SAFETY CASE TECHNICAL GUIDE

Jointly developed by

MINISTRY OF MANPOWER

National Environment Agency
Safeguard • Nurture • Cherish

SCDF
The Life Saving Force

SCIC
SINGAPORE CHEMICAL INDUSTRY COUNCIL

Updated: Oct 2016

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AEGL = Acute Exposure Guideline Levels

ALARP = As Low As Reasonably Practicable

CBA = Cost Benefit Analysis

CERT = Company Emergency Response Team

ERPG = Emergency Response Planning Guidelines

HAZOP = Hazard and Operability Study

IDLH = Immediately Dangerous to Life or Health

IPP = In-Place Protection

LC50 = Lethal Concentration 50

LD50 = Lethal Dose 50

MAH = Major Accident Hazard

MAPP = Major Accident Prevention Policy

MAS = Major Accident Scenario

MHD = Major Hazards Department

MHI = Major Hazard Installation

MOC = Management of Change

MOM = Ministry of Manpower

NEA = National Environment Agency

PEL = Permissible Exposure Level

PPE = Personal Protective Equipment

PTW = Permit-to-Work

PUB = Public Utilities Board

QRA = Quantitative Risk Assessment

SCDF = Singapore Civil Defence Force

SCE = Safety Critical Event

SDS = Safety Data Sheet

SHE = Safety, Health and Environment

SHMS = Safety and Health Management System

SI = International System of Units

SIF = Safety Instrumented Function

SLA = Singapore Land Authority

UK HSE = United Kingdom Health and Safety Executive

WSH = Workplace Safety and Health

Chapter 1: Safety Cases – Purpose and Key Concepts

1.1 Overview

1 Major Hazard Installations (MHIs) are presently required to comply with safety, health and environment (SHE) requirements under the Workplace Safety and Health (WSH) Act, Environmental Protection and Management Act (EPMA) and Fire Safety Act (FSA) administered by the Ministry of Manpower (MOM), the National Environment Agency (NEA) and the Singapore Civil Defence Force (SCDF) respectively. This includes, but not limited to, the following:

a) Quantitative Risk Assessment (QRA)
b) Process Hazard Analysis (PHA)
c) Safety and Health Management System (SHMS)
d) Emergency Response Plan (ERP)

2 To enhance process safety and regulatory oversight of MHIs, Singapore has embarked on implementation of Safety Case regime. Such regime has been implemented in the European Union and Australia. The regime requires MHIs to demonstrate to regulators how risks from Safety Critical Events (SCEs) are being reduced to As Low As Reasonably Practicable (ALARP) and thereby ensuring safe operations in a sustainable manner.

3 This safety case regime is targeted at installations which are defined as MHIs under the WSH (MHI) Regulations and are required to produce a safety case document for assessment.

4 This Safety Case Technical Guide describes how a safety case shall be structured and presented by MHIs to the Major Hazards Department (MHD)[1] to meet the WSH (MHI) Regulations.

1.2 Purpose of a Safety Case

5 A safety case is a written presentation of the hazards and risks that may lead to a major accident at an MHI and the technical, management and operational measures in place to control those hazards and risks.

6 A safety case is commonly presented using, and communicated through a structured set of documentation that focuses on preventing major accidents at the installations, and limiting their consequences to people and the vicinity.

[1] MHD comprising MOM, NEA and SCDF officers was formed as a single regulatory front for MHI-SHE matters including safety case assessments, inspections and incident investigations.

7 MHIs shall, through the information provided in the safety case, showcase that MHIs have control measures in place to prevent major accidents or limit their consequences. It can only be successful in this aim if MHIs have systematically examined their site activities, assessed the potential for major accidents and listed what MHIs have done or are going to do to prevent major accidents.

8 MHIs have to demonstrate that a systematic process is in place to identify and implement safety measures on-site. The value in writing a safety case is that it shows MHIs have assessed their safety measures and how organisational, technical and human factors contribute to safety in their installations. It also shows that MHIs have arrangements in place to rectify any shortcomings identified.

9 Therefore, through the preparation of the safety case, MHIs demonstrate how they meet the fundamental obligations under the WSH (MHI) Regulations – the prevention and limitation of major accidents.

1.3 Definitions

a) **Change** – a planned action or intervention that adds, removes or modifies an existing process, system or equipment on permanent or temporary basis.

b) **Containment System** – a system designed to prevent the accidental release of materials.

(i) **Primary Containment System**: process or storage related equipment or system (e.g. storage tanks, vessels, piping).

(ii) **Secondary Containment Systems**: containment system which hold the loss of containment material from primary containment (e.g. bund walls, drain systems).

c) **Control Measure** – means of preventing a hazard from escalating to an incident or mitigating the consequences of incident. It can be a design feature, an action of equipment or a human intervention. Control measures can be broadly categorised into:

(i) **Preventive Measures**: measures that are put in place to prevent the release of dangerous substance or loss of containment.

(ii) **Mitigative Measures**: measures that are put in place to mitigate or limit the harm caused to people and the vicinity.

(iii) **Risk Reduction Measures:** control measures which includes both preventive and mitigative measures.

d) **Controlled Water** – refers to any water bodies which include rivers, streams, estuaries, canals, lakes, ponds, ditches and groundwater sources which may be used as source of drinking water.

e) **Competent Person (CP)** – a person who has sufficient knowledge, skills and experience, to perform the work required to be carried out as required by the safety case regime. A CP can be:

(i) A Professional Engineer (PE), as conferred by the PE Board in Singapore, in the Mechanical, Civil, Electrical and Chemical disciplines;
(ii) A Chartered Engineer or equivalent, acceptable to the Commissioner for WSH; or
(iii) A suitable person, as justified by the MHI, possessing the required knowledge, skills and experience for the appointed role in the safety case.

f) **Environment** – consists of all or any of the following media, namely, air, water and land.

g) **Equipment** – any apparatus, instruments or items needed for a particular purpose in a facility

h) **Equipment of High Safety Concern** – an equipment is safety critical if either its failure could cause or contribute substantially to a major accident, or its purpose is to prevent, or substantially limit the effect of, a major accident.

i) **Facilities** – all technical features, whether at or below ground level, in which substances are produced, used, handled or stored. It includes all the equipment, structures, pipelines, pipework, machinery, private railway sidings, docks, unloading quays serving the MHI, jetties, warehouses or similar infrastructures, floating or otherwise, necessary for the operation of the MHI.

j) **Initiating Event** – event that can escalate and lead to the realisation of an accident.

k) **Major Accident** – refer to the WSH (MHI) Regulations.

l) **MHI Boundary Limit** – the maximum physical geographical extent or compound that is occupied and/or controlled by MHI.

m) **Necessary Measure** – measure that is considered to be reasonably practicable and should be implemented.

n) **Risk** – the likelihood of a specified level of harm occurring within a specified period.

o) **Safety Critical** – any equipment, control system, task, activity or utility which failure could cause or contribute substantially to a major accident, or its purpose is to prevent, or substantially limit the effect of, a major accident.

p) **Safety Critical Event (SCE)** – a subset of MAS that require ALARP demonstration, further details on SCE are provided in Chapter 4 of this technical guide.

q) **Scenario** – a sequence or development of events including an initiating event, cascading events and final outcomes (consequences).

r) **Sensitive Receptor** – refer to the Revised QRA Guidelines.

s) **Structures** – those elements needed to support and access equipment, e.g. civil foundations, control rooms, vessel skirts, pipe racks and pipe supports, platforms, access stairs, buildings or barriers designed to withstand the effects of accidental explosions.

t) **Vicinity** – the area surrounding the installation.

u) **Worst Case Scenario** – the outcomes which give the largest injury hazard distances for toxic release, fire and/or explosion.

1.4 Concept of 'Demonstration'

10 The understanding of the meaning of '**demonstration**' is essential to understanding the purposes of a safety case. To make a 'demonstration' means to **justify** the case through the information given. MHIs shall use measures that are established, appropriate and meaningful to their operating philosophies, safety culture and best practices.

11 The WSH (MHI) Regulations applies to a wide range of installations, differing in size, number of employees, complexity, resources and expertise, technology, culture and the vicinities. All sites have one thing in common: the potential for a major accident, albeit covering different hazards. Therefore, the safety case for a small chemical plant and a major oil refinery shall both make demonstrations to reduce risk of major accidents to ALARP.

12 The amount of information that MHIs have to provide for demonstrations depend on a number of factors:

a) the size and complexity of the installation, for example, usually more effort is required to describe an oil refinery than a tank farm;
b) the potential to cause harm, for example the MHI of a storage terminal storing many different chemicals may need to supply more information about potential consequences than the MHI of an LPG storage facility. Both would still have to describe the worst case scenario and a range of major accident scenarios (MAS) relating to the classes of chemicals stored as well as giving a description of the likelihood of the events;
c) the extent of process hazard analysis and risk assessment carried out shall commensurate to the major accident hazards (MAHs) of the installations;
d) the extent to which safety is demonstrated using the following approaches:
    (i) Regulatory guidance (e.g. MOM, NEA, SCDF) – this could be issued jointly or separately by the relevant agency (e.g. Revised QRA Guidelines);
    (ii) Singapore standards, international standards or such other standards, codes or guidance as is issued or approved by MOM, NEA or SCDF – the scope of the standards or code of practice and its limitations have to be understood and related to the risks from the MAHs;
    (iii) Internal company standards – full description of the underlying rationale and any deviation from published standards shall be justified;

(iv) Manufacturers' standards or advice– this requires a full justification of the underlying rationale, including where they deviate from published standards;

(v) Technical expert advice (e.g. consultants, chartered engineer, professional engineer in the various fields like chemical, mechanical, civil, electrical) – this can be a good source of information for demonstrating and justifying measures, particularly through risk assessment. However, the justification needs to be based on real on-site conditions, where possible;

(vi) Experience in relevant field – individual's personal experience or MHI's experience may offer important evidence on specific issues.

Appendix 1 provides some examples to illustrate how the amount of information provided and the depth of demonstration varies depending on the situation in different installations.

13 MHD will take the information and conclusions in the safety case largely as presented and presume they are factual, unless it has information to the contrary. MHD will assess the credibility and logic of the conclusions reached in the safety case and may ask to see documentations to prove the MHI's claims, particularly as part of a safety case inspection programme based on the information in the safety case.

14 **Making a demonstration does not necessarily mean 'proving beyond reasonable doubt' or 'providing an absolute proof'**. For instance, for a vessel manufactured to a particular international design standard, it is sufficient to quote the standard and explain why it is appropriate for the vessel concerned (e.g. by comparing key design parameters, such as pressure and temperature limits, with the scope of the standard) in the safety case. There is no requirement to include copies of certificates which prove that it is built to that standard. Where commonly found standards are referred to for a number of vessels, then a general comment outlining their general application is sufficient.

15 In situations where MHIs have not made conventional use of a standard in some part of the design but have adopted some other approach which is considered appropriate, MHIs shall then explain the reason of such approach. If MHIs have been consistently using a particular standard in a certain aspect of the installation such as in the design of pressure relief but has now decided to adopt a different standard, MHIs shall explain the reason and highlight any implications on safety, health or vicinity.

16 The safety case shall justify the use of a standard which is out of date or withdrawn, particularly if the safety case relates to the design of new plant. The MHI may have an installation, which complies with out-of-date standards, or even incomplete records for justifying design decisions. In these cases, the MHI shall show that the design is fit for purpose. However, the MHI shall also show that additional arrangements have been established, where appropriate, to prevent or limit a major accident, such as more frequent inspection and testing of plant equipment and systems, or more reliance on operator control. These arrangements should be described, including in case of operator controls, whether there has been increased emphasis on training and monitoring of performance.

17 To make the series of demonstrations as required by the WSH (MHI) Regulations, MHI shall ensure that the safety case:

a) shows that the identification and analysis of hazards is sufficiently rigorous, systematic and proportionate to the risk of the installation;
b) shows that an on-site emergency plan is in place, based on sound principles and reflecting the MAS identified;
c) shows how all necessary measures have been identified and linked to specified MAHs, and implemented to reduce risks to ALARP; and
d) justifies why identified control measures are not implemented by argument under ALARP principles. 'Argument' can be made using qualitative or quantitative statements appropriate to the level of risk. The definition and concept of ALARP will be further explained in Chapter 7 of the guide.

1.5 Writing the Safety Case

18 MHIs should follow these steps when preparing the safety case:

a) gather information;
b) analyse the information to make the demonstrations;
c) act on the information if the analysis shows that additional control measures are needed; and
d) present the information in a structured way to make the demonstrations clear.

1.5.1 Gathering information

19 There are four categories of information required in the safety case:

a) a description of the installation including the dangerous substances on-site and the nature of the vicinity (Chapter 2);
b) information about the MAPP and SHMS (Chapter 3);
c) detailed information about the installations, particularly about MAS and the technical measures to ensure safety and protect the vicinity (Chapter 4 and 5) and ALARP demonstration (Chapter 7);
d) information about the emergency response plans (Chapter 6)

20 The following information may be required during the preparation of the safety case. This information should be gathered before and during the writing of the safety case and MHIs shall ensure that the information used is up-to-date, accurate and reliable to facilitate future revisions of the safety case.

a) quantity of dangerous substances present or likely to be present in MHIs;

b) safety studies such as PHA (e.g. hazard and operability study), QRA, fire safety studies, risk assessments, likelihood analysis, safety integrity level (SIL) or safety instrumented function (SIF) studies, hazardous area zoning studies, safety and feasibility studies, mechanical integrity studies, process equipment layout studies;

c) past accidents and near-miss reports from the installation, organisation, industry or global sources;

d) information pertaining to the hazards of chemicals used or produced by the process. This information could include (but not limited to):

   (i) safety data sheets (SDS) or the below information if not included in the SDS:
   (ii) toxicity information;
   (iii) permissible exposure limits;
   (iv) physical, corrosivity and reactivity data;
   (v) thermal and chemical stability data; and
   (vi) chemical incompatibility data.

e) information pertaining to the technology of the process. This information could include (but not limited to):

   (i) block flow diagram or simplified process flow diagram;
   (ii) process chemistry;
   (iii) maximum intended inventory;
   (iv) safe upper and lower limits for identified critical operating parameters such as temperature, pressure, flow and composition;
   (v) design safety philosophy and designed operating conditions;
   (vi) existing operating philosophies and control strategies; and
   (vii) safety and health related consequences of deviation.

f) information pertaining to the equipment, hardware and facility used in the process. This information could include (but not limited to):

   (i) safety instrumented systems (e.g. interlocks, detection or suppression systems);
   (ii) materials of construction;
   (iii) maps or diagrams showing layout;
   (iv) piping and instrumentation diagrams;
   (v) relief system design and basis; and
   (vi) ventilation system design.

g) any design codes and standards (Singapore, international, corporate) relevant to the operations at the installation;

h) description of additional processes or activities undertaken in the installation;

i) surrounding population demographics and density;

j) assessment of current plant condition (e.g. integrity, reliability, equipment maintenance history); and

k) equipment reliability and failure rate data.

21 **For new or major modification projects, MHD may require detailed information on the suitability of certain materials to be furnished before actual submission of the safety case. MHD will inform and discuss with respective MHIs during QRA pre-consultation for the submission of these information. For existing MHIs, material suitability may be verified during on-site verification.**

22 Personnel with a range of knowledge, skills and work experiences in the design intent, hardware, systems and materials should be involved in the safety case development.

23 Existing MHIs should be able to use the factual information from their existing studies, wherever available. MHIs shall not submit these to MHD without reviewing them. It is important that MHIs are sure that the information is sufficient for the demonstrations required and that the arguments used are presented in a clear and logical way when making those demonstrations.

1.5.2 Analysing information to make the demonstrations

24 It is essentially, that the demonstrations link information about:

a) ‘what can go wrong’ to ‘what measures the MHI has taken to prevent it from going wrong’ and
b) whether measures described are justified by showing a sufficiently systematic and rigorous process for making the decisions on whether the measures taken are sufficient.

25 Regulatory guidance, local standards (e.g. Singapore Standard), international standards (e.g. API, ASME, IEC) and codes are all benchmarks for good practices, i.e. what is appropriate. If current measures on-site are evaluated to be inadequate or insufficient through risk analyses, then action shall be taken or planned to improve them. MHIs shall evaluate their current situation, and decide if it is reasonably practicable to improve their systems.

1.5.3 Acting on information if the analysis shows that further improvements are required

26 MHIs need to act if some information is not available or gaps are identified after analysis. For example, if the MHI does not have an up-to-date hazardous area classification drawing, the MHI should include this into their MHI overall action plan to have the drawing updated.

1.5.4 Presenting information in a structured way to make the demonstrations clear

27 MHIs shall refer to the minimum information required under the WSH (MHI) Regulations as the basis for deciding the necessary information. This guide describes how a safety case shall be presented and structured.

28 Sufficient information shall be provided in the safety case to allow assessors to understand why MHIs are doing things in a particular way. Other documents may be referred to if necessary. MHD may request for more information during the assessment, but MHIs are advised not to be too brief that the arguments cannot be understood without intimate knowledge of the documents referenced.

29 The presentation should be logical. MHIs should keep in mind that MHD is looking for demonstrations to be made, and for clear links to the WSH (MHI) Regulations requirements. In presenting the safety case, MHIs should move from an overview and progress to detailed descriptions. MHIs should describe things and then present the analysis and demonstration.

