

DIN EN ISO 17776

ICS 75.180.10

Einsprüche bis 2015-09-03
Vorgesehen als Ersatz für
DIN EN ISO 17776:2003-09

Entwurf

**Erdöl- und Erdgasindustrie –
Offshore-Produktionsanlagen –
Management der Gefährdungen durch schwere Störfälle bei der
Konstruktion neuer Offshore-Anlagen; (ISO/DIS 17776:2015);
Englische Fassung prEN ISO 17776:2015**

Petroleum and natural gas industries –

Offshore production installations –

Major Accident hazard management during the design of new installations;
(ISO/DIS 17776:2015);

English version prEN ISO 17776:2015

Industries du pétrole et du gaz naturel –

Installations des plates-formes en mer –

Lignes directrices relatives aux outils et techniques pour l'identification et l'évaluation des
risques; (ISO/DIS 17776:2015);

Version anglaise prEN ISO 17776:2015

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-07-03 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an noeg@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Erdöl- und Erdgasgewinnung (NÖG), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 107 Seiten

DIN-Normenausschuss Erdöl- und Erdgasgewinnung (NÖG)

Nationales Vorwort

Dieses Dokument (prEN ISO 17776:2015) wurde vom Technischen Komitee ISO/TC 67 „Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries“ Subkomitee SC 6 „Processing equipment and systems“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 12 „Materialien, Ausrüstungen und Offshore-Bauwerke für die Erdöl-, petrochemische und Erdgasindustrie“ (Sekretariat AFNOR, Frankreich) erarbeitet.

Für Deutschland hat hieran der Arbeitskreis NA 109-00-01-06 AK „Verfahrenstechnische Anlagen und Ausrüstungen“ im DIN-Normenausschuss Erdöl- und Erdgasgewinnung (NÖG) mitgearbeitet.

Dieser europäische Norm-Entwurf enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO Norm.

Dieser Norm-Entwurf enthält neben den gesetzlichen Einheiten auch die Einheit „in (inch)“ die in Deutschland nicht zugelassen ist. Es wird ausdrücklich darauf hingewiesen, dass die Anwendung dieser Einheit im nationalen amtlichen und geschäftlichen Verkehr aufgrund des Gesetzes über Einheiten im Messwesen nicht zulässig ist. Die Angabe dieser Einheit dient lediglich als Hilfe im amtlichen und geschäftlichen Verkehr (z. B. bei Einfuhr und Ausfuhr) mit solchen Staaten, die diese Einheit anwenden.

Umrechnung:

Nicht-SI-Einheit	SI-Einheit	Umrechnung
in (inch)	mm	1 inch = 25,4 mm

Änderungen

Gegenüber DIN EN ISO 17776:2003-09 wurden folgende Änderungen vorgenommen:

- a) neuer Abschnitt 2 „Normative references“;
- b) neuer Abschnitt 4 „Major Accident hazard management overview“;
- c) neuer Abschnitt 5 „Management of Major Accident hazards in design“;
- d) neuer Abschnitt 6 „Screening and concept selection process“;
- e) neuer Abschnitt 7 „Concept definition and optimisation“;
- f) neuer Abschnitt 8 „Detailed design and construction phase“;
- g) neuer Abschnitt 9 „Major Accident hazard management in operation“;
- h) neuer informativer Anhang A „Plan to manage Major Accident hazards“;
- i) neuer informativer Anhang B „Major Accident hazard management identification and evaluation tools“;
- j) neuer informativer Anhang C „Strategy for managing major accident hazards“;
- k) neuer informativer Anhang D „Barrier system performance standards“;
- l) neuer informativer Anhang E „Oil & Gas UK – Framework for risk-related decision support“;
- m) neuer informativer Anhang F „HAZID guidewords“.

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

Die Benummerung der folgenden Begriffe und Abkürzungen sind identisch mit der Benummerung in der englischen Fassung.

3.1 Begriffe

3.1.1

Sperre

Barriere

trennende Schutzvorrichtungen oder Einrichtungen zur Kontrolle/Überwachung in einer so ausgewählten funktionellen Anordnung, dass die Realisierung einer Gefährdung verhindert wird

Anmerkung 1 zum Begriff: Sperren können passive, aktive oder verfahrensmäßige Mittel/Maßnahmen sein, die inhärent sicher konstruiert sind.

Anmerkung 2 zum Begriff: Übernommen aus IOGP 415.

3.1.1.1

Sperren-Element

physikalische, technische oder betriebliche Komponente eines Sperren-Systems

3.1.1.2

Sperren-Funktion

Funktion, die zur Verhinderung, Kontrolle oder Abmilderung unerwünschter oder unfallbedingter Ereignisse vorgesehen ist

3.1.1.3

Sperren-Management

allgemeine Benennung für koordinierte Aktivitäten zur Einrichtung und Beibehaltung von Sperren, die jederzeit funktionsfähig sind

3.1.2

Kontrolle

Überwachung

Begrenzung der Ausdehnung bzw. Dauer eines Gefährdungsereignisses

Anmerkung 1 zum Begriff: Diese Definition gilt für die vorliegende Internationale Norm; in anderen Normen werden andere Definitionen angewendet.

3.1.3

Notfallreaktion

von der Besatzung innerhalb oder außerhalb der Offshore-Plattform durchgeführte Maßnahmen zur Überwachung oder Eindämmung eines schweren Störfalls (MA) oder zur Initiierung und Durchführung des Verlassens der Plattform

3.1.4

Umwelt

Umgebung, in der eine Organisation tätig ist, einschließlich Luft, Wasser, Land, natürlicher Ressourcen, Flora, Fauna, Menschen und deren Wechselbeziehung

3.1.5**Umweltbeeinflussung**

alle der Umwelt zu- oder abträglichen Veränderungen, die ganz oder teilweise auf die Aktivitäten, Produkte oder Dienstleistungen einer Organisation zurückgeführt werden können

3.1.6**Rettungsweg****Fluchtweg**

Weg zu einer Stelle, an der sich die Besatzung sammelt oder zu einem Bereich, von dem aus die Plattform in einem Notfall verlassen werden kann

3.1.7**Evakuierung**

planmäßiges Verfahren zum Verlassen der Plattform in einem Notfall

3.1.8**Schaden**

Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Eigentum/Besitz oder der Umwelt

[QUELLE: ISO/IEC Richtlinie 51:2014]

3.1.9**Gefährdung**

potenzielle Schadensquelle

[QUELLE: ISO/IEC Richtlinie 51:2014]

3.1.10**Gefährdungseignis**

Ereignis, das zu einem Schaden führen kann

[QUELLE: ISO/IEC Richtlinie 51:2014]

3.1.11**Einzelrisiko****individuelles Risiko**

Risiko, dem ein Individuum während einer bestimmten Zeit ausgesetzt ist

3.1.12**inhärent sichere Konstruktion**

Auslegung, bei der Gefährdungen durch einen schweren Störfall eliminiert oder reduziert werden, indem dauerhafte und in die Konstruktion integrierte Maßnahmen angewendet werden

3.1.13**schwerer Störfall****schwerer Unfall****MA**

Gefährdungseignis,

- das mehrere Tote oder Schwerverletzte oder
- umfangreiche Schäden an Bauwerken, Plattformen oder Anlagen zur Folge hat oder
- das signifikant umweltschädliche Auswirkungen hat (z. B. bleibende und schwere Umweltschäden, die zu einem Verlust der kommerziellen Nutzung oder der Freizeitnutzung oder zu einem Verlust der natürlichen Ressourcen in einem weiten Bereich oder zu schweren Umweltschäden führen können, die umfangreiche Maßnahmen erfordern, um eine erneute Nutznießung der Umwelt zu ermöglichen)

Anmerkung 1 zum Begriff: In dieser Internationalen Norm ist ein „schwerer Störfall“ das Ergebnis der Realisierung einer „schweren Gefährdung“.

