration; c) demonstrate that decisions on the requirement for additional risk reduction measures to bring down levels to ALARP are made by appropriately qualified and experienced technical personnel; d) demonstrate that decision making by MHIs is precautionary when the degree of uncertainty is larger, or the consequences of the SCE give rise to significant off-site risks. A precautionary approach means that there is a bias towards safety. The description must be convincing. This means that the rationale for deciding the completeness of the MAH and scenario identification and the adequacy of the control measures employed shall be supported and accompanied by all assumptions made and conclusions drawn. Where appropriate, MHIs shall present or summarise the results of supporting studies that have been performed. The description shall also demonstrate that the process was systematic which means that it followed a fixed and pre-established scope. Finally, the degree of analysis in support of the ALARP demonstration shall be proportionate to the risk and to the complexity of the MHI, hazards and the control measures.
10.3.1 Fundamental consideration for ALARP demonstration (part 1): ***What more can MHIs do to reduce the risks from SCEs?***	**To meet this criterion**, the safety case shall: a) include a systematic review of control measures applicable to all SCEs; b) draw-up in a qualitative and proportionate way, a list of control measures that have been implemented for each SCE. As a minimum the list should include all relevant good practices and sound engineering principles; c) draw-up in a qualitative and proportionate way, a list of control measures that could be **practicably** implemented to reduce risks from SCEs further. Suggestions for further risk reduction measures include:

	(i) relevant good practices or sound engineering principles not implemented; (ii) an option adopted elsewhere in similar circumstances; and (iii) any other option that has worked in practice. Where further risk reduction measures include automation (e.g. to remove human contribution to failure), the automation should be well-justified, well designed, and selected for the right reasons. Where relevant, MHD officers should note that training and procedures should not be viewed as the sole defence against human failure; they should form an integral part of a broader range of measures to reduce the potential for human failure.
10.3.2 Fundamental consideration for ALARP demonstration (part 2): ***What further risk reduction measures are "reasonable practicable"?***	**<u>To meet this criterion</u>**, the safety case shall: a) include for each control measure identified for further risk reduction that could practicably implemented, an assessment of: (i) the sacrifice, in money, time and effort, required to implement the control measure; and (ii) the foreseen benefits, in harm avoided, from implementing the control measure; b) include a comparison of the sacrifice and benefits, and a conclusion whether the sacrifice is grossly disproportionate to the benefits based on MHI's criteria. Review of MHI's ALARP criteria is an important aspect of the ALARP assessment. MHD shall look for the safety case to demonstrate the following when MHIs are using qualitative and/or quantitative argument during ALARP demonstration: **<u>Qualitative Argument</u>** a) describe the argumentation that focuses on relevant good practices and sound engineering principles. Several sources of good practice and engineering principles exist which are in order of precedence: (i) prescriptive legislation; (ii) regulatory guidance;

	(iii) standards produced by standard-making organisations; (iv) guidance agreed by an organisation representing a particular sector of industry; and (v) standard good practice adopted by a particular sector of industry. b) demonstrate, if good practice and sound engineering principles are used as the sole justification of ALARP, that: (i) good practice and sound engineering principles are relevant to the SCEs; (ii) adopted standards are up-to-date and relevant; (iii) where a standard allows for more than one option for conformity, the chosen option makes the risks ALARP; and (iv) good practice and sound engineering principles reduce the risk to an acceptable level. c) If ALARP cannot be demonstrated by good practice and sound engineering principles, the safety case shall demonstrate for further risk reduction measures: (i) that measures which are reasonable and practicable reduce the risk to an acceptable level; and (ii) the measures which are reasonable and practicable are implemented, or are included in the MHI's improvement or risk reduction plan. **<u>Quantitative Argument</u>** a) present **quantitative arguments** such as Cost Benefit Analysis (CBA) if applying qualitative argumentation is not sufficient to demonstrate ALARP.