30 MHIs are not required to provide extensive detail when it is possible to refer to other reports or studies already prepared. However, the safety case should present a sufficiently self-contained demonstration to facilitate the assessment process. Reference documents are a useful way of supporting arguments but are not a substitute for the demonstrations required in the safety case.

31 Where documents are cross-referred to support the statements in the safety case, MHIs should include a summary of the contributions made by the reference documents in the demonstration, and be prepared to provide copies on request.

32 Further information which includes sensitive proprietary documentation may be requested during the assessment process. MHIs may wish to have the material returned after MHD has finished with it. Information that does not form part of the safety case may also be requested during the assessment process.

33 MHIs shall include in the safety case a MHI overall action plan that is intended to be followed-up as a result of gaps identified during development of safety case.

34 To make the safety case easy to follow and refer to, the following is recommended:

a) All information in the safety case and any supporting documents should be legible. In particular, font sizes should be large enough, and diagrams and plans should be at an appropriate scale and of high enough resolution for details to be readable;

b) The use of table of contents, chapters, sections, numbering and appendices will help with text flow and allow for cross-referencing.

c) MHIs should use simple English and explanatory diagrams to aid in the description. All abbreviations and acronyms used in the safety case should also be explained clearly;

d) Each page should include in the header or footer sufficient information to identify the MHI to which it applies, preferably the company or other name, and the workplace number assigned by MHD;

e) Each page should include in the header or footer sufficient information to identify the document of which if forms part, including the date and/or version number, section number and page number (in the form 'page X of Y') and

f) The cover page should list the name and address of the MHI, the workplace number assigned by MHD, the name, designation and contact details for the person MHD should contact if details in the safety case require clarification, and the date of preparation and/or version number of the safety case.

g) MHI should write the safety case in the format that is most suitable for their needs. However, to aid MHI and MHD in assessing whether the safety case covered the necessary information for assessment, MHI should tabulate how the section of the safety case aligns to the individual assessment criteria under the Safety Case Assessment Guide.

1.6 References

35 The following documents may be referred while reading this technical guide:

a) WSH (MHI) Regulations;
b) Safety Case Assessment Guide;
c) Guide to WSH (MHI) Regulations;
d) Revised QRA Guidelines.

Appendix 1: Examples on Level of Demonstration

Example 1

36 A majority of MHIs run well-known and straightforward manufacturing processes or storage facilities. This means these MHIs can rely heavily on published standards or guidance to justify the measures they use, as long as they show they understand the limits of application of those standards or guidance.

37 An example would be an MHI running a small tank farm. The Singapore Standard Code of Practice for the Storage of Flammable Liquids (SS532) and the SCDF's Fire Safety Guidelines for Open Plant Structures in Oil, Chemical and Process Industries provide useful information on what is good industry practice. Such standard or guidance can be used in support of the demonstration. If the separation and spacing table from the SCDF fire safety guidelines is used, then the purpose, applicability, and limitations should be understood where possible.

Example 2

38 Sites with large numbers of employees and complex installations are likely to have more detailed management structures. A description of these structures with the relevant roles and responsibilities and, for example, the demonstration of good communication between those with responsibilities, plays a very important part in this type of safety case.

39 The risk assessment demonstrations will be more complicated than in Example 1. For straightforward processes included in the large site's activities, the use of published guidance and standards for demonstrations can be the same as for Example 1 in many cases. If processes are complex or unusual, then more information should be included, explaining how the MHI has selected appropriate measures for the MAS. The contribution of these measures to the overall risk control also needs to be explained.

Example 3

40 A safety case may describe a flammable gases vent system linked to a flare stack which is common to a number of vessels throughout the installation. This is a critical item of plant for ensuring containment and the safety case will need to describe its design parameters such as its flare size and capacity, flame stability, flashback protection and others. The safety case should describe how the system is designed to prevent deflagration and detonation spreading to other plants and installations, for example by the use of flame arrestors, and describe what the chances are of loss of containment and major accident. The safety case should mention that the MHI has identified an appropriate flame arrestor for all the different types of flammable gas that are likely to be present.

41 In these circumstances, there is no need to include details of the make and model of the flame arrestor or include manufacturers' catalogues with detailed specifications. The information provided will show sufficient description as to why the design is adequate. Further investigation or verification might be carried out by MHD as part of any subsequent inspection, to check the adequacy of the design and the management systems relating to construction, operation and maintenance.

Example 4

42 A safety case describes the scrubbing system for vessels handling very toxic chemicals, which could cause harm to the vicinity if released. As this is a critical measure for preventing loss of containment, the safety case should describe its design parameters such as the selection of scrubbing medium, control arrangements, and provision of back-up systems. The safety case should describe the filling and emptying operations, and the systems to prevent a major accidental release including procedures and design such as the use and location of isolation valves.

43 The safety case should also describe the bunding arrangements to limit the loss of containment for tanks with very toxic chemicals. The design parameters are described in the safety case. MHD may then carry out a more detailed examination of these features as part of its inspection programme.

Chapter 2: Descriptive Information of MHI

2.1 Introduction

44 This chapter outlines the descriptive information in the safety case to satisfy the minimum information to be included in the safety case as required by the WSH (MHI) Regulations.

2.2 Overview of MHI

2.2.1 Information on MHI, its activities and products

45 General information of MHI shall include, where applicable:

a) the name, workplace number[2] and address of the MHI;
b) the mailing address of MHI (if different from the address in (a));
c) details of whether the MHI is part of a larger group of companies, and other subsidiary offices 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 organisations involved in preparing the safety case and their area of contribution.

46 An overview of the installation, its activities, processes and products shall be described in the safety case. An overview is a general outline, without extensive detail, to set the context for the reader. The overview shall include:

a) purpose of 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 MAS;
e) historical development of activities and production;
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.

[2] A workplace number consists of the Unique Entity Number (UEN) followed by four digits e.g. 0001 after the UEN. An example of a workplace number is 19682233N0001

47 The layout of the installation shall be clearly presented on adequately scaled plan (i.e. usually at least 1: 10 000) plus description where applicable and this 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 MAS;
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 systems 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 buildings such as control rooms, offices, workshops and canteens that could be vulnerable in a major accident (with an indication of the numbers of persons likely to be present during peak and non-peak hours).

2.2.2 Information on dangerous substances

48 MHIs shall identify and tabulate a list of all **dangerous substances** and their respective maximum quantities present or likely to be present[3] in the installations as per the WSH (MHI) Regulations.

49 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 substances 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 other) and properties (e.g. P1, P2, H2);
e) proportion of each constituent in a mixture, where applicable; and
f) SDSs of respective dangerous substances identified. The SDS should, where relevant, contain information on the physical, chemical and toxicological characteristics such as:
    (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;

[3] 'Likely to be present' – inventory variations which may occur because of seasonal demand, fluctuations in business activity, etc, or dangerous substances which may be present sometimes but not at other times. It also includes dangerous substances which may be generated during the loss of control of an industrial chemical process.

(viii) miscibility;
(ix) partition coefficient;
(x) rates of decomposition;
(xi) data on sensitiveness of explosives and the behaviour of explosives on accidental initiation; and
(xii) appropriate data on toxicology.

50 Relevant physical and chemical data shall be presented in a clear and concise form using appropriate and consistent units of measurement, preferably following the SI system (e.g. in kilograms, metres).

51 For the dangerous substances identified, MHIs shall indicate the hazards, both immediate and delayed, for human health on-site and off-sites. 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 hazards such as irritation, asphyxiation, cancer or mutagenic damage;
b) toxicity data (e.g. PEL, LC50, LD50, IDLH, AEGL-3, ERPG-2);
c) harm caused by fire or explosion; and
d) effects on the vicinities (e.g. building damages or impacts on sensitive receptors)

52 Appropriate references shall be provided for recognised acceptable limits, in terms of concentration, distance from source, exposure time and other relevant parameters. If there is little knowledge of the effects, appropriate references shall also be provided to justify the harmful effects, hazardous concentrations and acceptable limits presented in the safety case. 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.

53 MHIs shall attach relevant current licences issued by NEA (hazardous substance licence) and SCDF (petroleum & flammable materials storage licence) in the safety case.

2.2.3 Information of the vicinity

54 A description of the installation's vicinities shall be provided. The extent of the area described shall take into account the hazard ranges of the representative MAS presented later in the safety case. A map of a suitable resolution should be used when describing the vicinities (outside the MHI's boundary limit).

a) On the map, MHIs should clearly indicate, where applicable:
   (i) sensitive receptors (e.g. schools, hospitals, residential areas or worker dormitories); and
   (ii) access routes and escape routes from the installation and other traffic routes significant for rescue or emergency operations.

b) Details of the installation's vicinity that may influence the impact of a major accident such as:
   (i) the surrounding water courses including controlled water (if any), and any water catchment area[4] in relation to the dispersion of liquid contaminants;
   (ii) sewage and rainwater systems, if they could be involved in the dispersal of liquid contaminants offsite;
   (iii) features of the vicinity that may hinder emergency response or containment measures.

c) Details of external factors which may lead to or exacerbate major accidents such as:
   (i) the topography, if it could have an effect on the dispersion of toxic or flammable gases or combustion products. This should include buildings, underground workings or other infrastructures where appropriate;
   (ii) local weather records, including wind speed, wind direction and atmospheric stability (refer to the Revised QRA guidelines for more information on this) and the relevance of this information to the behaviour of releases of dangerous substances;
   (iii) 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 (contributing to stress and strain on piping and equipment);
   (iv) the historical evidence of other external events that might cause accidents such as flooding, extreme weather conditions including temperature, rain, wind and lightning; and
   (v) transport activities that may have an impact, including shipping, major transport routes and dangerous substance movements.

d) Description of structures 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.

e) Description of protected parts of the vicinities such as:
   (i) nature reserves;
   (ii) reservoirs; and
   (iii) marine reserves.

f) Identification of neighbouring installations, pipelines and piperacks in the area.

55 On the basis of available information, in brief listing, the safety case should:

a) give the name, address, and type of business for the neighbouring industrial installations; and
b) describe for example nearby housing and other buildings where there might be large numbers of people, or people who might be particularly vulnerable to a major accident.

[4] Information on Singapore's water catchment area can be found under the PUB website at http://www.pub.gov.sg/water/Pages/LocalCatchment.aspx

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

3.1 Introduction

56 This chapter gives guidance on how to present the **Major Accident Prevention Policy (MAPP)** and the required elements of a **Safety and Health Management Systems (SHMS)** for implementing the MAPP.

57 The overall aim is for MHIs to ensure that the safety case:

a) contains a MAPP;
b) demonstrates that there is an SHMS for implementing the MAPP;
c) demonstrates that the MAPP and SHMS are adequate in the context of the MAHs in the MHIs; and
d) demonstrates that all reasonable practicable measures have been taken to prevent major accidents or to limit their consequences for people and the vicinity (further discussed in Chapter 5, 6 and 7).

58 The information presented from Chapter 4 to 7 would help to demonstrate that the MAPP and SHMS have been put into effect. Therefore MHIs shall aim to show in the safety case that there is a systematic approach for delivering the desired outcomes, and that the outcomes have not come about by chance or in an ad-hoc way.

3.2 Major Accident Prevention Policy

59 The MAPP is a key document in the safety case. Its purpose is to provide a statement of the senior management's commitment to achieve high standards of MAHs control and process safety performance.

60 The MAPP shall be proportionate in its scope and structure to the MAHs and lay down the framework for achieving adequate identification, prevention and mitigation of MAS. It shall describe management systems establishing an appropriate health and safety culture, backed by procedures and practices for all aspects of process safety which take account of human factors. The MAPP shall also demonstrate a commitment to continual improvement.

61 The MHI's MAPP shall:

a) specifically address MAHs; and
b) relate to protection of people and the vicinity.

62 The MAPP shall set down what is to be achieved, with an indication of how this is to be done, but does not need to go into extensive detail. The detail shall be contained in other documentation relating to the MHIs (e.g. safety and health management system, plant operating procedures, training records, job descriptions).

63 The MAPP in the safety case shall include:

a) a recognition that the nature of the MHI's activities could give rise to MAS for 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) a suitable statement of the MHI's aims and principles of action and its commitment towards continual improvement of its control of MAHs at the installation;
c) statements explaining the company's overall aims and principles of action in relation to the systematic control of major accidents; and
d) a commitment to provide and maintain a management system which addresses the issues described under Section 3.3.1.

64 The MAPP shall be signed and dated by an appropriate director or senior executive to signify that it is truly the policy of the organisation's leadership.

65 The MAPP shall be made available to employees and others in the MHI (e.g. contractors). It may be appropriately displayed in the installation for all employees and contractors to be reminded of the organisation's commitment.

3.3 Safety and Health Management System

66 It is important that the policies described in the MAPP are put into operation through an SHMS. The MAPP shall set out the high-level policy. Below this, an SHMS is required to implement the policy aims in the MAPP.

67 The SS 506: Part 3 is an amalgamation of Process Safety Management (PSM) elements with that of Occupational Safety and Health, arranged in a Plan-Do-Check-Act framework as in SS 506: Part 1 or OHSAS 18001. The SHMS described in the safety case shall therefore cover the elements of SS 506: Part 3 as an integrated management system for the protection of people and effective management of dangerous substances, equipment and facilities.

68 MHIs are not required to describe the entire SHMS because it extends to matters beyond major accident prevention (e.g. occupational health and manual handling). The safety case needs to only describe the elements that are important for preventing major accidents or limiting the consequences for people and the vicinity. The amount of detail in the document shall be proportionate to the nature of the MAHs in the MHIs.

69 MHIs shall justify that an effective and adequate SHMS is put in place. MHIs are to demonstrate that the SHMS implemented is robust by putting in place an auditing scheme. The scheme includes appropriate audit frequencies, adherence to stipulated auditing scope, competency of auditors and the timely close-out of audit recommendations and findings.

70 MHIs may choose to use their own SHMS model instead of SS 506: Part 3 when describing the SHMS in the safety case. However MHIs would need to demonstrate that their in-house SHMS are at least similar to the elements covered in SS 506: Part 3. The SHMS may also be integrated within other management systems on-site (e.g. quality management system).

71 If MHI has obtained certification of SS 506: Part 3 by an accredited Certification Body, this can be used to facilitate the demonstration that the MHI has implemented an SHMS that is operating satisfactorily over a period of time. Verification of the SHMS may be subjected to lesser scrutiny if the MHI has obtained the certification for SS506: Part 3.

3.3.1 Main Area of Focus for SHMS Demonstration

72 Although most of the following elements listed below are already covered under SS 506: Part 3, MHD deemed these elements to be integral to the safety case demonstration and hence these elements would be assessed with greater scrutiny. The important elements of focus are:

a) **Roles and Responsibilities** – demonstrate that all necessary roles and responsibilities in the management of MAHs have been clearly allocated and defined;
b) **Resources** – demonstrate how MHI allocates resources to implement the MAPP;
c) **Personal Performance** – demonstrate that the performance of people having a role to play in the management of MAHs are measured and that they are held accountable for their performance;
d) **Worker Participation** – demonstrate that the MHI has systems for ensuring that those working in the installation, where relevant, are actively involved in the control of MAHs;
e) **External Organisation** – demonstrate that the MHI has in place arrangements for cooperating with, communicating information to and securing the cooperation of, external organisations such as SCDF; contractors and their employees;
f) **Information Gathering** – demonstrate that the MHI has arrangements for gathering information from external sources (e.g. latest legal and technical developments) needed for the control of MASs;
g) **Internal Communication** – demonstrate that the MHI has arrangements for communicating information important for the control of MAS within the MHI's organisation;
h) **Priorities for Improvement** – demonstrate that the MHI has systems for
   (i) determining priorities to achieve the objectives of the MAPP;
   (ii) identifying areas for improvement in relation to the control of MAHs; and
   (iii) scheduling the identified improvement work.
i) **Procedures** – demonstrate that the MHI has adopted procedures and instructions for safe operation and maintenance;

j) **Management of Change** – demonstrate 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;

k) **Active Monitoring** – demonstrate that the MHI has devised proactive means of performance measurement, which provide information on whether the control measures taken to guard against the realisation of major accidents are operating as intended;

l) **Reactive Monitoring** – demonstrate that the MHI has adopted a system for reporting incidents and near misses, relating to failure of control measures for MASs;

m) **Investigation and Response** – demonstrate that the MHI has adopted mechanisms for investigating and taking corrective action:

   (i) in cases of the proactive performance standards showing a deterioration in risk control measures; and

   (ii) in relation to any incident or near misses with potential to cause a major accident.

n) **Audit** – demonstrate that the MHI has adopted a procedure for systematic assessment of SHMS for the effectiveness and suitability of the SHMS;

o) **Review** – demonstrate 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; and

p) **Documenting the Review** – demonstrate that results of review are documented and communicated within the organisation.

Chapter 4: Predictive Aspects of Safety Case (Risk Assessment)

4.1 Introduction

73 This chapter will describe the risk assessment part of the safety case covering:

a) description of the activities and processes relevant to major accidents at installations;
b) identification of **MAHs** and **MASs**;
c) selection of **representative set of MASs** for detailed assessment;
d) **consequences assessment** and **likelihood estimation** of representative set of MASs; and
e) selection of **SCEs** for **ALARP** demonstration.