Anmerkung 2 zum Begriff: Es ist vorgesehen, dass diese Definition weitere Benennungen einbezieht, z. B. „schwerer Störfall“, definiert in UK HSE.

[QUELLE: IOGP Bericht Nr 456]

3.1.14

schwere Gefährdung

Gefährdung, die das Potenzial besitzt, bei ihrer Realisierung zu einem „schweren Unfall“ zu führen

3.1.15

Abmilderung

Eindämmung

Begrenzung der Auswirkungen eines Gefährdungsereignisses

Anmerkung 1 zum Begriff: Diese Definition gilt für die vorliegende Internationale Norm; in anderen Normen werden andere Definitionen angewendet.

3.1.16

Sammelplatz

gekennzeichneter Bereich, an dem die Besatzung auf eine entsprechende Anforderung in einem Notfall antritt

3.1.17

Leistungsmaßstab

Leistungsanforderungen

Angabe der von einem System, einem Teil der Ausrüstung, einer Person oder einem Verfahren geforderten Leistung, die als Grundlage für das Management dient

Anmerkung 1 zum Begriff: Leistungsanforderungen gelten für aktive und passive Sperren.

Anmerkung 2 zum Begriff: Leistungsanforderungen können als qualitative oder als quantitative Bedingungen angegeben werden.

Anmerkung 3 zum Begriff: Leistungsanforderungen für Sperren betreffen die Funktionalität, die Zuverlässigkeit, die Überlebensfähigkeit und die wechselseitige Abhängigkeit von Sperren unter Notfallbedingungen.

3.1.18

Risiko

Kombination aus der Wahrscheinlichkeit eines Schadensereignisses und der Schwere dieses Schadens

[QUELLE: ISO/IEC Richtlinie 51:2014]

3.1.19

Risiko-Toleranzkriterien

qualitative oder quantitative Kriterien zur Angabe eines Risikogrades, der als Obergrenze anzusehen ist, um für die jeweilige Aktivität oder das jeweilige Vorhaben tragbar zu sein

3.1.20

Not-Zufluchtsort

TR

Stelle, an der die Besatzung für eine bestimmte Dauer Schutz finden kann, während Untersuchungen durchgeführt sowie Notfallreaktionen und die Evakuierung geplant werden

3.1.21

tragbares Risiko

in einem gegebenen Zusammenhang basierend auf den gegenwärtigen gesellschaftlichen Wertvorstellungen akzeptiertes Risiko

[QUELLE: ISO/IEC Richtlinie 51:2014]

3.2 Abkürzungen

CFD	Numerische Fluidodynamik (en: computational fluid dynamics)
EER	Flucht, Evakuierung und Rettung (en: escape, evacuation and rescue)
ER	Notfallreaktion (en: emergency response)
ESD	Notabschaltung; Not-Aus; Notabspernung (en: emergency shutdown)
F&G	Feuer und Gas (en: fire and gas)
HAZID	Gefahrenerkennung (en: hazard identification)
HAZOP	Gefahren- und Durchführbarkeitsstudie (en: hazard and operability study)
IOGP	Internationaler Verband der Erdöl- und Erdgasproduzenten (en: International Association of Oil & Gas Producers)
ISD	Inhärent sichere Konstruktion (en: inherently safer design)
LOPA	Analyse der Schutzebenen (en: layer of protection analysis)
MA	Schwerer Störfall; schwerer Unfall (en: Major Accident)
MOC	Management von Veränderungen (en: management of change)
P&ID	Rohrleitungs- und Instrumentierungsdiagramm (en: piping and instrument diagram)
PFD	Versagenswahrscheinlichkeit bei Anforderung (en: probability of failure on demand)
QRA	Quantitative Gefahrenanalyse (en: quantitative risk analysis)
TR	Not-Zufluchtsort (en: temporary refuge)

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	4
4 Major Accident hazard management overview	5
4.1 General	5
4.2 Project management commitment.....	6
4.3 Project management accountability.....	6
4.4 Project plan to manage Major Accident hazards	6
4.5 Objectives of Major Accident hazard management	7
4.6 Selection of hazard evaluation and risk assessment methods	7
4.7 Good practice	8
4.8 Documentation	8
4.9 Actions management	9
4.10 Management of change.....	10
5 Management of Major Accident hazards in design.....	10
5.1 Overview of MA hazard management.....	10
5.2 Key concepts and tools	13
6 Screening and concept selection process	18
6.1 General	18
6.2 Objectives	19
6.3 Functional requirements.....	19
7 Concept definition and optimisation	22
7.1 General	22
7.2 Objectives	23
7.3 Functional requirements.....	23
8 Detailed design and construction phase	28
8.1 General	28
8.2 Objectives	29
8.3 Functional requirements.....	29
9 Major Accident hazard management in operation	34
9.1 General	34
9.2 Objectives	34
9.3 Functional requirements.....	35
Annex A (informative) Plan to manage Major Accident hazards	38
A.1 General	38
A.2 Scope of the plan.....	38
A.3 Basis for the plan	38
A.4 Regulatory compliance.....	38
A.5 Primary codes and standards	38
A.6 Goals and criteria	39
A.7 Project organization	39
A.8 Responsibilities, leadership and commitment.....	39
A.9 Contracting arrangements	40

A.10	Procurement integrity	40
A.11	Study programme and timing	40
A.12	Arrangements for action management.....	40
A.13	Arrangements for integrity assurance and verification.....	40
A.14	Overview of timing of key deliverables	40
Annex B (informative)	Major Accident hazard management identification and evaluation tools	43
B.1	Hazard identification (HAZID)	43
B.2	Explosion hazard analysis	45
B.3	Fire hazard analysis	47
B.4	Smoke and gas dispersion and ingress analysis.....	48
B.5	Escape, evacuation and rescue (EER) analysis	50
B.6	Temporary refuge (TR) impairment analysis	53
B.7	Dropped object assessment.....	54
B.8	Ship collision assessment.....	57
B.9	Failure mode, effects and criticality analysis (FMECA)	58
B.10	Reliability/survivability analysis of emergency systems	60
B.11	Risk Analysis.....	62
B.12	Hazard and operability (HAZOP) study	64
B.13	Integrity analysis of instrumented systems.....	65
B.14	Analysis of human factors	67
B.15	Environmental risk assessment.....	69
B.16	Terms of reference.....	70
Annex C (informative)	Strategy for managing major accident hazards.....	72
C.1	Inherently safer design (ISD)	72
C.2	Barriers	73
Annex D (informative)	Barrier system performance standards.....	76
D.1	Performance standards for barriers	76
D.2	Design performance standards accountability	77
D.3	Verification of design standards	77
D.4	Operations performance standards.....	77
D.5	Inspection, testing and maintenance.....	77
Annex E (informative)	Oil & Gas UK — Framework for risk-related decision support.....	78
Annex F (informative)	HAZID guidewords.....	79
Bibliography		95

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

The committee responsible for this document is Technical Committee ISO/TC 67, *Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries*, Subcommittee SC 6, *Processing equipment and systems*.

This second edition cancels and replaces the first edition (ISO 17776:2000), which has been technically revised and the title changed from *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment* to the present title.

Introduction

The purpose of this International Standard is to establish requirements and provide guidance for the effective management of Major Accident (MA) hazards during the design of new offshore installations for the petrochemical and natural gas industries.

The management of MA hazards involves the application of engineering expertise and knowledge to provide the measures needed to meet the objectives set by the organizations involved in the project development. A range of tools for evaluating and assessing the likelihood and consequences of MAs is needed to help select measures to be implemented and to judge when sufficient measures have been provided.