74 This chapter, together with Chapter 5, 6 and 7, explains how an MHI's risk assessment shall be both suitable and sufficient for the purposes of WSH (MHI) Regulations. Appendix 4A illustrates the workflow for the identification of MASs, risk assessment and ALARP demonstration.

75 It is essential for MHIs to identify all MAHs before going on to perform a sufficient and suitable risk assessment and identify risk reduction measures on identified MASs.

76 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.

77 The depth of analysis of each MAS needs to be proportionate to the hazards and risks by judging the significance of risk estimates against specified criteria (e.g. company internal risk criteria with suitable justification).

78 Any subsequent risk assessment may be qualitative, semi-quantitative, quantitative, or a combination of these. A proportionate consideration of all possible risk reduction measures are required and partial implementation of the most effective options should also be considered when appropriate.

79 Risk assessment is fundamental to the demonstration and determines whether the measures taken are all that are adequate and sufficient. MHIs will have to ensure that the scope and nature of the risk assessment is fit for purpose in relation to the circumstances in the installation and the demonstration required. When the risks are not acceptable, e.g. based on company internal risk criteria (with justification), a proportionate consideration of additional risk reduction measures is required. Even if the risk is at the acceptable level, there is an obligation to look for further control measures and apply if reasonably practicable.

80 These analyses can reasonably be banded into three levels of risk assessment:

a) Qualitative risk assessment

(i) is a qualitative assessment of whether the measures in place make the risks ALARP;

(ii) can represent the range of possible events by a broad classification of the likelihood and consequences for comparison purposes and the identification of priorities; and

(iii) must qualify through qualitative methods, the severity and likelihood of the MAS in each consequence category (e.g. risk matrix).

b) Semi-quantitative risk assessment

(i) is represented by means of qualitative and quantitative descriptions of the likelihood, extent and severity of the consequences to people on-site and off-site. Any frequency value used in the assessment shall be justified; and

(ii) can involve the use of some mathematical models to estimate levels of harm to people.

c) Quantitative risk assessment

(i) produces a full numerical representation of the likelihood and extent of a specified level of exposure or harm, to people on-site and off-site, from a specified activity; and

(ii) may quantify individual risk for hypothetical people on-site and off-site.

81 MHIs are required to prevent major accidents or limit their consequences by incorporating adequate control measure to ensure safety of people, and facilities during its lifetime. The approach to selecting appropriate measures is discussed later on in Chapter 5. Emergency measures related to handling a major accident emergency are detailed in Chapter 6. The concept and demonstration that control measures in place reduce risk to ALARP is further discussed in Chapter 7 of this guide.

82 For new installations or major modifications to existing installations (e.g. major revamps), MHIs shall demonstrate that their risk assessment includes:

a) consideration of the elimination of hazards;

b) inherently safe approaches to reduce the scale of hazards;

c) preventive and mitigative measures to limit risk.

83 It is also important that human factors are taken into account throughout the risk assessment process. 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.

Note: Refer to Appendix 5A on details of implementing Human Factors and its elements in safety case submissions.

84 MHI without a prior approved QRA study for its installation shall conduct a risk contour development study. MHI can use selected scenarios from identified MASs in its safety case (SCEs and other such scenarios deemed relevant from the set of representative MASs) to conduct the study. Further details on site risk contour development are outlined in Appendix 4B.

4.2 Description of the MHI and its Activities and Processes Relevant to Major Accidents

85 The safety case shall contain plans, maps or diagrams with descriptions which clearly set out detailed information about the MHI with a potential for major accidents. For sections of the MHI that could give rise to major accidents, the safety case should contain detailed process descriptions such as:

a) block flow diagram or process flow diagram;
b) the operating parameters and envelopes of the MHI 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 operating 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. regeneration) 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 occur;
h) dangerous substance locations and at each location, an indication of the chemical and physical state and quantity of the dangerous substance; 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).

4.3 Preparing Information about MASs

86 The main elements required in preparing information about MASs include:

a) identifying all possible MAHs and MASs;
b) selecting a representative set of MASs for detailed assessment;
c) producing an adequate assessment of the extent and severity of the consequences for representative set of identified MASs;
d) providing a realistic estimation of the likelihood of representative set of MASs; and
e) selecting SCEs from representative set of MASs for the purpose of ALARP demonstration.

4.3.1 Identifying all possible MAHs and MASs

87 The safety case shall demonstrate that a systematic process has been used to first identify all possible MAHs and then the potential MASs from each hazard identified.

88 MHIs shall identify and describe the hazard identification methods used in the safety case. The safety case shall recognise that control measures can fail and therefore all hazards shall initially be considered as if no control measures were in place. The relevant expertise of the hazard identification team involved shall also be described.

89 MHIs should employ one or more recognised risk studies when identifying all possible MAHs and then the potential MASs. Risk studies that MHIs may use (but not limited to) include:

a) QRA studies;
b) PHA studies such as HAZOP, failure mode and effects analysis (FMEA), process hazards review (PHR);
c) safety reviews and studies of the causes of past major accidents and incidents;
d) industry standards or checklists;
e) job safety analysis (e.g. task analysis);
f) human failure identification method.

90 The safety case shall also demonstrate that a systematic process has been used to identify initiating events and event combinations which could cause MAHs to be realised. 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 sections 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) transportation of dangerous substances offsite (e.g. roads, pipelines);
   (iii) functional interdependence with the installations of neighbouring activities;
   (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. loss of power or steam disruption from external providers).

91 Some examples of the different types of MASs that could be identified are shown in Table 1 below. Scenarios influenced by emergency action or adverse operating conditions should also be taken into consideration during the hazard identification process.

	Scenarios Identified	Potential Consequences
a)	Loss of containment accidents due to vessel or piping failures	Toxic releases, or fire and explosion hazards such as BLEVE fireballs, flash fires, pool fires, jet fires and vapour cloud explosions (VCEs)
b)	Runaway exothermic reactions	
c)	Overfilling of storage tank	
d)	Detonation of solids or liquids that have a high heat of decomposition	Condensed phase explosions

Scenarios Identified		Potential Consequences
e)	Applying water to a storage tank on fire instead of allowing the flammable substance to burn to completion and water in the storage tank on fire	Boilover explosion
f)	Dumping reactor contents into the drain to avoid an explosion	Incompatible reactions occurring with other existing substances in the drain

Table 1: Table showing the relation between the hazard identified and its consequences

92 There shall be a suitable review of past accidents and incidents relevant to the MHI. 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 MHI.

93 For some safety case development, quantitative type risk analysis (e.g. QRA or other similar methodologies) may be used in conjunction with PHA or other safety reviews to identify MAS. Scenarios from quantitative type risk analysis studies are typically associated with release scenarios at specific isolatable sections of the facility (e.g. 10mm hole size release of propane from rundown pipe section), but with limited description of associated initiating events. Therefore, reference to scenarios in PHA or other safety reviews can be made to identify possible initiating events applicable within the specific isolatable sections (e.g. external corrosion at pipe support). It is therefore recommended to establish links between QRA and the relevant PHA or safety review scenarios with output presented in the form of a link table such as the following:

Isolatable section	Scenarios from QRA studies	Applicable scenarios from PHA or other safety reviews within same isolatable section
24" product rundown pipe from process unit rundown pump discharge to product storage tank	10mm hole size release from pipe	Flange leak due to overpressure from blocked outlet caused by inadvertent valve closure
Reactor section, including feed pumps, feed effluent exchangers, between upstream and downstream manual block valves	Catastrophic failure of reactor	Runaway exothermic reactions

Table 2: Link table showing the link between QRA and relevant PHA studies

4.3.2 Selecting a representative set of MASs for detailed assessment

94 From the hazard identification process, MHIs shall describe a representative and sufficient set of MASs for the purpose of detailed assessment (Section 4.3.3 and 4.3.4) which will then be followed by the selection of a set of SCEs for the demonstration of ALARP. The representative

set of MASs is a subset of all MASs considered during the hazard identification stage. This should include:

a) 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 such as vapour cloud explosion, pool fire, toxic dispersion (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.

95 Justifications shall be clearly presented and well-argued for eliminating possible MASs from further consideration.

96 Subsequently MHIs shall justify on the risk assessment methodologies used when conducting detailed assessment on the representative set of MASs. 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.

97 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.

4.3.3 Producing an adequate assessment of the extent and severity of the consequences for representative set of identified MASs

98 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 MAS has been carried out with respect to people.

99 The safety case shall:

a) Present **extent** information:
   (i) 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.:
   (i) Numbers of fatalities, serious injuries, hospitalisations;
   (ii) Banding in terms of consequences to people (e.g. 1-5, 5-20, 20-100);
   (iii) Where major accidents have been put into example groups, then it is acceptable to present extent and severity for each group;
   (iv) Occupancy based population data.

100 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, for example wind speed, atmospheric conditions and ground roughness in gas dispersion models.

101 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.

4.3.4 Providing a realistic estimate of the likelihood of selected representative set of MAS

102 The safety case shall contain:

a) estimates of the probability, in qualitative or quantitative terms, of each representative MAS analysed and
b) a summary of the initiating events and event sequences (operational, internal or external causes as outlined in Paragraph 90) which may play a role in triggering each MAS.

103 Any methods used to generate event sequences and to estimate the probabilities of potential major accidents shall be appropriate and used correctly. This should include the use of:

a) relevant operational and historical failure data;
b) fault tree analysis (FTA);
c) event tree analysis (ETA); or
d) other relevant methodologies.

104 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 shall be included if MHIs have used them.

105 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.

106 The selection of failure rate data shall be aligned to the Revised QRA Guidelines. Otherwise, MHIs shall justify and where appropriate includes references and methods of derivation 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.

107 Realistic and adequate justification shall be provided for estimates of, or assumptions made about, the reliability of protective systems and the times for MHIs to respond and isolate loss of containment accidents or others. Where possible, arguments shall be backed-up by credible performance data. Any qualitative arguments 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.

108 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.

109 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 MHD to make a judgement on the quality of the risk assessment.

4.3.5 Selecting SCEs from representative set of MASs for purpose of ALARP demonstration

110 The risk assessment shall show which events are critical from a safety point of view and this requires consideration of the likelihood of the various MASs and the associated consequences. The safety case shall identify SCEs and the basis for the choice of the identification. The following should be considered when identifying SCEs:

a) worst case scenarios such as pool fire, flash fire, jet fire, vapour cloud explosion, BLEVE, fireball, physical explosion and toxic release; and
b) the most likely scenarios in each consequence band.

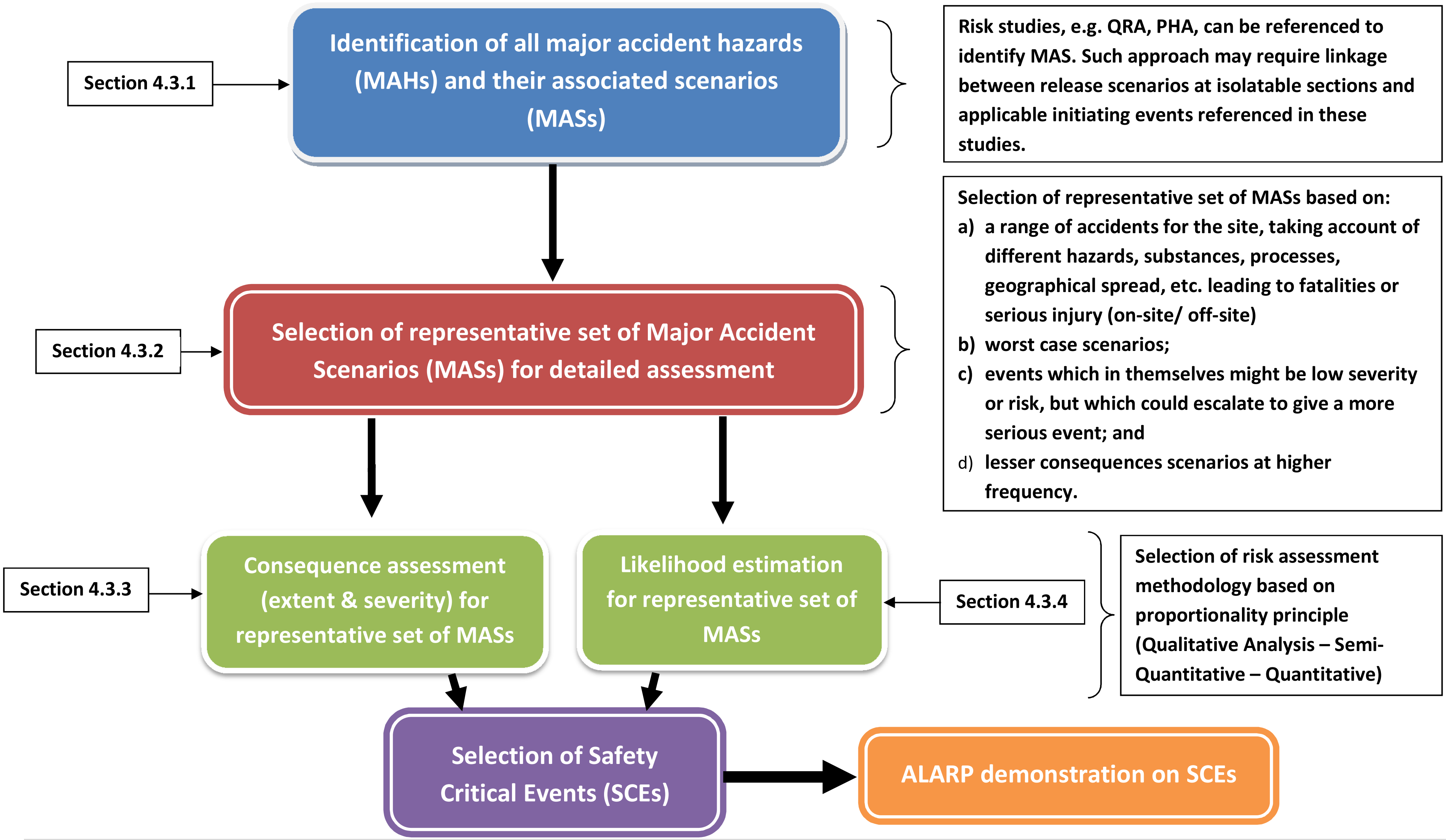
111 SCEs are those MASs that dominate the contribution to risk and thus are key to identifying suitable control measures for preventing major accidents or limiting their consequences. However, the failure of these control measures shall also be considered in assessing whether the residual risks are ALARP or whether more needs to be done.

112 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.

113 The risk matrix could also be used to inform of the proportionality of the installation as a whole. MAS 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.

114 While MHIs are not required to demonstrate ALARP for non-SCEs, MHIs are to continue to ensure that risks from all other scenarios are reduced to ALARP as required under the WSH Act.

Appendix 4A: Workflow for Risk Assessment and Selection of SCE for ALARP Demonstration



Appendix 4B: Site Risk Contour Development

115 The purpose of this appendix is to provide a pragmatic approach that legacy MHIs[5] could adopt to generate site-wide risk contours. The site-wide risk contours generated will enhance understanding of their on-site and off-site risks for the safety case.

<u>Methodology</u>

116 Site risk contours can be generated using UK HSE's, in-house or other established simplified or alternate QRA methodology. It is expected that the methodology (together with the selected scenarios) should be able to generate the risk contours that are approximate to that of a full QRA study. MHIs are advised to engage MHD on the intended methodology with supporting justifications.

<u>Reference to QRA Guidelines[6] with respect to parameters and outputs</u>

117 Reference should be made to the Revised QRA Guidelines in the development of site-wide risk contours for parameters including failure rates, frequency modifiers, consequence modelling and assumptions.

118 The Individual risk contours plot including fatality, injury, cumulative escalation and onsite occupied building risks shall be presented based on the Revised QRA Guidelines.

<u>Scenario Selection</u>

119 As per safety case, the SCEs derived are expected to encompass a selection of diverse events of the MHI, covering varying MAHs and consequence types, including those with potential off-site or on-site impacts. For risk contour generation, scenario selection could be based on the identified SCEs, and inclusion of additional scenarios from the list of representative MASs are to be considered with proper rationale and justifications. The additional MAS selected are to meet the following objectives:

a) Adequate geographical spread of off-site risk; and
b) Adequate geographical spread of on-site occupied building risk

<u>Note:</u> Legacy MHIs, which are developing risk contours based on the approach outlined in this appendix, are not expected to fulfil the Revised QRA Guidelines criteria. They are, however, required through a safety case to reduce risks to ALARP.

[5] Legacy MHIs are MHIs which have no prior approved QRA for their existing sites.
[6] Based on the latest version on NEA's website.

Chapter 5: Technical Aspects of Safety Case (Preventive & Mitigative Measures)

5.1 Introduction

120 This chapter deals with the part of the safety case which describes the measures taken to prevent major accidents and to limit their consequences to people and the vicinity. The information in this chapter and Chapter 4 are closely linked and MHIs shall therefore:

a) demonstrate that there is adequate safety during the life cycle of the installation and infrastructure relevant to major accidents; and
b) describe and justify the choice of control measures for making risks ALARP based on SCEs identified in Chapter 4 and demonstrate that performance standards and performance indicators are developed to provide the ongoing assurance that key systems relevant to major accidents are in place and working.

121 The WSH (MHI) Regulations requires a demonstration that adequate safety and reliability has been incorporated into the design, construction, operation and maintenance of the installation. The Regulations also specifies the minimum information to be included in a safety case and includes a description of the technical parameters and equipment used for the safety of the installations and a description of the equipment installed in the installation to limit the consequences of major accidents.

5.2 Description of Facilities and Infrastructure Relevant to Major Accidents

122 The safety case shall show a clear link between the measures taken and the SCEs described in Chapter 4 and demonstrate how each control measure (engineered or administrative) contributes to making the risks ALARP. Where representative scenarios have been chosen, the measures for preventing or limiting a major accident can relate to a broad range of scenarios with similar hazards and outcomes.

123 One way the link between the MAHs, SCEs and control measures can be represented by using a 'bow-tie' diagram (also called a cause-consequence diagram) as shown in Figure 1. The centre of the diagram is the loss of containment (LOC, i.e. top event). The left side of the bow-tie depicts all the possible initiating events or causes which could lead to the occurrence of the top event. The vertical bars on the left side refer to the control measures that are put in place to prevent the initiating event from cascading into a LOC of dangerous substances. These vertical bars also include efforts to sustain the intended effectiveness of the control measures in the event of escalation factors[7]. The right of the bow-tie describes the development of possible

[7] Conditions or situations that lead to the departure of the barrier function from their design intent and rendering the measures ineffective.

consequences resulting from the top event. The vertical bars on the right side refer to the control measures to mitigate or limit the harm caused to people and vicinity.

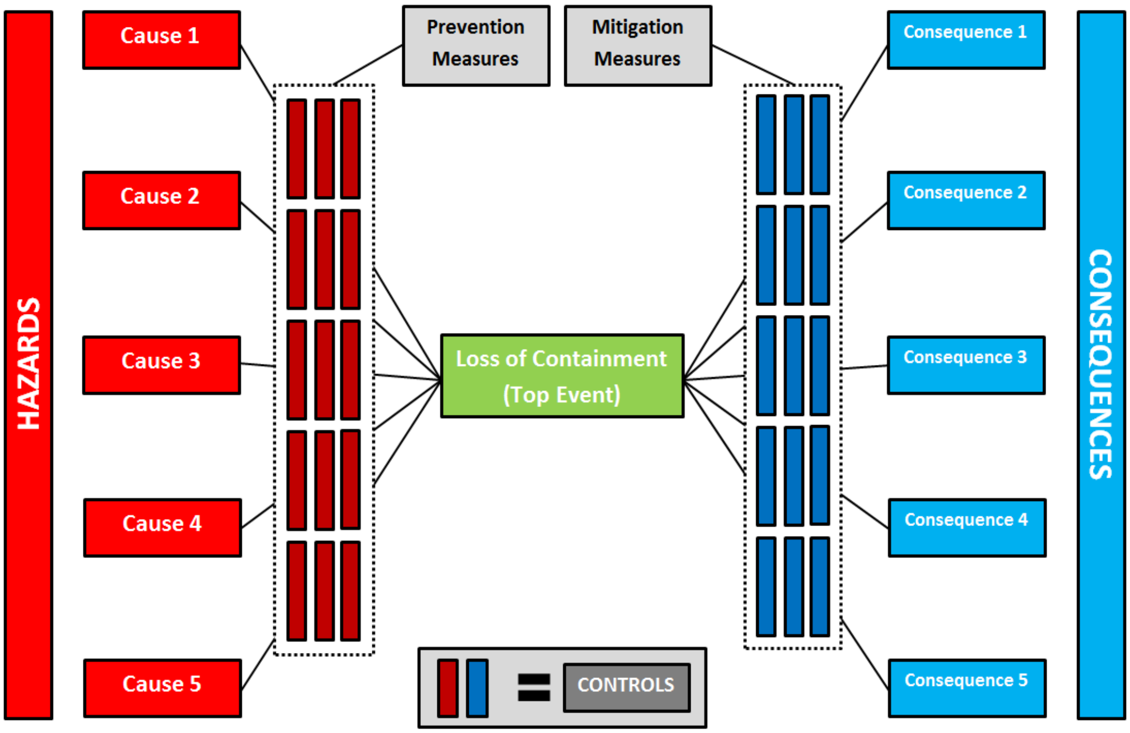


Figure 1: Bow-tie diagram depicting relation between hazards, consequences and measures

124 Control measures can be engineered, like hardware and software systems or administrative, like operating procedures or inspections. It is important that the performance specified for the control measures shall be related to MASs. The safety case shall provide clear descriptions and justifications for the applied control measures such as:

a) Control of the processes, taking into account of expected normal and abnormal operations;
b) Verification of the adequacy of the initial integrity and continuing integrity of the containment boundary (further elaboration in Section 5.3.1.2 – *Design key issue 5: containment*). Direct causes of failure of containment could include:
  - Corrosion;
  - Erosion;
  - External loading;
  - Impact;
  - Overpressure;
  - Low pressure or vacuum;
  - High or low temperature;
  - Vibration;
  - Wrong or defective equipment and
  - Human failures.
c) Use of safety instrumented systems (SISs) and their reliability;
d) Hazardous area classification and suitability of equipment within designated hazardous zones;

e) Effective human intervention.

Guidance on the range of measures to be applied and the issues to be considered in their selection are elaborated further in Section 5.3 of this chapter.

125 The safety case shall also contain technical information about items of the MHI relevant to MASs such as:

a) vessels or tanks, for example location, type, size, inventory, design and operating limits (e.g. temperatures and pressures), purpose and contents;
b) pipework systems containing dangerous substances (e.g. routes, types, size, design, flow rates and operating limits, and purpose);
c) utility services (e.g. steam, air, electricity, fuel, hot oil and water);
d) drainage, for example routes and purpose (e.g. fire-fighting run-off water);
e) stacks, flares, abatement systems (e.g. scrubber) such as location and purpose;
f) safety critical valves, instruments, control loops and detection systems;
g) fire-fighting and supply arrangements; and
h) monitoring equipment (e.g. for toxic products in air, sewers, discharges to water, and for fires, explosive or flammable atmospheres).

126 Where a number of hazards are comparable, the information provided about the control measures in place for one of these hazards is sufficient as long as this provides evidence that the other similar hazards are also adequately controlled. MHIs may also decide to provide information of the equipment and control measures that is common to the installation or common to some particular sections and only deal with differences from these descriptions in relevant parts of the safety case. An example of where this might be applicable is in the description of overpressure protection for similar storage vessels. MHIs may have a policy of providing protection to prevent rupture of vessels as a result of fire engulfment, which MHIs could justify once and not repeat in the safety case. MHIs then only need to identify, say, those vessels protected by pressure relief valves to prevent overpressure from other causes, such as exothermic reactions and process excursion.

127 For existing MHIs, in undertaking risk assessment and providing justification, MHIs should also consider if newly adopted control measures could pose additional hazards or contribute to MASs (e.g. during installation, commissioning or operation of new control equipment).

128 For any risk reduction measure that is planned but not implemented, specific commitments shall be included in the MHI overall action plan that demonstrates the MHI's intention. Depending on the level of risks faced by the MHI, the action plan shall take a risk-based approach (based on proportionality principle) and take appropriate interim measures while long-term solutions are being implemented.

129 Control measures shall be independent from the cause of the initiating event and independent of the other control measures identified within the same scenario, so as not to fail as a direct result of the initiating event or cascading event.

130 The basic requirement for control measures for SCEs is that they shall collectively reduce the risk to the health and safety of people to ALARP. Methods of ALARP demonstration are detailed in Chapter 7.

5.3 Describing how the Control Measures Taken will Prevent Foreseeable Failures which could lead to Major Accidents or Mitigate their Consequences

131 There are five main elements, relating to the life cycle of the installation, to be considered when demonstrating how MHIs prevent major accidents or limit their consequences. The five main elements are:

a) **Design** – includes plant layout, process design and design of equipment; discussion of conceptual design is important for new or modified installations;
b) **Construction** – includes the manufacture, installation, construction of facilities, testing, initial inspection and commissioning;
c) **Operation** – includes plant start-up, shutdown, normal operation, including foreseeable temporary operations, emergency shutdown and the extent to which deviation from normal operation will be tolerated;
d) **Maintenance** – includes preventive maintenance, repair, replacement, periodic examination by competent personnel, and the assessment of any defects found; and
e) **Modification or decommissioning** – includes the measures to deal with changes that may take place on the installation during its life, including all alterations, and during decommissioning, which could affect the integrity of the remaining installation.

132 In addition to the abovementioned five main life cycle elements, MHIs shall also demonstrate that appropriate codes and standards are considered and applied throughout the life cycle of the installations. Use of industry codes and standards are further elaborated in Section 5.3.1 of this chapter.

5.3.1 Use of Industry Codes and Standards

133 The safety case shall show that plants have been designed to appropriate codes and standard and give references to standards and codes of practice used as the basis for the design of the plant process and the selection of appropriate risk control measures. This is essential for safety cases for new or modified plants. In principle, such standards may be regulator's guidance, international standards, Singapore standards, international industry practices, company-specific standards, etc. However the existence of a published standard does not imply that it is always useful or correct. Whichever standards are being used, these standards and the control measures that are applied, shall all be shown to be suitable and appropriate to MHIs, taking account of its type, scale, activities, location, etc.

134 MHIs have the responsibility to consider the available standards, specify the correct one, and use the system or equipment correctly. Validation of suitability of standards for equipment of high safety concern is also necessary. Whatever standard or set of standards is used for equipment of high safety concern, MHIs shall take care to justify applicability and recognise limitations of those standards. MHIs shall clearly outline and justify the rationales for combining different design codes or standards to make the demonstrations in the safety case.

135 For new projects or major modifications, MHIs shall include information about any deviations with standards used. For existing installations, this applies to control measures for SCEs.

136 Standards are good at a system or equipment level but not necessarily suitable at a holistic level; they cannot be relied upon to give an indication of the adequacy of risk management of a combination of unique hazards on a specific MHI. In this situation, it is common for an MHI to adopt a suite of standards, perhaps taken from a number of different organisations. In such cases, significant effort may be necessary to show that this overall suite of standards is suitable and appropriate, as well as the individual parts. For particular issues that are not covered by the individual standards and need additional consideration, there will be benefits for MHIs in developing a “basis of safety” for its specific installation.

137 There may be cases where the current most relevant standard is not complied with in certain respects. An example may be a complex or novel facility where there are no applicable standards. In such cases, MHIs shall show that a gap analysis has been conducted between design standards and codes applied at their installation and relevant current standards and codes for control measures (i.e. prevention and mitigation measures) applicable to SCEs. MHIs could subsequently show that additional measures have been introduced to compensate (i.e. to show that equivalent safety has been achieved), or that additional measures are not reasonably practicable. Examples of measures that may achieve equivalent safety are re-rating of equipment and introduction of more frequent testing or inspection.

138 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.

139 Where gaps are known or suspected to exist, for example if there is a gap in overall control measures, or a measure has been compromised by age, this shall be explicitly identified. Solutions for addressing these weaknesses shall be explored and the chosen solution incorporated.

140 The review of MASs and risks shall be a planned periodic process whereby the applied standards on an MHI are reviewed against new and updated standards. If new standards or requirements are introduced, they cannot be dismissed because the installation was built prior to them; neither should they be automatically adopted: the risk assessment process shall be undertaken. The task would be to understand the intent of the new standard and the change that it evokes

from the current or existing operating situation. Once the assessment has taken place then decisions can be made about implications for a new understanding of risks of the MHI and the steps that need to be taken. Review of standards shall be limited to those applicable for control measures for SCEs for older installations.

5.3.2 Design

5.3.2.1 Suitability and selection of control measures

141 MHIs shall describe the hierarchical approach used to select the control measures for their installation. The initial design stage presents the best opportunity to remove hazards and reduce risk. The use of a hierarchical approach to the selection of measures will help to ensure that precedence is given to those measures that avoid major accidents (i.e. through inherent safety and prevention measures). However, prevention cannot be guaranteed in all circumstances and therefore it will be necessary to also identify other control measures to control and mitigate the consequences for all identified SCEs. The demonstration that risks from SCEs are eliminated or reduced to ALARP may need to be made individually, in groups, and as a whole.

142 MHIs shall show how their hierarchical approach will be applied to new and modified facilities that are being installed, and what procedures there are for applying this approach when designing new plants or major modifications to existing ones. The approach of selecting measures shall reflect the levels in the hierarchy as follows:

a) inherent safety;
b) preventive measures; and
c) mitigative measures.

143 MHIs shall also apply the hierarchical approach to the design of modifications and older MHIs shall be alert to the possibility of taking advantage of technical advances in their industry to improve safety.

a) Inherent safety

144 Inherent safety is concerned with the removal or reduction of a hazard at source. Examples of inherently safer techniques include:

a) elimination, reduction of hazardous inventory;
b) substitution of a hazardous process for a less hazardous process or replacing a hazardous material for a less hazardous alternative;
c) reduce hazardous process conditions (i.e. pressure, temperature, etc.);
d) use of corrosion-resistant construction materials;
e) minimising potential leak paths (e.g. reducing the number of flanges in a piping system);
f) design for maximum foreseeable operating conditions;
g) fail-safe design principles (e.g. valve position on failure);

h) avoiding undue complexity in design to reduce risk of human failure (e.g. simpler systems or processes to reduce possibility of errors causing a potential LOC or hazardous event); and
i) appropriate plant layout (e.g. domino effects consideration).

b) Prevention measures

145 Prevention measures are intended to prevent the initiation of events which could lead to a LOC that could further escalate into a major accident. They could include but not limited to:

a) management systems;
b) design of the installation;
c) design to prevent failure of equipment or human failure and include specific activities (e.g. maintenance or inspection) aimed at preventing specific failures;
d) hardware arrangements such as double-walled piping to provide a secondary containment or use of canned or magnetic drive pumps;
e) relief valves;
f) safety-related control systems; and
g) manually initiated or automated emergency shutdown procedures
h) venting to scrubbing systems or flare stacks.

c) Mitigation measures

146 Mitigation measures which are intended to mitigate the potential consequences of a LOC or to minimise the consequences of a major accident once it has occurred. Examples of these include:

a) safety refuges or in-place protection (IPP) facilities against toxic dispersion and blast overpressure (e.g. suitably designed control room);
b) bunding systems;
c) fire-fighting facilities;
d) gas detection systems;
e) deluge systems;
f) emergency response procedures; and
g) traverses or mounds for explosive buildings.

147 Chapter 6 of this guide provides more detail on mitigation measures relating to emergency response.

5.3.2.2 Adequate safety and reliability in design

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

<u>Key Issues in Design</u>

1. Redundancy, diversity, separation and segregation;
2. Impact of a single event which may have multiple effects;

3. Layout of the plant;
4. Reliability, availability and survivability of utilities;
5. Containment;
6. Structural integrity, including:
    a) evidence of conformity;
    b) normal operation and foreseeable extremes and
    c) materials of constructions;
7. Protection from excursions beyond design condition, including:
    a) normal operating limits; and
    b) safe operating limits;
8. Safety-related control systems;
9. Human factors; and
10. Systems for identifying locations where flammable substances could be present.

149 For new or modified facilities, justifications shall be clearly presented in the safety case for not considering any of the key design issues mentioned above. Demonstration of design considerations in a safety case could be done through an MHI's project design philosophy or instituted in an MHI's management system when administrating design policies, etc. Details of the design philosophy could be verified during on-site safety case assessments.

Design key issue 1: redundancy, diversity, separation and segregation

150 MHIs shall show in the safety case how the principles of redundancy, diversity, separation and segregation have been applied to reduce the risk of common-mode or common-cause failure and to ensure the availability of back-up systems if required, for example a battery back-up to an essential power supply or availability of back-up pumps or compressors which are available on an auto start basis.

151 MHIs shall include potential failure of equipment of high safety concern, and address events which may disable protective systems.

Design key issue 2: impact of a single event which may have multiple effects

152 Where a single event, such as the loss of power supply, can affect some or all parts of an installation at once, then the risk of it leading to a major accident may be increased. The safety case shall show that the cumulative effects of such an event have been considered. This includes events that are internal to the installation such as power failure, and external events such as flooding or other natural events wherever applicable.

Design key issue 3: layout of the plant

153 The layout of the plant shall limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement.

154 The design of plant layout can make a big contribution to reducing the likelihood and consequences of a major accident. The safety case shall show that 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) low congestion of structures, equipment, plant or any other obstacle to gas flow that could aggravate the overpressure effects resulting from the ignition of a release of a flammable substance;
b) separation between facilities with MAHs or dangerous substances and storage areas to limit the spread of fire and other domino effects;
c) adequate safety refuge or IPP facilities during any toxic release and adequate means of escape during other emergencies;
d) access for emergency services;
e) access for inspection, testing, maintenance and repair, at all times throughout the life of the plant;
f) 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;
g) safe positioning of occupied buildings;
h) separation of facilities with MAHs or dangerous substances and processes from ignition sources, roadways or other activities which may impact on safety.

Design key issue 4: reliability, availability and survivability of utilities

155 Utilities that are needed to implement any control measure (safety critical utility) defined in the safety case shall have the necessary reliability, availability and survivability to prevent or limit the consequences of a major accident. Site utility systems may include:

a) electrical power;
b) steam or condensate;
c) inerting gases (e.g. nitrogen);
d) compressed air;
e) vacuum systems;
f) cooling water;
g) process or service water;
h) fuel (e.g. oil, gas);
i) refrigeration; and
j) any other safety critical utility.