This process is built on the underlying integrity provided by the application of internationally recognised codes and standards.

This International Standard covers the following main elements:

- establishing general requirements for identifying MA hazards and their causes;
- evaluating MA hazards to understand their likelihood and possible consequences;
- developing suitable strategies for managing MA hazards;
- progressively improving the understanding of MA hazards and their consequences to guide design decisions during the development phases of the installation;
- providing the measures needed to manage a MA;
- maintaining the measures throughout the life of the installation.

This International Standard should be read in conjunction with ISO 13702 and ISO 15544.

Petroleum and natural gas industries — Offshore production installations — Major Accident hazard management during the design of new installations

1 Scope

This International Standard describes processes for managing Major Accident (MA) hazards associated with the design and operation of offshore oil and gas production installations. It provides requirements and guidance on the development of strategies both to prevent the occurrence of MAs and to control and mitigate the possible consequences.

This International Standard is applicable to the design of

- fixed offshore structures, and
- floating systems for production, storage and offloading

for the petroleum and natural gas industries.

The scope includes all MA hazards with the potential to have a material effect on personnel, assets and the environment.

This International Standard is intended for large capital projects related to offshore operating installations. However, the principles are also applicable to small or simple projects or design changes to existing facilities, and can also be relevant to onshore production facilities.

This International Standard is not applicable to mobile offshore units and subsea installations, although many of the principles contained in this International Standard can be used as guidance. It does not cover the construction, commissioning, abandonment or security risks associated with offshore installations.

The decision to apply the requirements and guidance of this International Standard, in full or in part, is intended to be based on an assessment of the likelihood and possible consequences of MA hazards.

The technical content of this International Standard is arranged as follows:

- a) Objectives: the goals to be achieved;
- b) Functional requirements: activities considered necessary to meet the stated objectives;
- c) Annexes: guidelines in support of the functional requirements.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 31000, *Risk management — Principles and guidelines*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms, definitions and abbreviated terms apply.

3.1 Terms and definitions

3.1.1

barrier

functional grouping of safeguards or controls selected to prevent the realisation of a hazard

Note 1 to entry: A barrier may be a passive, active or procedural measure and includes inherently safer design measures.

Note 2 to entry: Adapted from IOGP 415.

3.1.1.1

barrier element

physical, technical or operational component in a barrier system

3.1.1.2

barrier function

function intended to prevent, control, or mitigate undesired or accidental events

3.1.1.3

barrier management

general term to cover the coordinated activities to establish and maintain barriers such that they at all times maintain their function

3.1.2

control

limiting the extent or duration of a hazardous event

Note 1 to entry: This definition is applied to this International Standard; alternative definitions are used in other standards.

3.1.3

emergency response

action taken by personnel on or off an installation to control or mitigate a Major Accident or initiate and execute abandonment

3.1.4

environment

surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans and their interrelation

3.1.5

environmental impact

any change to the environment, whether adverse or beneficial, wholly or partially resulting from an organization's activities, products or services

3.1.6

escape route

route leading to the place where people muster, or to an area from which people can leave the installation in an emergency

3.1.7

evacuation

planned method of leaving the installation in an emergency

3.1.8

harm

injury or damage to the health of people, or damage to property or the environment

[ISO/IEC Guide 51:2014]

3.1.9

hazard

potential source of harm

[ISO/IEC Guide 51:2014]

3.1.10

hazardous event

event that can cause harm

[ISO/IEC Guide 51:2014]

3.1.11

individual risk

risk to which an individual is exposed during a defined period of time

3.1.12

inherently safer design

design which eliminates or reduces Major Accident hazards through measures that are permanent and inseparable from the design

3.1.13

Major Accident

MA

hazardous event that results in

- multiple fatalities or severe injuries; or
- extensive damage to structure, installation or plant; or
- large-scale impact on the environment (e.g. persistent and severe environmental damage that can lead to loss of commercial or recreational use, loss of natural resources over a wide area or severe environmental damage that will require extensive measures to restore beneficial uses of the environment)

Note 1 to entry: In this International Standard, a Major Accident is the outcome of realisation of a major hazard.

Note 2 to entry: This definition is intended to incorporate terms such as “Major Accident” as defined by UK HSE.

Source: IOGP Report No. 456.

3.1.14

major hazard

hazard with the potential, if realized, to result in a Major Accident

3.1.15

mitigation

limitation of the effects of a hazardous event

Note 1 to entry: This definition is applied to this International Standard; alternative definitions are used in other standards.

3.1.16

muster area

designated area to which personnel report when required to do so

3.1.17

performance standard

statement of the performance required of a system, item of equipment, person or procedure, and used as the basis for its management

Note 1 to entry: Performance standards are applied to active and passive barriers.

Note 2 to entry: Performance Standards can be expressed in qualitative or quantitative terms.

Note 3 to entry: Barrier performance standards address the functionality, reliability, survivability and interdependency of barriers under emergency conditions.

3.1.18

risk

combination of the probability of occurrence of harm and the severity of that harm

[ISO/IEC Guide 51:2014]

3.1.19

risk tolerance criteria

qualitative or quantitative criteria used to express a risk level that is considered as the upper limit in order for the activity or undertaking to be tolerable

3.1.20

temporary refuge

TR

place provided where personnel can take refuge for a predetermined period while investigations, emergency response and evacuation preparations are undertaken

3.1.21

tolerable risk

level of risk that is accepted in a given context based on the current values of society

[ISO/IEC Guide 51:2014]

3.2 Abbreviated terms

CFD	computational fluid dynamics
EER	escape, evacuation and rescue
ER	emergency response
ESD	emergency shutdown
F&G	fire and gas
HAZID	hazard identification
HAZOP	hazard and operability study
IOGP	International Association of Oil & Gas Producers
ISD	inherently safer design

LOPA	layer of protection analysis
MA	Major Accident
MOC	management of change
P&ID	piping and instrument diagram
PFD	probability of failure on demand
QRA	quantitative risk analysis
TR	temporary refuge

4 Major Accident hazard management overview

4.1 General

The process to manage MA hazards shall align with the principles and framework set out in ISO/IEC 31000, and shall

- establish the context prior to starting or executing any of the elements of the process;
- update the context throughout the process;
- apply a thorough process for communicating, consulting, monitoring and review.

In developing the context for managing MA hazards, 'lessons learned' from other organizations, accident reports and general safety bulletins made available for public review shall be taken into account where these identify additional hazards, additional measures, or highlight deficiencies in the current measures for the management of MA hazards on offshore installations. This is part of a continual improvement effort which requires users to seek opportunities for improving their designs on a continual basis.

A process to manage MA hazards shall be applied throughout all stages of a project. Designs shall be regularly reviewed during their development and changed as necessary to achieve the strategies developed to meet the defined objectives and risk criteria.

Modifications to an existing installation shall be conducted under an appropriate management of change (MOC) process. To assess how any modification can change the likelihood or consequences of an MA, a good understanding is needed of the existing MA hazards and any new MA hazards introduced by the change. It is also necessary to understand the effectiveness of the current strategies to manage the existing MA hazards, in order to avoid compromising design measures already implemented to reduce risk.

If strategies for managing the MA hazards are not available, the requirements and guidance provided in this International Standard shall be used to identify the existing MA hazards and develop suitable strategies to manage them.

The outcome of this process is the measures necessary to manage each type of MA hazard for the life cycle of the installation. In order to determine the most effective range of design measures, a systematic analysis, using a range of tools and techniques, is needed to evaluate the likelihood and consequences of each identified MA hazard.

An integral part of decision-making is a framework which allows judgement of when the risks to human beings, the environment and assets are reduced to a tolerable level. Effective decision-making requires a transparent process which promotes dialogue and engagement with stakeholders to assist in identifying where improvements can be made in managing MA hazards.