156 Failure of a utility, for example water, air, steam or electricity (including power surge or partial loss), often results in a process upset, and may have effects across the entire installation. Failure of an emergency facility for example firewater, has the potential to cause a relatively small incident to escalate into a major accident. The safety case shall justify the measures taken to ensure that these utilities and facilities will be available when required.

157 The justification that the utilities are suitable may include reference to:

a) the routing of services;
b) physical protection (e.g. barriers and fire-proofing);

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.

Design key issue 5: containment

158 MHIs shall identify the means by which dangerous substances can be accidentally released from the containment system and the prevention measures provided. It shall also demonstrate the suitability of the measures to prevent releases. Such measures may include:

a) Prevention 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 or 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, for example 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.

159 With certain exceptions such as explosives where confinement may increase the hazard, dangerous substances pose less of a hazard if they are contained within the plant (e.g. secondary containment bunds, kerbs at plant boundary). MHIs shall show in the safety case how the installation has been designed with this in mind.

160 MHIs shall also include details of systems designed to prevent LOC and to manage unplanned releases. These could include:

a) **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.

b) **Secondary and Tertiary containment measure***s* – where LOCs of a significant quantity of dangerous substances are foreseeable, the safety case shall describe the measures to mitigate the consequences. These mitigation 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.

c) **Venting systems** – the safety case shall justify the design basis for any venting system, taking into account foreseeable hazards, including the loss of utilities or the effects of fire, and the consequences of venting to the vicinity.

d) **Isolation arrangements** – the safety case shall describe and justify the emergency automatic and manual isolation arrangements to manage a release, including consideration of the time required to isolate.

(Note: 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.)

e) **Other prevention and containment systems** – the safety case shall justify the design basis for each of these measures taking into account the foreseeable hazards.

(Note: 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.)

f) **Detection of releases** – the safety case shall describe the measures to detect a LOC or other incident at an early stage. These measures include level monitoring, loss of pressure, gas detection, visual methods (cameras), etc.

161 All foreseeable direct causes of LOC incidents shall be considered at the design stage. The majority of direct causes fall into one of the following categories. The safety case shall show that these causes have been considered and suitable measures taken:

a) **corrosion** – may be internal or external, and may be enhanced by synergistic effects such as stress corrosion cracking or erosion-corrosion. MHIs shall identify particular areas where corrosion may occur and the measures taken to prevent and monitor such effects, for example design codes, construction standards, protective systems (inert linings, cathodic protection, etc.) and periodic inspection.

b) **erosion** – may be caused by excessive fluid velocity, a change in phase, cavitation or the presence of particulates. MHIs shall identify particular areas where erosion may occur and the measures taken to prevent and monitor such effects, including periodic inspection.

c) **external loading** – may be caused by extreme weather or ground movement (e.g. land subsidence), by the forces applied during construction or during operation, and by failures of pipe or vessel supports nearby. MHIs shall show that the foreseeable events will not affect the integrity of the containment or its supporting structure.

d) **impact** – damage may occur from road vehicles and ship vessels. MHIs shall identify the main sources of impact considered in the design and the critical items of plant exposed to impact damage. It shall also show that adequate precautions have been put into effect.

e) **pressure** – over- or under-pressure may cause LOC. MHIs shall show how excess pressure will be prevented during foreseeable failures, such as in the event of single failure or event of:

(i) failure of process controls between the system and other higher pressure systems or sources;
(ii) failure of over-pressure safety devices;
(iii) pressure surge or water hammer;
(iv) external fire;
(v) internal explosion;
(vi) excessive reaction rate; and
(vii) liquid expansion or exothermic reaction causing an increase in temperature and pressure.

Note: MHIs shall also cover vacuum, if it has been identified as a hazard condition.

f) **temperature** – high or low temperatures of the equipment may reduce its strength or make it susceptible to creep or brittle failure. Excessively high rates of change in temperature may also generate high thermal stresses. MHIs shall identify the measures in place to prevent thermal problems due to process upsets, fire, or possibly adverse weather conditions in the case of plant exposed to the elements. Examples of measures taken may include separation, water deluge, insulation, fire walls, heat tracing or other suitable means.

g) **vibration** – may be generated within the containment, caused by changes in phase, water hammer, high pressure drop or cavitation. Externally generated vibration may be due to the incorrect positioning of pumps, poor piping design, etc. Excessive vibration may induce fatigue failure of the containment. MHIs shall show how vibration has been assessed, and any potential problems addressed.

h) **wrong equipment** – if the wrong equipment has been specified or installed, there is a potential for failure. MHIs shall identify the management controls in place to ensure correct specification, supply and installation of equipment, including spare parts.

i) **defective equipment** – may cause failure due to pre-existing flaws, high stress, etc. MHIs shall show that suitable management procedures are in place to identify faults and control or limit effects of failure.

j) **human failure** – human failure may cause failure of the containment system by overfilling or overloading, or by some other manually initiated maloperation (e.g. operator initiates valve opening) and includes failure to take the required action. MHIs shall consider the possibility and effects of human failure and describe the measures in place to minimise the risk.

Design key issue 6: structural integrity

162 The safety case shall show how equipment and structures important to safety have been designed to provide adequate integrity.

163 MHIs shall provide sufficient evidence to show that the design of facilities important to safety has been based on sound engineering principles.

164 Reference to recognised standards (e.g. ASME Boiler and Pressure Vessel Code) is normally sufficient as long as the plant is operating within the parameters set by the standards. Deviations from the principal design codes used or features not within the standard design type, shall be highlighted and described in the safety case. They warrant special attention as shall any features not within the standard design type. If a relevant design standard or code has not been used, MHIs shall provide a justification for and description of, the design method adopted.

165 Other key structural items, such as support structures, civil foundations, control rooms, buildings or barriers designed to withstand the effects of accidental explosions, shall also be included where they are important to the demonstration.

166 There are three elements to this key issue:

a) evidence of conformity;

b) normal operation and foreseeable extremes; and

c) materials of construction.

a) Evidence of conformity

167 MHIs shall confirm that the design of equipment and structures important to safety is supported by any necessary documentation to give an assurance of conformity. Compliance with design standards and codes establishes a baseline for the structural integrity of the plant.

b) Normal operation and foreseeable extremes

168 MHIs shall show how the equipment and structures have been designed to withstand the loads experienced during normal operation of the plant and all foreseeable operational extremes during its expected life.

169 Information presented in the safety case shall therefore show that it has taken account of all the conditions that the equipment and structures must withstand, 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).

170 MHIs shall show that facilities will perform their required safety functions throughout their total life, under all foreseeable operational and fault conditions. The demonstration shall consider the various loading conditions arising, and show how the effects of any degradation processes on the integrity of the containment have been catered for in the design (e.g. corrosion allowance approach).

171 MHIs shall define the basis of safety margins incorporated in design such that the safe working limits of the plant (e.g. pressures, temperatures, flow rates) are compatible with all expected operating extremes.

172 Specific details shall be given where actual applied margins differ significantly from the approach normally applied or industry practice. The safety implications arising from the variation shall be described and justified.

c) Materials of construction

173 MHIs shall show that construction materials used in the plant are suitable for the application. It shall provide evidence that:

a) all materials employed in the manufacture and construction of the plant are suitable; particular attention shall be given to the selection of materials used for the primary containment of hazardous substances;
b) materials have been selected with regard to the nature of the environment in which they will be used for example the substances being handled, process conditions such as temperature, pressure and flow, possible sources of corrosion, and erosion;
c) the external environment, such as the effects of sea air in coastal areas, has been considered; and
d) the effects of impurities on the containment materials have been allowed for (impurities are regarded as including unwanted by-products of reaction as well as imported impurities). The evidence shall consider the impurities likely to be present under normal operating conditions and those that could foreseeably be present due to abnormal conditions, such as process upset or maloperation.

174 If a design code or standard has been used which includes materials selection criteria, any deviation from the materials specified in the code shall be justified in the safety case.

175 In such cases, MHIs should show that alternative materials were considered and assessed before the final selection was made.

176 Where materials selection is critical to prevention of MASs for new and SCEs for existing installations, MHIs shall include a description of the materials selection approach, for example where:

a) vessels will be used at very low temperature;
b) materials are required to contain particularly aggressive or corrosive substances;
c) materials will be used with explosives; or
d) a novel or unusual use of materials is proposed.

Design key issue 7: protection from excursions beyond design conditions

177 MHIs shall show that adequate control measures have been provided to protect the plant against excursions beyond design conditions.

a) Normal operating limits

178 A plant is usually designed to operate within a given range of process variables: the normal operating limits. These are the operating constraints which apply to normal operating conditions. Normal operating limits are set to ensure that a suitable margin is present between normal operating conditions and the safe operating limits. The margin shall be set so that for foreseeable failures (e.g. equipment failure), appropriate corrective actions can be taken before the safe operating limits are exceeded. The corrective actions can be either automatic, manual, or a combination of both.

179 Control systems (automatic and manual) are the first line of defence against excursions beyond normal operating limits. Alarm systems usually detect excursions beyond normal operating limits, using sensors that may or may not be entirely independent of the control system.

b) Safe operating limits

180 There are also the safe operating limits, which are the rated values on which the safety of the plant is based. An excursion beyond the safe operating limits may result in an increased risk of LOC, fire or explosion. Hence, safe operating limits are determined primarily by the process design and material specification (design conditions), but are also influenced by the age and condition of the facilities. Where a control or alarm system has a role in the defence against excursions, beyond the safe operating limits, it shall be assessed as a safety-related control system (see Design key issue 8).

c) Protection from excursions beyond design conditions

181 Safe operation depends on the measures to prevent excursions from occurring (e.g. safety-related control systems, relief systems, shutdown procedures, emergency vents and disposal systems). The safety case should therefore describe the safety-related control measures including alarms designed to prevent or warn of excursions beyond safe operating limits.

182 The safety case shall also describe how chemical reaction hazards are evaluated and justify the sufficiency of the control measures to prevent runaway reaction, 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. In this respect, the safety case shall:

a) provide details of the physical parameters of possible conditions (i.e. flows, temperatures and pressures) with respect to excursions, runaway, worst case scenarios, etc.;
b) show that the design standards and other applied codes of practice are appropriate to the conditions under which the design must work;
c) demonstrate that hazard identification has covered the possibility of beyond design conditions; and
d) show that accident history for a type of plant has been considered where relevant.

183 MHIs should identify and describe the control measures to prevent operating outside the safe operating limit and show that these are fit for purpose. These measures include:

a) the safety-related controls and alarms designed to prevent or warn of excursions beyond safe operating limits and upon which the safety of the plant is based;
b) the pressure relief and emergency venting arrangements. The method for the sizing of the pressure relief and emergency venting shall be specified;
c) explosion relief;
d) occupied building risk assessment (OBRA);
e) interfaces with other measure designed to prevent excursions beyond safe operating limits such as:
    (i) shutting off feed streams;
    (ii) shutting off heat sources;
    (iii) adding inhibitors;
    (iv) dump systems;
    (v) inerting;
    (vi) flushing through of continuous processes;
    (vii) applying process cooling;
    (viii) operating vents;
    (ix) shutting down equipment; and
    (x) sprinklers or water deluge.

184 MHIs shall describe in the safety case whether interventions are automatic or manual. For intervention related to MASs (for new) or SCEs (for existing), 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.

Design key issue 8: safety-related control systems

185 MHIs shall describe the principles of how safety-related control systems have been designed to ensure safety and reliability. References could be made to relevant documents rather than providing detailed descriptions.

186 In this context, a control system or device is deemed to be safety critical if it provides functions which significantly reduce the risk of a hazard, and in combination with other risk reduction measures, reduces the overall risk to an ALARP level or if it is required to function to maintain or achieve a safe state for the equipment under control. It includes protective systems such as emergency shutdown systems, trips and interlocks.

187 MHIs shall show how the safety-related control systems will provide the required level of risk reduction, when related to the risk of a major accident and the reduction of risk achieved by other measures in place.

188 Evidence shall be provided in the safety case to show that the complete system (from sensor to final element, including software and the human interface) has been considered (e.g. Safety Integrity Level). This may include the use of accepted good practice, codes and standards, etc. It shall also show the appropriate application of redundancy, diversity, separation and segregation to safeguard against the risks of common cause failure. This shall include hardware, software and human interfaces.

189 MHIs shall explain how the following have been identified and accounted for in the design of the safety-related control systems:

a) safe operating limits and their relation to the set points for safety functions, including the selection of appropriate measurement instrumentation;
b) independence and separation from other systems or the initiating faults which require the operation of safety-related control systems. If the safety-related control systems are not separate from other equipment, the safety case shall show that failures of connected equipment cannot affect the safety function. It shall also show that single-point failures cannot result in the failure of both systems. If this is impossible, the connected equipment or system shall be regarded as being part of the safety-related control system;
c) operating conditions, including start-up and shutdown and unusual operating conditions, for example single train operation;
d) operating duty, including shut-off requirements for valves and how their performance will be affected by the presence of corrosive or erosive conditions;
e) inspection and maintenance requirements, including the provision of facilities for carrying out proof testing; and
f) environmental considerations, including requirements to operate in flammable atmospheres, equipment which requires special environments, prevention and consideration of electromagnetic interference and weather.

190 MHIs shall identify and describe support systems and backup measures for the control and protective systems, including their component parts, for example power supplies or pneumatic systems. Information shall be presented to show that support systems and backup measures have adequate safety and reliability.

Design key issue 9: human factors

191 MHIs should demonstrate a structured and systematic approach to managing human performance in the context of MAHs in the safety case. The approach should be 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 SCEs;
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 (PIFs) and introduces measures to optimise performance.

192 In addition MHIs should also demonstrate that 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 consequence of SCEs.

193 The human factor discipline covers a range of topics including:

a) ergonomics associated with the design of plant, equipment, working environment and tasks;
b) demonstration of the safety of any activities which rely primarily on human action; and
c) optimisation of organisational PIFs.

194 MHIs should demonstrate that human factors are integrated into the MAH risk assessment process and also show that the potential for dependency between successive human tasks has been recognised and accounted (e.g. different people doing the same task may make the same error).

195 MHIs should show how human factors have been accounted for in the design of equipment and in the operation, maintenance and modification of systems. Equipment or systems should be designed after consideration of how human failure can be reduced.

196 MHIs should show how systems which require human interaction have been designed to take into account the needs of the users, and that they are reliable. This includes manual control of systems, control room and interface design, and alarm handling.

197 Suitable evidence which MHIs can present in the safety case may include, for example:

a) consideration of how equipment design and the associated operating environment minimise human failures or improving equipment design to provide a more error tolerant system;
b) a description of procedures for activities requiring human interaction;
c) a description of training, including refresher training;
d) a description of staffing levels and supervision;
e) where a measure relies on human intervention, an explanation as to why human intervention has been selected in preference to an automated system; and

f) shift work and overtime arrangements to minimise fatigue.

Note: Refer to Appendix 5A on details of implementing Human Factors and its elements in safety case submissions.

Design key issue 10: systems for identifying locations where flammable substances could be present

198 MHIs shall describe the systems for identifying locations where flammable substances could be present and describe how the equipment has been designed to take account of the risk.

199 MHIs shall explain how potentially hazardous (flammable and explosive atmosphere) areas have been identified and classified. This may have been through an area classification study in which those areas where a risk exists, owing to the normal, occasional or accidental release of process materials to atmosphere, have been designated in accordance with recognised standards.

200 Sources of ignition for flammable atmospheres may include electrical equipment, naked flames or hot surfaces, and static electrical discharge. MHIs shall indicate how the likely sources of ignition have been considered in the design, for example:

a) electrical equipment selection for defined hazardous areas;
b) avoidance of hot surfaces or naked flames, or sparks associated with equipment, such as through the use of spark arrestors; and
c) control of static electrical build-up.

201 Radio-frequency (RF) radiation may cause an ignition hazard if present (e.g. RF equipment such as plasma enhanced chemical vapour deposition in the semiconductor industry). MHIs shall indicate whether there are strong radio transmitters in the vicinity, or whether the process includes devices which are particularly sensitive to RF radiation (e.g. manufacturing of explosive detonators).

202 Equipment selected for use in hazardous areas shall be suitable for use in these areas under all foreseeable operating conditions, including normal operation, start-up, shutdown, emergency, cleaning, or any other expected condition throughout the life of the installation.

5.3.3 Construction

5.3.3.1 Adequate safety in construction

203 MHIs shall show that the facilities have been constructed to appropriate standards at the time of construction to prevent major accidents or limit the consequences. For facilities already built, MHIs shall give assurance relating to the following sections if actual construction documents cannot be located. However for new facilities, construction documents used to demonstrate for the following sections shall be provided on request during assessment.

204 MHIs shall show that construction of plant and associated equipment is managed to ensure that it is built in accordance with the design intent. This can form part of the description of an MHI's 'management of change procedures'.

205 MHIs shall also show, wherever available, that the manufacture and construction of the facilities have employed appropriate materials and construction methods, to minimise the occurrence of defects or damage which might affect plant integrity. Evidence shall be provided by MHIs to show that the construction work has been carried out by suitable personnel in accordance with appropriate procedures.

206 There shall be a reference in the safety case to any relevant construction codes or standards which have been used. MHIs shall provide evidence on the adequacy of the procedures adopted if codes or standards have not been used or do not exist.

207 MHIs shall 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. Details shall be provided where significant nonconformities in manufacture have been identified, or where substantial remedial work has been carried out.