4.2 Project management commitment

Project managers shall establish a broad view of the context of the proposed project and the associated risks to people, the structure, installation or plant and the environment over the lifetime of installation and beyond.

To ensure effective implementation of the process of managing MA hazards, the project management shall

- establish the context for the project, such as key development parameters and expectations of stakeholders;
- highlight the importance of managing MA hazards within the overall project objectives, and include stakeholders in the development of the objectives;
- establish and communicate objectives for managing MA hazards and risk to those involved, both internally and externally (in some jurisdictions these may be written into legislation);
- define the decision-making process related to managing MA hazards, including who is authorised to make decisions and the criteria to be used;
- develop the organization of the project team, with clear roles and responsibilities for managing MA hazards for all key personnel, including lead discipline engineers;
- make competent and sufficient engineering resources available to the project team (including safety and other technical disciplines needed to deliver the MA hazard management objectives);
- provide sufficient time and resources for managing MA hazards, particularly taking account of the iterative nature of the process;
- implement the measures which result from the process to manage MA hazards;
- define how the process for managing MA hazards and the outcomes will be documented.

4.3 Project management accountability

The project management shall be accountable for the effective implementation of the process for managing MA hazards across all contributors to the work, including design contractors, equipment/system suppliers and service providers. The project management shall endeavour to ensure that any such contracted organizations understand the requirements and are competent to conduct the specified tasks.

The lead safety engineer in the project organization shall be capable of specifying and commissioning work necessary for evaluating MA hazards and performing risk assessments. Where appropriate, that work may be supported by external consultants. The project management shall develop the terms of reference for the work, and shall decide how the results are to be used to manage any MA hazards.

4.4 Project plan to manage Major Accident hazards

The process to manage potential MA hazards for each of the design development stages shall be set out in a plan. This shall define the project-specific objectives needed to manage MA hazards and the criteria to judge their tolerability. The plan shall set out the key activities and when they shall be conducted in order to allow timely implementation of suitable MA hazard management measures.

The plan to manage MA hazards shall be developed at the earliest reasonable opportunity, updated for the start of each new phase in the project development and as required to accommodate new events and information. Further details can be found in Annex A.

4.5 Objectives of Major Accident hazard management

Many competent organizations define objectives, standards and criteria for managing MA hazards. In addition, some regulatory authorities also define minimum standards for specific types of incidents, and these can include criteria for tolerable risk.

Irrespective of whether such objectives, standards and criteria have been defined by regulation or the owner, the project management team, with the support of the lead safety engineer and other disciplines' engineers, shall define the specific objectives and criteria for MA hazard management which are applicable to the project or installation.

Suitable objectives, and any criteria that are needed to support them, shall address the following:

- eliminating or avoiding MA hazards where it is reasonable to do so;
- designing for maximum credible life of the installation without the need for extensive inspection, maintenance or operational activities;
- reducing the likelihood of MAs by providing facilities that can meet the full operational envelope, including foreseeable upset conditions;
- reducing the likelihood of MAs by providing the functionality to safely allow all foreseeable operational and maintenance activities;
- preventing escalation so that small incidents or problems do not lead to MAs;
- limiting the extent and duration of any MAs that do occur;
- providing protection for personnel on board while emergency response is undertaken and, if necessary, evacuation is planned.

4.6 Selection of hazard evaluation and risk assessment methods

The lead safety engineer is responsible for selection of appropriate methods for hazard evaluation and risk assessment. The methods chosen shall be dependent upon factors such as the size and complexity of the installation, the types of major hazard, the severity of the MA consequences, the degree of uncertainty, the level of risk, the number of personnel exposed to the risk and the proximity of environmentally sensitive areas.

The type of hazard evaluation and risk assessment performed may vary depending upon the scale of the installation and the life cycle phase when the analysis is undertaken. For example:

- for simple installations, such as wellhead platforms and other small platforms with limited process facilities, checklists based upon previous risk assessments of similar installations and operations may allow a consistent approach to MA hazard management which relies on conformance with applicable codes and standards;
- for new installations which are a repeat of earlier designs, the evaluations undertaken for the original design may be used providing they meet current objectives, standards and criteria, new knowledge and technology and they adequately cover any significant differences from the earlier installation which can affect the management of MA hazards. In some cases, the earlier hazard management work may be deemed sufficient or may mean that only limited new work is needed;
- complex installations, such as large production platforms with complex processing facilities, drilling modules and accommodation, shall always use a structured process for MA hazard management;
- for installations in the early design phase, evaluations will necessarily be less detailed than those undertaken during later design phases.

4.7 Good practice

An integral part of MA hazard management is the application of recognized and accepted good engineering practice within the project team, primary contractors, sub-contractors and suppliers. Although these may not specifically be defined in codes and standards, it is the generic term for recognised risk management practices and measures that are used by competent organizations to manage well-understood MA hazards arising from their activities. It involves a combination of competence, implementation of standards (both internal and external) for managing MA hazards, learning from past experience (own and others) and generally acting in a way which reduces risks.

Guidance for such risk-related decision-making is available in reference [35]. This document illustrates the relative importance of good practice, engineering risk assessment or a more precautionary approach in making risk-related decisions. The precautionary approach is applied when available engineering and scientific evidence about the MA is insufficient, inconclusive or uncertain. This will mean that more conservative assumptions are applied and make it more likely that a safety measure is implemented.

4.8 Documentation

4.8.1 General

The process for managing MA hazards within a project shall be documented, in order to provide a clear record of activities that have been undertaken to

- explain the strategies for managing MA hazards and how they reduce risk,
- demonstrate that the MA hazard management objectives and risk-tolerability criteria have been achieved, with an audit trail to the appropriate supporting documentation.

To achieve this, documentation shall

- a) identify all MA hazards and the evaluation of potential consequences of any MAs;
- b) document the design strategies for managing MA hazards and the reasoning used to develop them;
- c) document key decisions made during the development of design strategies for managing MA hazards;
- d) describe the approach taken to risk assessment, and how uncertainties have been taken into account;
- e) report the risk assessed, and when necessary calculated, for the design. This shall detail the contributions from each identified MA hazard;
- f) identify the range of barriers implemented (including ISD measures) and why they are considered sufficient;
- g) define design and operations performance standards for each of the barriers (including ISD measures);
- h) demonstrate that the emergency response arrangements are appropriate;
- i) describe how engagement and input from operational and technical staff has been managed;
- j) describe why the design is considered suitable for operation
- k) describe the role of operating procedures and practices in maintaining MA hazard management and risk provisions.

Reports which define the purpose, scope, methodology used and the outcome of each activity shall be included or referenced. This includes all formal studies for identification and evaluation of major hazards and related MAs.

The documentation shall be subject to formal review by the Pproject management team to provide assurance that objectives have been achieved. External acceptance can also be required by local legislation.

The documentation is intended primarily for the information of the technical and operational teams who will be operating and modifying the installation. In some jurisdictions, a 'Safety Case' or Major Hazards Report that includes this type of documentation is a legal requirement.

The project management team shall ensure that an effective system records and tracks MA hazard management activities, and that the records are available for reference by the project and in the operational phase.

4.8.2 Register of Major Accident hazards

A register of MA hazards shall be prepared to summarise the following:

- all the MA hazards identified;
- the identified initiating mechanisms (i.e. failure modes or causes);
- the potential consequences of MAs, including the escalation potential;
- the primary design measures for inherently safer design;
- the barriers provided for prevention, detection, control and mitigation of MAs;
- the primary design measures for protection of escape routes, the temporary refuge, muster locations, evacuation facilities and the associated structural supports;
- reference to the barrier performance standards and safety-critical tasks necessary to maintain them;
- requirements to verify barrier performance standards;
- reference to supporting evaluation/study reports.

4.9 Actions management

A defined management process is required to ensure effective close-out for actions arising from the various formal design review and study activities. Actions shall be defined, recorded in a clear and actionable manner, and closed out or rejected in a systematic way.

The process shall include as a minimum:

- raising, vetting and recording of actions in a consistent and systematic manner;
- identifying the ownership of actions and preparation of responses;
- identifying responsibilities and authorisation for verification of close-out or rejection.

Requirements for managing actions shall also be applied to the primary contractors, and secondary contractors and vendors where applicable.

By the end of the project phases, all actions that could be resolved by design shall be closed in the manner defined by the actions management process. Any actions remaining for operation teams to resolve shall be documented and formally handed over.

4.10 Management of change

Changes are an ongoing feature of projects and installations. A policy and formal system for managing changes that could have an impact on design strategies for managing MA hazards shall be established. Although the details of MOC are outside the scope of this International Standard, it is essential that a formal MOC process be established.

During the early stages of the project development, a less formal MOC approach may be established to ensure that MA hazard management is considered when changes are proposed. For this to be successful, all design personnel need to be made aware of the developing design strategies for managing MA hazards, and encouraged to seek a review by the appropriate technical specialists (including safety engineering).

A formal MOC system shall be introduced at the appropriate phase in the project development. This may be when the design definition is fixed in readiness for detailed design and construction, but may be earlier if design definition is unlikely to require widespread changes. The MOC system shall require that all proposals for change be recorded, made available for review by the appropriate personnel and approved or rejected in accordance with the project decision-making process.

5 Management of Major Accident hazards in design

5.1 Overview of MA hazard management

5.1.1 Design definition

Developing the design strategies for MA hazards shall be an integral part of developing of the overall project design definition.

Figure 1 provides an overview of how MA hazards shall be managed as an integral part of the overall design process for a new installation.

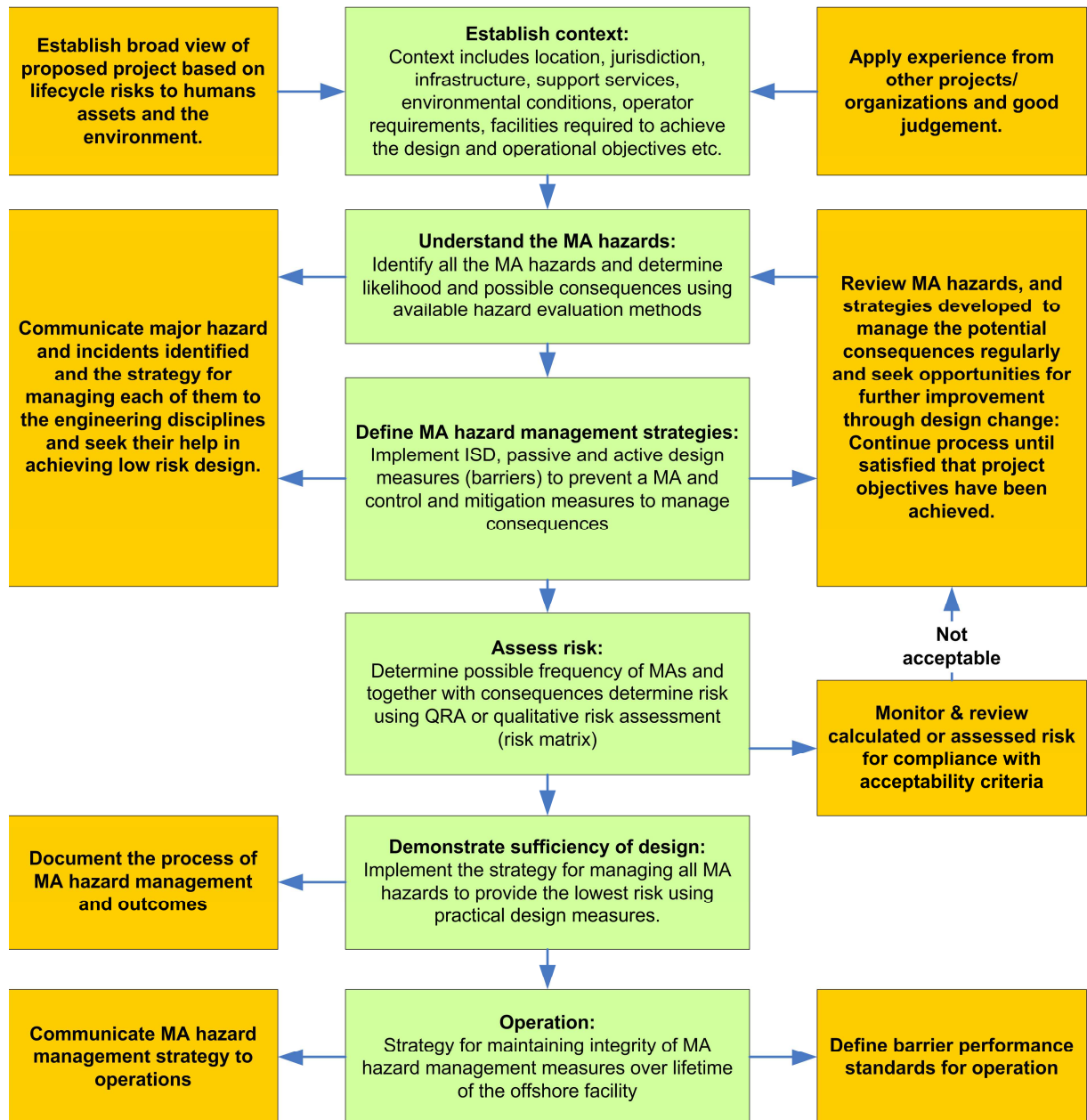


Figure 1 — Overview of managing MA hazards

In the early stages of a project, design definition is limited by a high level of uncertainty. Design strategies for managing MA hazards may initially have to be based largely on experience, generic MA knowledge, and comparisons with other similar facilities. During the subsequent phases of the project, uncertainty is reduced and the strategies for managing MA hazards shall be improved in line with the quality of the available input data. The following subclauses provide functional requirements for the development of the design definition for each phase of a project.

5.1.2 Front-end strategy

Major accident hazard management shall commence at the start of the project. In the early phases of design definition, information will be limited and there is likely to be uncertainty regarding the strategies for reducing frequency of MAs and managing the potential consequences. It is important to implement inherently safer designs (ISD) in the early phases of the project because the opportunities to avoid, substitute or moderate the hazards that could lead to MAs diminish as the design progresses. Application of the ISD principles shall start during the screening and concept selection phase, and continue through to concept definition and optimisation. The selection of the concept, such as subsea, tie-back, installation type (semi-submersible, spar, fixed platform, etc.), storage, loading or export pipelines and tie-ins, will have a major impact upon the consequences or frequency of MA hazards.

In the early phase of the project, allowance needs to be made for possible errors and uncertainty in the prediction of MA consequences and their likely frequency. This shall be addressed by applying good practice and by using conservative values for design loads so there is a good prospect of being able to withstand the actual anticipated loads once they are available.

As the design develops, the installation configuration, size, layout, process plant, inventory sizes, riser configuration, isolation and primary structure decision will have a significant impact on managing MA hazards.

The range of barriers necessary to manage MA hazards shall be identified as early as possible, even though at this stage it is not possible to define the performance standards in detail. For barriers which are widely used on offshore installations, generic information is likely to be available from similar facilities and recognised standards. For unusual barrier design requirements, the most appropriate tools and techniques to develop a functional specification need to be selected.