208 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.

209 MHIs shall describe how the construction of all plant and systems is assessed and verified against the appropriate standards to ensure adequate safety. The information provided shall show that the construction process has not compromised the design intent.

210 MHIs shall identify the key assessment and verification activities, and the stages at which they are undertaken. MHIs shall also provide an explanation and show how the methods used will ensure safety. The acceptance criteria for testing and examination programmes shall be identified, where appropriate. Suitable information might include:

a) how the required quality of work has been achieved;
b) hydraulic or pneumatic pressure testing of equipment, where this is a code requirement;
c) examination of engineering structures using appropriate non-destructive testing techniques;
d) leak testing to confirm the capability of containment to prevent liquid or gaseous leakage;
e) the mechanisms used to confirm the safety of all the elements of control systems, including valves, instruments, software, trips and alarms;
f) the role and competence of personnel used to verify compliance with code requirements; and
g) a reference to relevant quality assurance procedures.

211 MHIs shall provide information to show how commissioning phases are intended to be conducted to confirm safety provisions relating to plant design, operating limits and predicted performance. Procedures for managing the hazards associated with plant commissioning shall also be described.

212 MHIs shall describe the arrangement for managing outstanding issues or actions (e.g. punch lists) identified during the 'pre-handover' inspection after the construction, expansion or modification of installations. Residual issues classified as 'low risk' at the project handover stage (e.g. incomplete painting of pipework systems) may impact in-service integrity if timely remedial action is not taken.

5.3.4 Operation

5.3.4.1 Adequate safety during operation

213 MHIs shall show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions, including start-up, shutdown and abnormal operating conditions. Safe operating procedures shall also take into account how safe operating limits are not exceeded for all reasonably foreseeable conditions.

214 MHIs shall identify how reviews of operating procedures are undertaken and recorded, to take account of operational experience or changing conditions in the plant (SS506: Part 3 – 'Operating procedures and safe work practices' provide more details on this).

215 During the operational life of the plant there may be temporary constraints applied (e.g. the use of overrides and procedures covering abnormal operation, start-up and shutdown). MHIs shall show how these operational constraints are applied and managed, to ensure safety.

216 Information provided by MHIs on the management systems (see Chapter 3) will be relevant to show that adequate safety have been built into the operation of the installation. Any unit-specific management systems to ensure safety shall be provided in details in the safety case.

5.3.5 Maintenance

5.3.5.1 Adequate safety and reliability involving maintenance

217 MHIs shall show that an appropriate maintenance regime is established for plant and systems, to prevent major accidents or limit their consequences. The safety case shall also demonstrate that suitable inspection regimes are in place for equipment or machineries which contribute to the initiation, prevention and mitigation of SCEs. The typical contents of an inspection regime shall include the following and should be made available upon request:

a) identifications of the equipment or machineries within the system;
b) those parts of the system which are to be examined;
c) the nature of the examination required, including the inspection and testing to be carried out on any protective devices;
d) where appropriate, the nature of any examination needed before the system is first used;
e) the maximum interval between examinations;

f) the critical parts of the system which, if modified or repaired, should be examined by a competent person before the system is used again;
g) the name and position (where applicable) of the competent person approving the inspection regime; and
h) the date of the inspection.

218 MHIs shall show in the safety case that the maintenance procedures are sufficiently comprehensive (as in line with international and/or corporate best practices, vendor guidance, relevant standards and codes, etc.) to maintain the facilities in a safe state. MHIs shall also show that maintenance activities will not compromise the safety of the installation and that maintenance staff will not be exposed to unacceptable risks.

219 MHIs shall describe the organisation of maintenance activities. The general principles of roles and responsibilities, competence, employee participation and communication which shall be demonstrated are covered under SS506: Part 3. For maintenance systems, the following information shall be available:

a) fault reporting systems;
b) ranking and scheduling and ranking of routine maintenance activities; and
c) availability and deployment of suitable personnel and equipment.

220 MHIs shall identify those plant items and systems for which maintenance is considered to be a safety critical activity. Evidence shall be provided to justify the maintenance strategy adopted. The information presented may include:

a) arrangements for the periodic inspection and calibration of pressure relief devices;
b) the monitoring of internal corrosion, where this is a life-limiting feature;
c) the maintenance of utilities systems, for example electricity distribution, or ancillary equipment (e.g. pumps), where failure may lead directly to a hazardous situation;
d) the provision of installed spare equipment or spares in stock, where extended plant or system downtime could affect safety;
e) arrangements for the proof testing of all safety-related control system elements (e.g. sensors, transmitters, actuators, alarms, trips and confirmation of software modification). This is to reveal any faults which are not apparent during normal operation;
f) arrangements for the maintenance of control and instrumentation systems; and
g) inspection and maintenance of electrical earthing and lightning protection systems, particularly in a hazardous environment.

221 MHIs shall show that the impact of maintenance work on the safety of the installation has been adequately considered. Suitable evidence may describe, for example:

a) measures taken to ensure that the isolation of vessels will not compromise pressure relief systems;
b) the use of overrides or bypasses in safety systems; and
c) relevant safe work practices.

222 MHIs shall show that procedures and equipment are in place to ensure that plant is made safe before starting maintenance work and for the reinstatement of plant to the operating state after maintenance is properly managed. Appropriate information may include:

a) a description of the types of permit-to-work (PTW) system in use;
b) procedures and equipment used for the release of pressure, draining, isolation, purging and ventilating of plant, and the removal of temporary isolation following maintenance; and
c) auditing arrangements to ensure that the PTW system is being properly used.

223 The information shall include, where appropriate, reference to any maintenance records kept, or other relevant documentation. Where statutory pressure vessels are concerned, the safety case shall provide evidence that maintenance has been carried out and records have been kept in accordance with either the WSH (General Provisions) Regulations or with the Guidelines on Scheme for Extension of Statutory Examination Period of Pressure Vessels at Workplaces (if any).

Hazardous conditions

224 MHIs shall identify the procedures that are necessary to enable maintenance activities to be carried out safely to prevent an SCE. Safe work practices and method statements shall have been established to enable all activities which could result in dangerous situations to be identified. The information provided may refer to:

a) hazards posed by electrical equipment and the procedures for making safe;
b) hazards associated with hot work, procedures for assessing the risk, and testing for flammable gases; and
c) underground services, and procedures for keeping contractors informed about such services in the area where they are working.

225 MHIs shall identify which activities are subject to a PTW system and describe the key features of the systems in use on the installation. Suitable evidence shall show how controls and limitations are placed on the maintenance activity, such as safe work procedures, location of work, type of work, extent of work, competence of personnel, and time.

226 MHIs shall show how all personnel, including contractors, involved in maintenance activities are made aware of the conditions and limitations of the PTW system.

227 Where equipment has been certified by a third party (e.g. certified suitable for use in a flammable atmosphere), the safety case shall justify how the maintenance system ensures the level of safety of that equipment. For instance this can be done by maintaining to standards in accordance with manufacturers’ instructions.

Plant inspection

228 MHIs shall show that systems are in place to ensure that equipment of high safety concern and systems are examined at appropriate intervals by a competent person.

229 Examinations by a competent person at intervals may be necessary because certain specialised skills or equipment are required, or because it is required by specific legislation, for example, WSH (General Provisions) Regulations for statutory pressure vessels.

230 MHIs should provide information to show that any competent person employed has the appropriate training, knowledge, experience and degree of independence from the production activity.

231 MHIs shall describe how the plant and systems which are subject to examination by a competent person are selected, and the reasons for the selection.

232 MHIs shall outline and justify the interval between examinations by a competent person for the various types of equipment of high safety concern and systems. MHIs shall identify, in general terms, the examination techniques which are employed and provide suitable justification for their selection. MHIs shall also explain how examinations by a competent person are properly planned and considered.

233 MHIs shall identify any equipment of high safety concern or systems which are known to be susceptible to defects, which have been repaired, or where there is a history of failures. In such cases, evidence shall be presented to show adequate monitoring of the situation and to provide details of any replacement programme.

234 MHIs shall describe and justify the arrangements for reporting, recording and acting on the results of examinations by a competent person.

235 In the case of electrical equipment, there shall be evidence of examination programme for equipment provided for use in hazardous areas.

236 MHIs 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. MHIs shall describe how defects detected during maintenance or examinations are properly assessed by a competent person to determine their significance and appropriate action taken. In summary, appropriate information in the safety case shall include:

a) management responsibilities for ensuring that defects are assessed and that any necessary corrective action is taken;

b) the use of suitable assessment procedures, including references to published or company guidelines used to set defect acceptance levels; and

c) the competence of any person carrying out the assessment of defects, and undertaking any associated corrective action.

5.3.6 Modification and Decommissioning

5.3.6.1 Adequate safety involving modification and decommissioning

237 MHIs shall describe the systems in place for ensuring that modifications are adequately designed, installed and tested.

238 Management systems for change are described in detail under SS506: Part 3 (Management of Change). Modifications to processes and associated equipment, and structures, or to operations and procedures, which could affect the safety of the installation shall normally be subject to a formal modification system. This shall cover both hardware (e.g. pumps, piping arrangements and structures) and software (e.g. control system software and operating systems).

239 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.

240 The assessment and control over the modification process shall remain at the same standard for temporary arrangements. Temporary arrangements may require higher level of scrutiny where the nature of temporary plant is inherently less safe than permanent arrangements (e.g. the use of flexible hoses or connections, or 'site-run' piping in place of permanent fully designed hard-piped systems).

241 Throughout the lifetime of an MHI, there may be occasions requiring the decommissioning, mothballing and/or removal of plant or components, for example as part of a modification programme or as part of risk reduction through the removal of redundant plant. MHIs shall then identify significant decommissioned or mothballed plant and its relationship to the remaining related plant and systems. Removal or mothballing of such plant shall not lead to an increased risk associated with the use of the remaining plant and systems.

242 Particular care shall be given to ensuring the integrity of remaining related safety systems following the removal of plant, and such arrangements shall be included in the description of the change system. For example, this might include ensuring that:

a) sections of fire protection systems, such as deluge supplies to a pressure vessel, are not compromised by physical isolation following the removal of redundant sections of the firewater supply system;
b) shutdown systems are not compromised through computer software logic changes; and
c) levels of equipment protection have not been reduced through the decommissioning of selected instrumentation or utility services, etc.

5.4 Performance Standards and Indicators

243 MHIs are required to demonstrate in the safety case that performance standards and indicators (including safety indicators covered under SS506: Part 3) are implemented to provide the ongoing assurance that key systems relevant to major accidents are working well.

244 Performance standard is the acceptable level of response or the required performance for a control measure to be considered effective in managing the risk of SCEs. Standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe.

245 When selecting performance standards, the SMART principle (Specific, Measurable, Appropriate, Realistic and Timely) should be considered. Performance standards shall relate to the specific function performed by the control measure, and there may be more than one performance standard necessary for a single control measure. An example of performance standards for some control measures is as shown below in Table 3.

246 Performance standards shall be developed for equipment of high safety concern which are control measures for SCEs.

247 Performance indicators shall measure how well the management system is monitoring and maintaining the control measures. An example of the performance indicators for the relief valve management system is as shown below in Table 4.

248 Performance indicators and performance standards should enable MHIs to:

a) measure, monitor and test the effectiveness of each control measure;
b) take corrective action based on failure to meet the performance standard; and
c) generate performance management reports on the integrity of the MHI's control measures and how well they are being managed.

Control Measures	Performance Standard	Target
Pressure relief valve	Relief capacity	'x' kg/s
	Popping pressure tolerance	Within +/- 3% of set pressure for pressures above 70 psig in accordance to ASME BVPC Section VIII
	Reliability	98% function at set pressure
Operating procedure	Compliance check	0 major deviations <=1 minor deviation

Table 3: Example of performance standards and its corresponding metric/criteria

Note: The relief capacity is only required for the specification and purchase of the equipment. Once installed, the relief capacity is assumed to be correct provided the relief valve and piping is clear, no changes to the process have occurred and the relief valve is maintained.

Performance Indicator	Target
Percentage of relief valves tested within scheduled time	95%
Percentage reliability	98%
Number of pressure relief valves exceeding inspection interval by three months	‘x’ valves

Table 4: Example of performance indicators for relief valve management system

Note: Reliability is assessed as the percentage of failed valves (‘failed in dangerous state’) when tested.

Appendix 5A: Phased Implementation of Human Factors in Safety Case

249 MHIs are required to demonstrate that the risk assessments carried out to aid decision-making on the measures necessary to prevent major accidents or to mitigate their consequences, including the appropriate consideration of human factors. MHIs are allowed the flexibility to take a phased implementation approach towards human factors in their safety cases, based on the proportionality rule and selected elements of human factors (elements detailed in Human Factor Assessment Guide) shall be implemented within three submission cycles. The phased implementation approach has to be justified and outlined in the MHI's safety case in the form of a human factors implementation roadmap, indicating the milestones to be achieved.

250 It is recommended that MHIs take one of these, or similar approaches:

a) Facilities or work processes where human factors are crucial in preventing major accidents are first addressed while the remaining systems are listed to be implemented by stated due dates, as part of the MHI's human factors implementation plan.

b) Identification of all safety critical tasks at the MHI are first conducted while the analysis for the potential for human failure and the appropriate risk control measures to optimise performance are documented in an implementation plan with due dates.

c) Human factors deficiencies identified during risk assessment process are reviewed and addressed in risk reduction improvement plan. Additional elements of human factors as per the Human Factor Assessment Guide may be implemented in accordance with the MHI's human factors implementation plan.

An example of a human factors implementation roadmap developed based on a risk-based approach is shown in the next section. MHIs have flexibility to develop their own human factors implementation roadmap.

Appendix 5B: Sample Human Factors Implementation Roadmap (Risk-Based Approach)

S/No	Topic	SC Submission Cycle			Remarks
		Cycle 1	Cycle 2	Cycle 3	
1	**Human Failure Prevention**				
1.1	**Task & Human Failure Analysis of human actions for Safety Critical Tasks**				
1.1.a	Initiation	Y	Y	Y	
1.1.b	Prevention		Y	Y	
1.1.c	Mitigation			Y	
1.2	**Maintenance Activities**		Y	Y	
2	**Ergonomics Design of Facilities, Working Environment and Tasks**				
2.1	HF integrated in MHI's MOC and design processes		Y	Y	Cycle 1 implementation for major modifications/ new projects
2.2	HF in work environment design		Y	Y	
2.3	Alarm handling		Y	Y	
3	**Optimisation of Organisational Performance Influencing Factors**				
3.1	Management of Organisation Change		Y	Y	Cycle 1 implementation for major modifications/ new projects
3.2	Shift Staffing level		Y	Y	
3.3	Fatigue Management		Y	Y	
3.4	Communication & Shift Handover	Y	Y	Y	
3.5	Site supervision		Y	Y	
3.6	Incident investigation covering Human Factors		Y	Y	

Chapter 6: Emergency Response Aspects of Safety Case

6.1 Introduction

251 This chapter covers the information that shall be provided in the safety case about the range of emergency response measures implemented to respond to major accidents. These include resources which can be mobilised (e.g. fire-fighting equipment) for mitigation and the provision for clean-up.

252 This chapter should preferably be prepared by the person responsible for the MHI's emergency response. He should consult the relevant subject matter experts to fulfil the requirements in this chapter.

253 MHIs should include the detailed operation of the emergency response measures in the emergency response plan which shall also be submitted as an annex with the safety case.

254 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 (in particular, the representative set of MASs) described elsewhere in the safety case.

255 The emergency preparedness and response forms part of the SHMS and could follow the management model described in Chapter 3. It is described again in this chapter to provide an overview of emergency response.

256 This chapter also deals with resources (i.e. human resources and equipment) that can be mobilised but are not engineering control measures relating to facilities which are detailed in Chapter 5. However, MHIs may like to deal with these resources together in safety case.

257 The safety case shall also provide, wherever relevant, the list of applicable regulations, standards and codes of practice that have been followed. Demonstration of compliance with these will help MHD in the assessment of the safety case.

258 MHIs shall review the contents of the emergency response plan annually and update them if there are any changes in the MHIs, within the emergency services concerned or if some new technical knowledge is adopted in emergency planning.

6.2 Summarising the Emergency Response Measures That have been used to draw up the Emergency Response Plan

259 The summary should cover:

a) equipment and systems installed in the plant to limit the consequences of a major accident;
b) organisation, arrangements and provisions for the alerting and intervening in the event of a major accident;
c) on-site and off-site resources that can be mobilised;
d) maintenance and inspection;
e) training for emergency response and
f) testing of emergency response.

6.2.1 Equipment and system installed in the plant to limit the consequences of a major accident

260 MHIs will need to describe the fixed equipment and systems installed in the plant that limit the consequences of major accidents and how these equipment and systems support emergency response activities (e.g. emergency shutdown arrangements, secondary containment systems fitted with an isolation device). This shall include the extent of manual intervention required. A description of such equipment or systems and their design and maintenance will generally be included with the information described in Chapter 5.