Engineering managers and discipline engineers are key contributors to the identification, evaluation and implementation of ISD and development of barriers. They shall have a good understanding of MA hazards and of their role in developing the design strategies for managing them. Good practice demands that all MA hazards are considered, with particular focus on those MAs with the potential for the most severe consequences.

5.1.3 Screening and concept selection

In this stage of a project, the outline layouts and main facilities are likely to be specified in sufficient detail to allow the most significant MA hazards to be identified and evaluated. This evaluation may use generic data or comparisons with similar installations for which MA hazard management information is known. The definition of all concept options being considered shall be to a similar level of detail to allow a comparison of the risk of MA hazards.

The concept options shall be assessed according to:

- MA hazards that are credible for the option;
- likely difficulty in developing effective strategies to manage MA hazards in future phases of the project;
- predicted risk profile of the final design.

By the end of this phase, the design definition of the selected concept shall be sufficient to evaluate the most significant MA hazards. The design shall also include ISD measures incorporated and preliminary proposals for further ISD measures. Design schemes for shortlisted concept options shall provide sufficient design detail for outline MA hazard management strategies to have a reasonable level of confidence that they will achieve the project hazard management objectives.

5.1.4 Concept definition and optimisation

Significant risk reduction can be achieved in this phase through continuing and developing the earlier work on ISD and engineered barriers. The level of detail required to enter detailed design will vary depending on the contracting strategy.

In general, prior to the start of detailed design

- all MA hazards shall be identified, and effective design strategies for managing them shall be developed;
- all the major hazard management features of the installation shall be defined in the basis of design; and
- there shall be a high level of confidence that risk for personnel, assets and the environment will be minimised, and that the project goals and risk criteria will be achieved.

One or more primary design contractors may be involved in developing the design definition. Arrangements shall be implemented to ensure that contract boundaries are not an obstacle to seamless development of design strategies for managing MA hazards. Contractor responsibilities shall be defined in the contracts and interfaces for MA hazard management, and action management well defined and accepted by each contractor.

5.1.5 Detailed design and construction

In developing the detailed design, the objective is to ensure that the ISD and barriers implemented are further developed and not compromised by design changes.

By the end of this phase the design definition will be essentially complete, and it shall be possible to demonstrate that all MA hazards have been identified, evaluated and suitable strategies implemented to manage them. All design-related actions shall be closed. It shall also be possible to demonstrate that the project goals and risk criteria are achieved.

One or more primary design contractors may be involved in detailed design and construction. Arrangements shall be implemented to ensure that contract boundaries are not an obstacle to implementation of the design strategies for managing MA hazards. Contractor responsibilities in this respect shall be defined in the contracts and interfaces for MA hazard management, and action management shall be defined and accepted by each contractor.

5.2 Key concepts and tools

5.2.1 Hazard identification (HAZID)

HAZID is a technique for early identification of potential threats that could result in harm to personnel or to the environment, and forms the basis for MA hazard management. The benefit of undertaking HAZID during screening and concept selection is the early identification and assessment of MA hazards which will provide essential input to critical project development decisions. The HAZID shall be updated periodically through the concept definition and optimisation stage.

5.2.2 Hazard and operability study (HAZOP)

The HAZOP process forms an important structured hazard identification and evaluation process which also helps the operational teams prepare for operation of the facility. HAZOP studies shall be conducted at defined stages during the project development, and updated as required throughout the lifecycle of the installation, including as part of a MOC process. Any additional MA hazards or causes and consequences identified during the study shall be recorded, and addressed as part of the MA hazard management process.

5.2.3 Understanding the MA hazards

Each of the identified MA hazards, hydrocarbon and non-hydrocarbon related, shall be evaluated to provide a good understanding of its likelihood and consequences.

These evaluations shall be documented in order to

- a) maintain a record of the purpose, process adopted, personnel involved, input data, methodology used and results;
- b) define
 - 1) assumptions made and their basis;
 - 2) uncertainties inherent in the results, and the possible implications for the project;
 - 3) sensitivity of the results to changes in key design parameters;
- c) provide a record of actions arising from each study.

The following shall be addressed when defining the methods, models and tools to be used in evaluating the MA hazards:

- the suitability with respect to the defined objective(s), scope for the evaluation and the decisions to be made;
- the validity of the models or tools and the availability of input data. In general, only recognized and validated methods, models and tools shall be used;
- the effect of human and organizational factors. This may range from a qualitative discussion to a detailed analysis of human and organizational errors, depending on the criticality of such aspects;
- the use of alternative approaches (e.g. expert judgements, non-representative data, etc.) to compensate for lack of relevant and/or required input data and models;
- limitations in the validity of the results due to lack of availability of relevant data and models.

5.2.4 Inherently safer design (ISD)

ISD shall be used either to eliminate MA hazards or to reduce their potential consequences by design measures that are inherent in the design, being permanent and inseparable features of the installation.

Particular attention shall be given to applying ISD concepts at the concept selection and optimisation phases to eliminate MA hazards. Where MA hazards cannot be eliminated, ISD shall focus on passive rather than active means of prevention, control and mitigation.

The general ISD strategies are the following:

- Eliminate or avoid: eliminate the hazards or remove the exposure to MA hazards by design;
- Minimize: reduce the hazardous inventories or the frequency or duration of exposure;
- Substitute: replace hazardous materials with safer materials (but recognize that there could be some trade-offs between plant safety and the wider product and life cycle issues);
- Moderate: use less hazardous conditions, or facilities that minimise the impact of a release of hazardous material or energy;

— Simplify: reduce complexity and make operating errors less likely.

5.2.5 Design strategies for managing MA hazards

Strategies shall be developed to identify how the MA hazards will be managed in order to meet the overall project objectives.

The strategies shall describe

- a) the nature, extent and causes of MAs;
- b) design measures to reduce the likelihood of incidents (prevention barriers);
- c) design measures that detect and control the hazardous event and prevent or reduce escalation (control barriers);
- d) design measures that protect personnel and barriers that prevent or reduce unwanted consequences (mitigation barriers);
- e) how the barriers combine to manage MA hazards (i.e. how they provide multi-layer protection);
- f) those critical barriers (prevention, control or mitigation) where failure could cause an otherwise controllable MA to escalate;
- g) emergency response measures necessary to allow escape to muster locations, to protect the temporary refuge and to allow controlled evacuation without external support;
- h) emergency response measures to mitigate potential pollution at sea;
- i) performance standards necessary for barriers and emergency response measures.

ISO 13702 provides more details on fire and explosion strategy and ISO 15544 provides more details on emergency response strategy.

Further information concerning the development of design strategies for managing MA hazards is given in Annex C.

5.2.6 Barriers

5.2.6.1 General

All reasonable options to eliminate or avoid MA hazards shall be applied before consideration is given to the provision of barriers. However, for large installations it is likely that barriers providing multiple layers of protection will be required in order to provide a robust MA hazard management strategy.

Barriers may be classified as passive, active or procedural and can be used to prevent, control or mitigate MA hazards. The classification of barriers is based on their intention on demand. Passive barriers shall be preferred over active barriers which, in turn, shall be preferred over procedural barriers.

Where failure of a barrier, or element of a barrier, is a possibility, there shall be sufficient alternative barriers, or redundancy within the barrier, to maintain effective MA hazard management. The analysis of possible barrier failure shall also take account the vulnerability of barriers to MAs (see Annex B, ESSA).

5.2.6.2 Passive barriers

Passive barriers are engineered equipment and systems that do not need to be activated on demand, as they are always in place by design.

Examples include

- prevention barriers, e.g. mechanical integrity (pipework, pressure vessels), facility layout;
- control barriers, e.g. minimised vessel inventory, firewalls, secondary containment (bunds);
- mitigation barriers, e.g. explosion protection (blast walls); passive fire protection.