6.2.2 Organisation, arrangements and provisions for alerting and intervening in the event of a major accident

261 The safety case shall describe the organisation for alerting and intervening in the event of a major accident. The description could include the following if they are relevant to MASs on-site:

a) the functions of key posts and groups with duties in the emergency response and the arrangements for deputies, for example:
   (i) the posts authorised to set the emergency procedures in motion and the conditions for doing so;
   (ii) the contact details of the Site Incident Controller (SIC) responsible for the coordination of the on-site containment action;
   (iii) the contact details of the Site Main Controller (SMC) responsible for liaising with external emergency services (e.g. SCDF, SPF, NEA); and
   (iv) the role of any specialist groups required under the emergency response plans. Some examples are Company Emergency Response Team (CERT), process engineers to give advice on the risks from the processes or substances involved.
b) the arrangements for informing individuals on-site, neighbouring facilities, where relevant:
   (i) the different types of alarms and the plant conditions required to activate them; and
   (ii) the initial actions required in response to alarms and warnings.

c) the arrangements and conditions for alerting and mobilising:
   (i) individuals or groups with defined responsibilities under the emergency response plans (e.g. CERT), including essential personnel on-site and off-site;
   (ii) the emergency services (e.g. SCDF, SPF);
   (iii) neighbouring installations, which may be affected by the off-site effects from the incident or where mutual aid agreements exist and
   (iv) external agencies (e.g. NEA, JTC).

d) 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.

e) where relevant, the provision that has been made for monitoring wind speed and direction, and other environmental conditions, where applicable in the event of a major accident;

f) provisions for establishing and maintaining communications during the emergency response;

g) the nature of and arrangements for maintaining any mutual aid agreements with nearby installations (e.g. provision of equipment and human resources, first aid and specialised medical services);

h) the nature and location of any facilities which may require special protection;

i) the nature and location of any facilities which may require special rescue operation;

j) 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) IPP facilities;
   (iv) sheltering buildings;
   (v) evacuation assembly area;
   (vi) predefined control points (e.g. staging point, assembly areas) along with any identified secondary, back up locations and
   (vii) any other relevant items.

k) the location of access routes for emergency services, rescue routes, escape routes, and any restricted areas;

l) occupancy load of occupied areas during peak and non-peak periods;

m) evacuation arrangements and any transport requirements, with considerations given to persons with disability;

n) headcount roll call and search and rescue arrangements;

o) conditions for and 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;

p) nature and location of any pollution control devices and materials and

q) consideration of the effects of emergency response actions, including fire-fighting activities, to minimise the overall impact on people and the vicinity. This should include short-term and long-term effects, and alternative options for disposal or discharge of released chemicals.

6.2.3 On-site and off-site resources that can be mobilised

262 The safety case shall describe the on-site and off-site resources which can be mobilised. The description should be in sufficient detail and relate to MASs described elsewhere in the safety case. In this way, MHIs should be able to demonstrate that there are necessary and suitable resources available to contribute to the overall measures necessary to limit the consequences of a major accident to people and to the vicinity.

263 In providing this information, the safety case shall include the available resources:

a) located on-site;
b) located at neighbouring facilities with which mutual aid agreements may exist; and
c) which can be brought in by the MHI from elsewhere.

264 The safety case shall explain how the emergency response will be complementary to and coordinated with existing roles of SCDF.

265 This information shall cover the key issues listed here, where appropriate. The following paragraphs provide more detail about the type of information that MHD is looking for:

a) human resources;
b) hardware fit for purpose when called upon;
c) personal protective equipment;
d) fire-fighting and fire protection;
e) minimising the release and limiting the consequence of dangerous substances;
f) monitoring and sampling;
g) provisions for clean-up;
h) first aid and medical treatment; and
i) ancillary equipment.

6.2.3.1 Resources that can be mobilised: human resources

266 The safety case shall indicate the personnel that can be made available within appropriate timescales to carry out the containment actions required by the emergency response plan.

267 The safety case shall show, relating to the conditions in the MHIs, that:

a) the various functions required to implement the emergency response have been identified, and included in the emergency response plans and supporting procedures where appropriate, for example, SMC, SIC, Fire Safety Manager (FSM), operations staff, engineering and maintenance teams, riggers, drivers, medical staff, special technical experts such as chemists and toxicologists, CERT, and spillage treatment teams;
b) the number of people (including third parties) with the appropriate expertise and training, required to achieve the necessary level of response have been determined, and that these staff can be assembled within the necessary response time;

c) containment actions are achievable in practice, particularly in the early stages of the incident, given the rate at which the accident could escalate; and

d) there are contingencies if the 'decision makers' such as key appointment holders are incapacitated.

6.2.3.2 Resources that can be mobilised: hardware fit for purpose when called upon

268 The safety case shall show that there are appropriate arrangements to ensure that equipment is fit for purpose in the event of the major accidents that were identified as reasonably foreseeable.

269 The safety case shall describe, wherever relevant, that:

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) equipment is capable of operating in the ambient conditions, (e.g. the equipment has where necessary adequate weather protection);

c) equipment is capable of operating in the conditions expected to be experienced during a major accident;

d) 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);

e) possibility of losing essential services, such as power, water, communications and other facilities, has been taken into account and alternatives provided where necessary;

f) emergency equipment provided is compatible where necessary with that of the SCDF (e.g. SCDF mobile water monitors, foam concentrate) and that of organisations with which a mutual aid agreement exists by the provision of adapters where appropriate and

g) electrical equipment used in the emergency response is suitably protected for the foreseeable environmental conditions, so that its use does not introduce additional hazards.

6.2.3.3 Resources that can be mobilised: personal protective equipment

270 The safety case shall show that suitable and sufficient personal protective equipment (PPE) are readily accessible in the event of a major accident, and that their specifications are appropriate to the range of containing actions required of the response team.

271 There should be information about whether suitable and sufficient PPE is readily accessible to other individuals not directly involved in dealing with the emergency response, who may be required to wear it (e.g. emergency escape respirators for site personnel in the event of a toxic gas release).

272 The description of the PPE provisions shall include, where relevant, respirators, breathing apparatus sets and protective clothing for radiant heat or specific chemical hazards.

6.2.3.4 Resources that can be mobilised: fire-fighting and fire protection

273 If the identified MASs include the possibility of fire, the safety case shall justify that suitable and sufficient on-site fire-fighting and fire protection provisions can be mobilised in the event of a major accident. MHIs should take account of resources available from other organisations with mutual aid agreements, where applicable.

274 MHIs shall show that the quantity and specifications of the on-site fire-fighting provisions are adequate for the MASs that have been identified in Chapter 4.

275 Where MHIs can foresee circumstances that make the use of fire-fighting or other containing measures impracticable or unsafe (e.g. it may be unsafe to fight certain fires involving explosives), the safety case shall show that there are arrangements to identify those circumstances. MHIs should also give details of the additional arrangements necessary to limit the consequences of a major accident.

276 The description in the safety case shall include the following to help make the demonstrations about the MHIs' ability to limit the consequences of a major accident, where applicable:

a) that fire-fighting roles of the on-site personnel (e.g. full-time on-site fire brigade, auxiliary fire fighters, and other site personnel), during an emergency are defined and are appropriate;
b) that fire-fighting roles of CERT are complementary to the role of SCDF;
c) that quantity and specification of on–site fire-fighting equipment is sufficient;
d) that 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) that 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 is appropriate);
h) that 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 incompatible substances (e.g. hazardous substances that may react violently with water) which may require additional mitigation measures to limit the consequence of a major accident.

6.2.3.5 Resources that can be mobilised: minimising the release and limiting the consequences of dangerous substances

277 The safety case shall show that suitable and sufficient provisions can be mobilised to minimise the release of and mitigate the consequences of major accidents related to toxic or flammable substances.

278 These actions may be covered by normal operating procedures but the safety case shall still show that MHIs have considered the practicability of carrying them out in the foreseeable accident conditions and that MHIs have the appropriate equipment, tools and PPE that would be required.

279 The safety case shall refer to any provisions to reduce the evolution of toxic or flammable vapours from spilled hazardous material and to reduce the effects of its vapours.

280 The safety case could identify any resources which may be required, such as:

a) equipment that will be used to terminate or reduce the leak at source, such as patching or plugging of leaks in lines and vessels, the closure of valves and the isolation of sections of plant by blinding or blanking off;
b) 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 and
c) floating booms for immiscible lighter-than-water products that have entered the water, including controlled waters, where applicable.

281 The safety case shall describe any provisions for treating and removing spilled material. These provisions might include mobile pumps, and special chemicals and other materials for neutralising or absorbing the spillage.

6.2.3.6 Resources that can be mobilised: monitoring and sampling

282 The safety case shall show that there are suitable and sufficient provisions for on-site monitoring or sampling, wherever necessary, which can be mobilised in the event of a major accident.

283 The safety case shall identify the purpose of the monitoring and sampling provisions and explain how the results might influence decisions concerning the emergency response.

284 The need for monitoring or sampling depends on factors such as the type of hazardous substance involved, the rate at which it might disperse to safe levels and the speed at which the results can be obtained.

285 Provisions for monitoring and sampling might include the monitoring of oxygen levels, combustible gases and airborne toxic substances on-site and off-site and taking of samples from air, water and ground. The analysis could be carried out using portable analytical equipment or static or mobile laboratories.

286 The safety case should refer to any special technical expertise and other provisions required to analyse or interpret the results, as well as how those sampling and monitoring measures can help with emergency response.

6.2.3.7 Resources that can be mobilised: provisions for clean up

287 The safety case shall describe the provisions that have been made for clean-up of the environment and which are suitable and sufficient for the MASs identified in the safety case.

288 The safety case could 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).

289 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.

6.2.3.8 Resources that can be mobilised: decontamination, first aid and medical treatment

290 The safety case shall show that there are suitable and sufficient provisions 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 to hospital as quickly as possible, such as those who have been exposed to toxic substances. 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.

291 This could be achieved by discussing:

a) the number and availability of first aiders;
b) facilities available at the MHI;
c) confirming both the expectations and limits of the first aiders training;
d) relevant information any hazard specific medical treatment that MHI has catered for;
e) liaison with SCDF could be described, making references to how the MHI’s casualty control or decontamination strategies have been determined.

6.2.3.9 Resources that can be mobilised: ancillary equipment

292 The safety case should 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

293 Examples of ancillary equipment include vehicles or vessels to transport emergency equipment to and from the site of the accident, heavy lifting gear, earth-moving equipment, emergency lighting, and special tools and parts required to carry out emergency repairs and actions.

294 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.

6.2.4 Maintenance and inspection

295 The safety case shall show that suitable arrangements have been made for the maintenance, inspection, and testing of resources and other equipment to be used during the emergency response.

296 The arrangements shall cover equipment used for containment, fire-fighting, as well as other equipment with a key function such as alarms to warn personnel of the accident. The information provided should demonstrate that specific equipment is included in relevant plant maintenance inspection and operations schedules, records, procedures, instructions, etc.

6.2.5 Training for emergency response

297 The safety case shall show that suitable arrangements have been made for training individuals on-site in the emergency response in compliance with the guidelines laid out in the National CERT Standard.

298 The training shall cover those members of staff with specific roles in the event of a major accident, as well as providing the training and information for other employees, contractors and visitors to the site. The safety case could also outline the type of information that is provided during such training.

6.2.6 Testing of emergency response plan

299 The safety case shall describe the arrangements in place to validate the emergency response plans at all levels (e.g. local plant response, the site-wide response and the interface with SCDF). The different shift patterns should also be included in the tests.

300 MHIs need to describe the arrangements for integrating the lessons learnt from these exercises when revising the emergency response plans, where necessary.

6.3 Summarising the Elements that have to be included in the Emergency Response Plan

301 The MHIs shall follow the SCDF template which can be found in "**General Guidelines for Emergency Response Plan"** on the SCDF website as the baseline requirement for the emergency response plan. The emergency response plan shall include all relevant information outlined in this chapter. The emergency response plan shall be submitted together with the safety case.

302 The following considerations are useful in assessing the adequacy of an emergency response plan:

a) The incidents considered shall be planned according to the representative major accidents identified including off-site consequences from neighbouring premises encroaching into the premises.
b) Have the consequences of the various incidents considered been adequately addressed?
c) Are there sufficient resources in terms of personnel and equipment in the MHI available at all times, to carry out the emergency plan for the various incidents in conjunction with SCDF?
d) Have the timescales been assessed adequately?
e) Is there a logical sequence of actions for the key personnel that are identified and given a role in the emergency response plan?
f) Has suitable consultation taken place with the relevant stakeholders who are involved in the development of the emergency response plan?
g) Are these plans communicated to relevant persons working in MHIs?
h) Are arrangements in place to cover emergency response round the clock?

Chapter 7: ALARP Demonstration

7.1 Introduction

303 This technical guide has provided a broad overview on the concept of demonstration in Section 1.4. This chapter will further deal with ALARP demonstration in a safety case to ensure that risks arising from MAHs in MHIs are reduced to ALARP levels.

304 In a safety case, MHIs are required to show, through reasoned and supported arguments, that all practicable control measures that can be reasonably implemented have been implemented to reduce the risk for SCEs (i.e. all necessary measures). The adopted control measures for any identified SCE shall be shown to collectively eliminate or reduce the risk to health and safety to ALARP levels. The approach employed in providing evidence of ALARP demonstration within a safety case is at the MHI's discretion. In practice, a combination of approaches are likely to be necessary and this chapter attempts to provide clarity of the possible approaches while not limiting the possible options available for any MHI's ALARP demonstration.

305 It is expected that each MHI's safety case will be different, but each safety case has to feature ALARP demonstration. Sufficient information has to be provided to make the link between identified SCEs and ALARP demonstration of the control measures implemented to prevent major accidents or limit their consequences.

306 Risk Reduction Measures are control measures which includes both preventive and mitigative measures that are specific to the SCEs used in ALARP demonstration.

7.2 Key Concepts Underpinning ALARP Demonstration Principle

307 **Risk** – Risks span across a spectrum from very low to very high. The greater the unmitigated risk (risk without consideration of existing control measures) under consideration, the greater the degree of rigour required to demonstrate that risks have been reduced to as low as is reasonably practicable. Proportionality should drive depth of risk analysis, the time, cost and trouble expended on reducing risk and the on-going resources allocated during operations to manage risk. Level of rigour should be proportionate to:

a) the scale and nature of the MAHs assessed, based on the installations and activities within it, and
b) the risks posed to people.

308 **Reasonable practicability** – In the context of risk, practicability is whether a control measure can be implemented based on current technological capabilities. However, **sacrifices** (in money, time and/or effort) would bring into perspective the reasonableness of implementing a control measure. Hence, determining whether SCE risks have been reduced to ALARP involves an assessment of risk to be reduced, an assessment of the sacrifice involved in implementing control measures to reduce that risk and a comparison of the two (risk reduced or avoided and sacrifice). The basis on which the comparison is made involves the test of '**gross disproportion'**.

309 **Gross disproportion** – When risks are reduced, there are benefits derived, such as safer workplace, no loss of lives and increased productivity. The benefits are a result of the risk reduction as sacrifice (i.e. a combination of money, time, effort, etc.) has been made to implement a control measure. When more sacrifices are made, the risk is reduced further. However, there is a point or region where any incremental sacrifice to implement more control measures does not derive significant additional benefit. At this point or region, risk reduction is considered ALARP and further measures to reduce the risk can be ruled out.

310 The comparison to judge gross disproportion between sacrifice and benefit gained is always in the favour of safety. Demonstrations that the cost of implementation is grossly disproportionate shall be proportionate to the level of risk reduction required.

311 **Inherently safer design** – It is good practice to apply the principles of prevention as a hierarchy:

a) Eliminate risk by removing the hazard;
b) Substitute a hazard with a less hazardous one;
c) Prevent potential events;
d) Separate people from the consequences of potential events;
e) Reduce the magnitude and likelihood of an event;
f) Mitigate the impact of a major accident on people and emergency response.

312 MHIs are strongly encouraged to apply these general principles in a hierarchical manner and implement a combination of these principles as they see fit in the life cycle of the installation to prevent major accidents or limit their consequences.

313 **Choosing between options** – For new MHIs or brown-field redevelopment projects, a selection among options may be needed not only at the design stage but at any stage in any project where opportunities arise, which will involve making a choice between differing design concepts for the project as a whole. In making choices, MHIs shall consider the risks associated over the whole life cycle of a project. However, it is expected that a new installation would not give rise to a residual level of risk greater than that achieved by existing good practice for similar functions. The reasonable practicability of any further risk reduction shall be measured against this baseline. Safety cases shall show that the lowest risk option has been selected in all cases, or the reason for selecting the higher risk option is ALARP.

314 **Good practice** – This is taken to refer to any well-defined and established standard or codes of practice adopted by an industrial or occupational sector, including ‘learnings’ from incidents that may yet to be incorporated into standards. Good practice generally represents a preferred approach; however it is not the only approach that may be taken. While good practice informs, it neither constrains nor substitutes for the need for professional judgement. Good practice may change over time because of technical innovation or because of increased knowledge and understanding.

315 **Reverse ALARP** – The practice of using QRA, cost benefit analysis (CBA) or other risk assessment methodology to justify not implementing a good practice for new projects or removal of an existing control measure in existing facilities that achieves only a small level of risk reduction compared to the potential high benefit gained, is termed ‘Reverse ALARP’. It uses the assessments to show that cost of a measure is grossly disproportionate to the benefit gained (as compared to level of risk reduction) and hence, the continued implementation of the control measure is not reasonably practicable. Such reverse ALARP justifications are <u>not acceptable</u> as it contradicts the ALARP principle. Similar practice of Reverse ALARP is not acceptable for new projects.