5.2.6.3 Active barriers

Active barriers are engineered systems that require action to be taken to function on demand, without human action.

Examples include

- prevention barriers, e.g. process control; safety-instrumented systems; relief systems;
- control barriers, provide e.g. emergency shutdown and depressurisation, isolation of electrical equipment;
- mitigation barriers, provide e.g. active fire-fighting systems, explosion suppression.

5.2.6.4 Procedural barriers

Procedural barriers are decisions and/or actions undertaken by a person, who may be on or off the installation, when required to do so. If a barrier has a human element such as 'operator response to alarm', it should be considered a procedural barrier even though equipment such as the detection device and the end device is part of the barrier.

Examples include

- prevention barriers, e.g. undertaking inspection and taking any necessary corrective action, executing planned maintenance, operating within the operational envelope of the plant;
- control barriers, e.g. operator response to alarms, manually initiated fire and gas detection and isolation, closing of blow-out preventer, manual plant shutdown;
- mitigation barriers, e.g. manual fire-fighting, emergency response, evacuation.

If procedural barriers are used for managing MA hazards, these shall be recorded in operational procedures as critical activities related to MA hazard management. A process to manage competency of those performing these tasks shall be established.

5.2.7 Performance standards

5.2.7.1 General

Performance standards shall be unambiguous statements specifying the minimum expected standards for key aspects of each barrier such that it is able to fulfil its role.

Performance standards shall be specified for each barrier (including emergency response measures) to include the barrier's

- a) role — a high level description of what the barrier is intended to achieve;
- b) scope — extent of the barrier;
- c) functionality — specific standards or criteria that the barrier shall meet in order to achieve its intended objective;
- d) availability/reliability — the required availability or reliability of the barrier;
- e) survivability — the type and severity of MAs that the barrier shall survive and continue to function.

Multiple but linked performance standards may be written to support a complete barrier.

Any critical dependency or interaction between barriers shall be evaluated to ensure this does not jeopardise hazard management strategies.

Activities to provide assurance of performance standards shall be planned for design, procurement, construction, commissioning and operations phases of the installation lifecycle.

5.2.7.2 Design performance standards

Performance standards for design shall be initially defined during the concept definition and optimization stage. In some cases performance standards for unusual or high criticality barriers will be required during concept selection to support decisions, e.g. selection of pipelines not rated for the maximum operating pressure. As the design progresses, the initial performance standards shall be updated and additional performance standards created.

Performance standards for design shall be verifiable by reference to design documentation, evaluations of MA hazards or subject to specific performance testing.

The design performance standards shall allow for some degradation of equipment or function to occur as an expected part of operating service without significant impairment of the ability of the barrier to perform its role.

5.2.7.3 Operations performance standards

All performance standards shall have a periodic assurance process to confirm that they are able to meet their contribution to the MA hazard management strategies.

Those performance standards that the operations team are required to maintain through periodic inspection, maintenance and test schemes shall be defined in the documentation handed over to operation.

Performance standards shall define the frequency of the assurance process to verify performance, based on the possibility of failure or impairment when in service. Information on the frequency of failure or impairment shall be drawn from equipment reliability and failure data, operating experience or specific evaluation (e.g. FMECA). The effect of failure or impairment of each barrier, and how that can change the design strategies for managing MA hazards, should be evaluated to determine the reliability or availability required.

Technical and operational teams in the operating entity are accountable for the ongoing maintenance of barriers once the facility is handed over by the project team.

The ISD choices and measures to manage the MA hazards shall be developed in collaboration with the technical and operational teams to ensure they are appropriate and do not impose an unreasonable burden to inspect, test and maintain for the maximum credible lifetime of the installation. The longer-term operational perspective shall be the major factor in any project.

6 Screening and concept selection process

6.1 General

When screening and selecting the design concept to be carried forward for development, project management shall take account of the requirements for managing MA hazards. Figure 2 provides an overview.

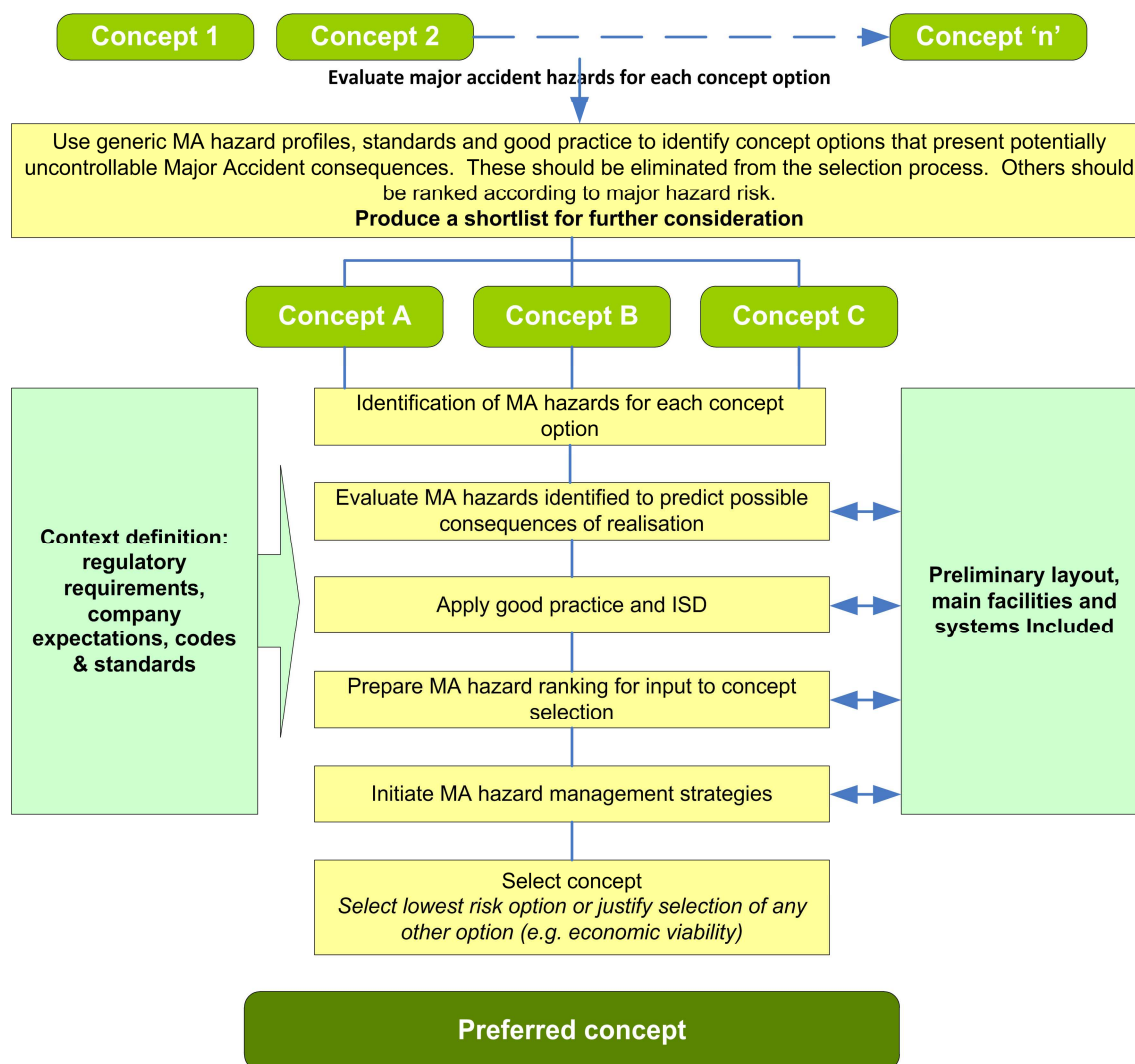


Figure 2 — Screening and concept selection process

In practice, many factors are important in selecting the concept to be carried forward, including economics, technical viability, technical risk and availability of resources. If the lowest risk option is not selected, it is important that the project management understand the implications and develop suitable strategies for managing MA hazards in subsequent project phases. The implications shall be identified for specific consideration in subsequent phases.