316 **Risk uncertainty** – It is expected that risk related decision should be made with sufficient certainty and understanding of both the likelihood and the consequence of a SCE occurring. Where there is significant uncertainty which leads to a wide range of risk outcomes, sensitivity analysis on the effects of the range of input parameters should be carried out.

317 **Precautionary approach** – Uncertainties in risk are replaced by conservative assumptions (e.g. worst case) resulting in risk reduction measures being more likely to be implemented. MHIs shall use precautionary approach where there are greater levels of uncertainty in the determined consequence or likelihood (e.g. from the use of new technology, disagreement in opinions or limited relevant industry standards or the consequences of the SCE give rise to significant off-site risks). In cases where uncertainties are present, risk reduction measures shall take more precedence over the economic considerations by MHIs.

318 It might not be reasonably practicable to apply retrospectively to existing MHIs for example, all the good practice expected for a new MHI. However, there may still be ways to reduce the risk e.g. by partial solutions.

319 ALARP is reasonably practicable, not reasonably affordable: justifiable cost and effort is not determined by the budget constraints or viability of the project.

7.3 What are the Fundamental Approaches to Consider for ALARP Demonstration?

320 There is no prescribed methodology for demonstrating that the necessary control measures have been and will continue to be identified to reduce risks to ALARP. However, there are several basic approaches which may be used to support an MHI's provision of evidence and justification within the safety case. MHIs could consider using one or more of these approaches as appropriate to their installation. In practice, it is likely that most MHIs will require a combination of approaches.

321 The ALARP argument may be qualitative and focus on relevant good practices and sound engineering principles. Several sources of good practice and engineering principles exist which are in order of precedence:

a) prescriptive legislation;
b) regulatory guidance;
c) standards produced by standard-making organisations;
d) guidance agreed by an organisation representing a particular sector of industry and
e) good practice adopted by a particular sector of industry.

322 If good practice and engineering principles are used as the sole justification of ALARP, the MHI shall demonstrate that:

a) the good practice and engineering principles are relevant to the MHI's situation;
b) any adopted standard shall be up-to-date and relevant (in particular for new projects and modifications, refer to the most current as at the time of implementation);
c) where a standard allows for more than one option for conformity, the chosen option makes the risks ALARP and
d) the good practice and engineering principles reduce the risk to an acceptable level.

323 In some situations it is not sufficient to assume that applying current good practice and engineering principles will ensure that the risks are ALARP, unless for example the risk is well understood and uncertainty is minimal. Where relevant, qualitative and/or quantitative arguments shall be presented in order to provide the justification that all necessary measures have been taken (see Paragraphs 324 to 327 below for more details).

324 In setting out to provide evidence that the risks are reduced to a level that is ALARP, it is a fundamental requirement to show the clear link between the MAH identification and risk assessments and the measures taken to make the risks ALARP. The MAH identification and risk assessments carried out in Chapter 4 provide the foundation on which to base the control measure selection. The following approaches may be considered:

a) **Hazard and risk criteria approach** – define criteria that is considered to correspond to 'reducing risk to a level that is ALARP', assess performance quantitatively or qualitatively (using matrices for example) and compare against the criteria (corporate or internal risk tolerance criteria).

b) **Comparative assessment of risks, costs and benefits** – evaluate risk and associated costs for a range of control measure options for the MHI and compare the relative merits of the different options, selecting the options which are practicable.

c) **Cost benefit analysis (CBA)** – the numerical assessment of the costs of implementing a design change or modification and the likely reduction in risk that this would be expected to achieve. CBA may be used in cases where it is difficult to determine whether the cost is justified after completing risk assessments of sufficient rigour. The UK HSE website[8] provides an in-depth explanation on the uses and limitations of using CBA for ALARP decision making. MHIs using CBA shall ensure that all data and assumptions are justified in the safety case.

d) **Comparison with good practices, codes and standards** – compare design, the management system framework and operational procedures against recognised national, international or industry standards, codes of practice, guides, etc. The basis and implementation of the management system, including operations and maintenance systems, should be audited against good practice for process units, or relevant similar industries.

e) **Technical analysis** – evaluate control measures in technical terms; assess strengths and weaknesses, e.g. effectiveness, functionality, availability, reliability, technical feasibility, compatibility, survivability, correspondence of control measures to hazards and risks, appropriateness of performance standards.

f) **Performance data** – evaluate safety-related performance data for MAS as evidence of adequacy or satisfactory levels of performance, e.g. data on the operational effectiveness or reliability of a control measure may support the demonstration of its appropriateness for that service.

g) **Improvement approach** – demonstrates the extent of relative improvements in performance for the MHI based on past, present and planned modifications and enhancements.

h) **Judgement approach** – present considered judgements of suitability and adequacy of control measures and the management systems, or the perceptions of a cross-section of various stakeholders, e.g. key members of the workforce, senior management, plus independent observers.

i) **Practical tests** – demonstrate that the management system and/or control measures function effectively, using MAS simulations, management system tests, equipment breakdown and recovery tests, etc. For example, it may be possible to conduct fire impingement tests to show that fire rating of the material being used is appropriate.

325 Decisions on the requirement for additional risk reduction to bring down levels to ALARP should be made by competent persons.

326 The output from the ALARP demonstration should be a list of the risk reduction measures considered for each SCE, with a conclusion as to whether it is to be implemented or not. If it is to be implemented, it should form part of an action plan, including responsibilities, accountabilities and timescale. Otherwise, the reasons should be documented and justified on the basis of reasoned argument.

---

[8] http://www.hse.gov.uk/risk/theory/alarpcheck.htm

327 For safety case acceptance purposes, the MHI's approach on ALARP demonstration will be evaluated in terms of its robustness, transparency and appropriateness to its installation. MHIs shall therefore define the underlying rationale, criteria and decision-making basis for the case. The description shall be convincing; this means that the rationale for deciding the completeness of the hazard identification and the adequacy of the risk reduction 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, MAHs and the control measures.

7.4 Critical Success Factors

328 MHIs are expected to address at least the following specific factors in their consideration of ALARP in the safety case submission:

a) Timeliness. For the case of new MHI or new projects and brownfield developments, the earlier an MHI starts undertaking an ALARP evaluation, the greater the ability to reduce risks to a level that is ALARP.
b) Safety case content that is consistent with the requirements specified in the WSH (MHI) Regulations.
c) Involvement of people who know the MHI or a very similar operation. This includes (but not limited to) managers, operators, contractors, subject matter experts.
d) Access to a wide range of reference material such as standards, safety alerts, etc.
e) Description with a sufficient level of detail that explains the means by which the MHI ensures suitability of the design, construction, installation, operation, maintenance or modification that is appropriate to the MHI.
f) A transparent and robust presentation of evidence showing that the adopted control measures reduce risk to ALARP.
g) A transparent and robust presentation of evidence that the SHMS provides for and will continue to provide for reduction of risk to ALARP, and that the SHMS is comprehensive and integrated.

7.5 Summary of Factors in Selecting or Rejecting Risk Reduction Measures

329 Multiple factors come into play when selecting or rejecting risk reduction measures for ALARP demonstration. Table 5 below lists some of the common factors to consider when demonstrating ALARP.

Methodology for understanding controls	Points to consider
Control Measure Selection Hierarchy • Inherent safety • Prevention measures • Mitigation measures	• Is there an option higher up the hierarchy that would more effectively eliminate or manage the hazard? • Where appropriate, is there a spread of controls across the hierarchy?
Types of Control Measure • Technical (Hardware, software) • Other (SHMS, Procedural)	• Is there an appropriate spread of technical and other controls?
Common Mode Failures	• Have failure modes been identified for each control measure and then compared to common mode failures?
Layers of Protection • Design Standards • Control Systems • Operating Procedures • Safety Devices • Emergency Systems	• Are the layers of protection provided adequate for the level of risk posed by the hazard?
Operating Circumstances • Environment • Operating conditions • Activities being carried out	• Have the controls been assessed for effectiveness over the range of different operating circumstances they may have to operate in?
Focus of Control Measure	• Does the relative importance or vulnerability of the control measure justify a higher depth of scrutiny than others?
Effective • Functionality • Availability • Reliability • Survivability (Refer to Chapter 5)	• Has the functionality, availability and reliability been established for control measures? • Has survivability been considered for utilities? • Have means of improving these aspects been considered?
ALARP	• Has each risk reduction measure been assessed for reasonable practicability, and those found reasonably practicable been implemented while those found to be not reasonable practicable noted as such with sufficient justification?

Table 5: Summary of Factors in Selecting or Rejecting Risk Reduction Measures

7.6 ALARP Demonstration Examples

[Note: The following examples use a combination of approaches to guide decision-making in relation to risks. These are included as an illustration only and are not required to be prescriptively followed. Do note that following such a model can provide guiding principles for an MHI's ALARP demonstration but does not necessarily lead to reducing risks to ALARP levels.]

Example: Application of a decision-making model using a combination of approaches

330 The UK offshore oil and gas industry has developed a framework to assist risk-related decision making ("Oil & Gas UK", formerly UKOOA, 2014), which helps decision-makers choose an appropriate basis for their decisions. A summary of the framework is shown in Figure 2 below.

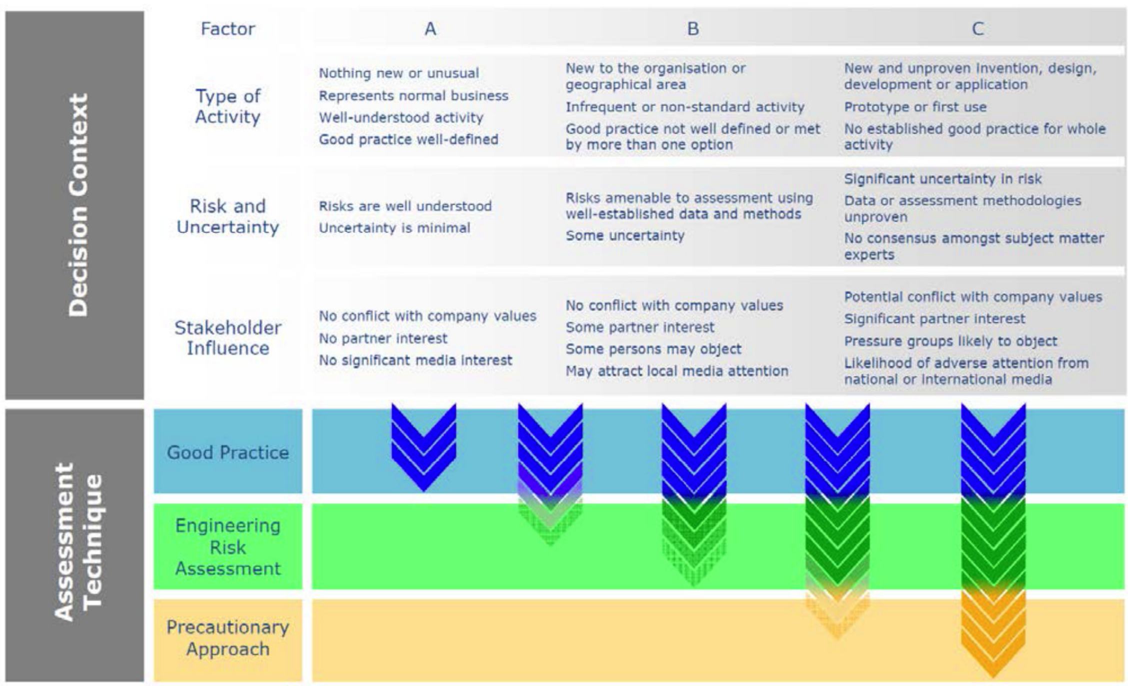


Figure 2: Risk-related decision support framework (Oil & Gas UK, 2014)

331 The framework takes the form of three different decision contexts (A, B & C). The first step in the decision-making process is to determine the decision context (i.e. the combination of circumstances, knowledge and events within which the decision is to be made) based on these factors: activity type, risk & uncertainty and stakeholder influence. The assessment techniques used will depend on the selected decision context. The chevrons shown in Figure 2 show the assessment techniques likely to be needed to make an ALARP decision. More details about this framework are provided in the Oil & Gas UK Guidelines.

332 This approach shows that good practice would predominantly influence Type A decisions. In cases where good practices are not sufficiently well-defined or available, engineering risk assessments may be required to guide the decision. Engineering risk assessment and good practice would have major inputs to Type B decisions involving infrequent non-standard

activities, deviation from standard practice, some risk uncertainty, etc. Type C decision context identifies the need for a precautionary approach in the decision-making based on significant uncertainty in risk, unproven or novel design, conflict of values, etc. For Type C, relevant good practice and detailed engineering risk assessment will still be used to support the decision.

333 As an additional caution, MHIs who are making Type A decisions that rely predominantly on codes and standards as a decision basis shall ensure they truly understand how the codes and standards act to minimise risks. Without this knowledge it is difficult to identify when change (planned or otherwise) will undermine the effectiveness of that standard or code as a control measure.

334 **Should an MHI choose to adopt this framework, it is advisable to make reference to the Oil & Gas UK Guidelines for details on the use of the framework.**

335 Table 6 below gives an application of the framework for illustration purposes: three facilities, three different outcomes.

MHI	1	2	3
Scenario	Standard temperature and pressure pipeline conveying a hydrocarbon with a flash point above 60^0C, with no known unique environmental concerns that could exacerbate a MAS relating to this pipeline.	The MHI has installed new hydrocarbon processing equipment. There is nothing new or unusual about the equipment or process but this is the first of this type that has been installed and operated by the MHI.	MHI with novel technologies and complex hydrocarbon processing equipment that requires frequent monitoring during the initial start-up phase of operations. The MHI has a large number of personnel on-site and is located in the vicinity of other MHIs processing hydrocarbons.
Decision Type	Nothing new or unusual, corporate and industry codes cover this application extensively. The best design, installation and maintenance approaches are known and well-established over many years. **The decision is type A.**	Hydrocarbon processing facilities are not novel but they are new to this MHI and thus deviate from established company practice. Qualified engineering judgement and some risk based assessment will be required to determine that the design is ALARP. **The decision type is B.**	Some new and novel technologies are utilised and the number of potentially exposed personnel is high. The impacts from any loss of containment are potentially very high and could lead to domino impacts. A precautionary approach to decision making is required. **The decision is type C.**
Risk Reduction Measures	Good practice approach – Standard control measures specified in design codes and adopted on the existing infrastructure are put in place.	Good practice approach coupled with engineering risk assessment – Standard control measures put in place for processing facilities and decisions made regarding increased monitoring and inspection.	Precautionary approach – This decision type means that much more effort is expended on examining risk reduction options and proving the design is ALARP.

Table 6: Illustration on use of Oil & Gas UK Decision Framework

336 **UK HSE's guidance provided other alternative framework for ALARP demonstration. Should an MHI choose to adopt this framework, it is advisable to make reference to UK HSE's Guidance on ALARP Decisions for details on the use of the framework**.[9]

[9] http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/

Acknowledgements

The Major Hazards Department (MHD) would like to thank all members of the Safety Case Joint Government-Industry Work Group (SC JWG) for dedicating their time and efforts in providing inputs, reviews, technical advices and encouragement throughout the preparation of this Safety Case Technical Guide and the accompanying Safety Case Assessment Guide.

MHD would also like to express appreciation to stakeholders of the MHI industry for their feedback and support.

The SC JWG consists of the following members:

	Name	**Capacity**
Co-Chair:	Mdm Jaime Lim	Ministry of Manpower
Co-Chair:	Mr Amit Bhatnagar	Singapore Refining Company Private Limited
Secretary:	Mr Marcus Soh	Singapore Chemical Industry Council
Members:	Mr Evert Klein	ExxonMobil Asia Pacific Pte Ltd
	Mr Low Wai Hoe	ExxonMobil Asia Pacific Pte Ltd
	Ms Gloria Wang	Shell Eastern Petroleum Pte Ltd
	Mr Randy Cha	Ministry of Manpower
	Ms Jacqueline Liew	Ministry of Manpower
	Mr Soh Zi Quan	Ministry of Manpower
	Mr Lim Eng Wee	Ministry of Manpower
	Mr Oh Hong Jia	Ministry of Manpower
	Ms Lynnette Goh	Ministry of Manpower
	Mr Chui Jian Wei	Ministry of Manpower
	Mr Chen Fu Yi	National Environment Agency
	LTC Ng Geok Meng	Singapore Civil Defence Force
	MAJ Lo Wai Mun	Singapore Civil Defence Force
	CPT Teo Soon Chye	Singapore Civil Defence Force
	CPT Matthew Goh	Singapore Civil Defence Force

References

In the preparation of this Safety Case Technical Guide, references were made to the following publications:

1. SS506 Part 3: Requirements for the chemical industry
2. UK HSE HSG 190: Preparing safety reports: Control of Major Accident Hazards Regulations 1999 (COMAH)
3. COMAH 2015 Safety Report Assessment Manual
4. L111: The Control Of Major Accident Hazards Regulations 2015
5. L138: Dangerous Substances and Explosive Atmospheres
6. UK HSE Guidance on ALARP Decisions in COMAH
7. NOPSEMA ALARP Guidance note N-04300-GN0166 Rev.6 June 2015 (https://www.nopsema.gov.au/assets/Guidance-notes/N-04300-GN0166-ALARP.pdf)
8. Safe Work Australia Guide for Major Hazard Facilities: Safety Assessment