6.2 Objectives

The hazard management objectives for this phase are to screen the proposed design concept options in order to provide recommendations for elimination of high risk options and for ranking of others in terms of the risks of MAs associated with each option.

To achieve this overall objective, the process to manage MA hazards shall

- identify the generic MA hazards associated with each of the concept options and understand the likely consequences;
- identify the strategies for MA hazards that could eliminate or reduce major hazard consequences and risk for each concept option;
- define any unusual or innovative technology required;
- rank concept options in order of possible difficulty in implementing effective strategies for managing MA hazards, taking into account the potential ISD measures and barriers available;
- identify and reject concept options that are unlikely to achieve the risk objectives for MA hazards.

In addition, the shortlist of concept options shall:

- a) demonstrate that each concept option is able to achieve the project goals for managing MA hazards;
- b) identify remaining uncertainty and any follow-up actions needed in the next phase;
- c) prepare documentation to support the concept option selection decision.

6.3 Functional requirements

6.3.1 Overview

The activities required as a minimum during this phase are summarised in Table 1. Further details are found in the subclauses following the table.

Table 1 — Screening and concept selection activities

Screening	— Determine parameters for ranking of concept options for MA hazard management and risk; — identify concept options to be screened out because they have the potential risk of MAs that does not align with hazard and risk management objectives of the organization(s) managing the installation or the authorities having jurisdiction over the operation; — estimate the degree of uncertainty, particularly with regard to novel technology and the possible implications for future project phases; — identify the key safety focus areas for subsequent phases of development; — identify any possible regulatory compliance issues; — produce a short-list of acceptable concept options.
Hazard Identification	— Use comparisons with similar types of installation or specific facilities to identify MA hazards; — conduct a high-level assessment of concept options, mainly to identify MA hazards that could materially affect selection due to the possible severity of consequences and uncertainty over developing an effective design strategy for MA hazard management; — conduct preliminary HAZID study for each of the short-listed concept options.
MA hazard evaluation	— Develop outline understanding of the MA hazards, their causes and possible consequences through review, assessment, and comparison with known major hazard incidents on similar installations; — assess the effect of possible ISD and barrier systems for reducing the impact of major hazard consequences; — assess whether potential major hazard consequences could prove difficult (or impossible) to manage in later phases of the project, taking into account available technology.
Assess risk	— estimate likely risk profile using generic risk data against the outline concept option designs; — identify major hazards that potentially produce a high risk
ISD and barriers	— Identify ISD measures that could reduce the likelihood of MA hazards and the possible consequences; — identify any unusual or high criticality barriers required to manage potentially severe MA hazards; — propose a generic range of barriers to support a multilayer design strategy for MA hazard management for each of the identified major hazards; — for the short-listed concept options, define preliminary strategies for managing MA hazards.
Performance standards	— Establish performance requirements at a functional level for unusual or high criticality barriers, otherwise assume generic performance standards for generic barriers as a starting point.
Sufficiency of measures	— Assess whether sufficient information exists to support concept screening conclusions, both in respect of elimination of unsuitable options and the ranking of others; — explain uncertainty and its possible implications for future phases.
Register of MA hazards	— Prepare an outline register of MA hazards for the selected concept option.
Documentation	— Prepare documentation to explain how the screening and selection process addressed MA hazard management; — prepare a plan to manage MA hazards for the concept definition and optimisation phase

6.3.2 Screening

A degree of uncertainty is inevitable at this phase, and the knowledge and experience of the concept evaluation team, particularly of project safety engineering specialists, is important. The evaluation team shall be drawn from engineering disciplines, operations and construction personnel.

The concept options selected to be carried forward shall be restricted to those where there is a high degree of confidence that the risk to people, the environment and the assets can be effectively managed for the full lifecycle of the installation. If uncertainty is identified, it should be clearly defined in the documentation for concept screening and selection, with recommendations for action in future phases of the project.

If the preferred concept option for managing MA hazards has not been selected, the reasons shall be documented together with the areas of concern to be addressed in subsequent stages of development.

6.3.3 Hazard identification (HAZID)

Major hazards that could affect the selection of a concept option shall be identified in time to allow evaluation and understanding of the likely consequences, and to propose measures needed for MA hazard management.

The most effective approach is to conduct a HAZID study, calling on the expertise and knowledge of competent and experienced personnel from design, construction and operation. As a minimum, a formal HAZID shall be carried out for each of the short-listed concept options.

A summary schedule of all MA hazards shall be prepared for each concept option, including cause and consequences in terms of loss of life, environmental damage, business loss and harm to company reputation.

6.3.4 Major accident hazards evaluation

Preliminary assessment of the MA hazards identified for each concept option shall be carried out. The evaluation shall be based on generic information, comparisons with similar facilities and assumptions. The evaluation techniques and methodologies used shall reflect the limitations of design data available and focus on the most significant MA consequences, using largely qualitative judgement. Good practice and judgement are required to assess the level of uncertainty and provide appropriate guidance for decision making.

Where MA hazards are unusual, not well understood or there is no suitable design strategy for their hazard management, further analysis shall be conducted.

An outline design strategy for MA hazard management shall be developed, where possible, to explain how the hazards could be managed in future stages of the project, explaining any unusual or high-criticality barriers required. Where no suitable strategy can be foreseen, these concepts shall be regarded as potentially unacceptable.

6.3.5 ISD and barriers

Opportunities for inherently safer design shall be identified where such measures are likely to influence the screening and selection of the concept options.

For each concept option, the acceptability of any unusual or high-criticality barriers shall be assessed and a judgement made of the viability for MA hazard management.

Opportunities offered by the implementation of innovative measures and technology shall be assessed to determine the potential benefits and possible implications for the project and future operation.

Multidiscipline knowledge and experience shall be used to identify inherently safer design or specific barriers needed to optimise MA hazard management.

For each of the short-listed concept options, a preliminary ISD review shall be conducted to identify opportunities to eliminate or reduce the severity of hazards, and to provide effective emergency response. The aim is to optimise MA hazard management so that a consistent and balanced selection decision can be made.

6.3.6 Performance standards

Where unusual barriers, or barriers that are required to perform a particularly critical role (high integrity), exist, the nature and associated uncertainty shall be highlighted and preliminary performance standards defined.

Where generic barriers have been defined, generic performance standards should be assumed.

6.3.7 Sufficiency of measures

Preliminary strategies for managing MA hazards shall be proposed to determine the degree of confidence with which each of the identified hazards can be managed using known and well understood design measures. Particular focus shall be applied to those hazards for which a suitable strategy cannot be defined, owing to either a poor understanding of the consequences or because appropriate measures for managing MA hazards are not available, or a combination of both.

Further effort shall be applied, using specialist assistance where appropriate, to reduce the level of uncertainty before a selection is made. This is particularly important if there are significant uncertainties associated with the 'preferred' concept.

6.3.8 Documentation

Documentation shall be prepared to include a summary of the activities carried out during the screening and selection process covering the following:

- MA hazards identified, and outcome of preliminary evaluation of severity of consequences;
- outline design strategies for managing MA hazards;
- explanation of concept options eliminated due to high risk or perceived difficulty in developing design strategies for managing MA hazards;
- explanation of ranking of concept options for MA hazards;
- identification of the preferred concept option for managing MA hazards, and reasoning applied;
- if the preferred option has not been selected, the reasons to justify this decision, together with identification of areas of concern to be addressed in later phases of the development.

7 Concept definition and optimisation

7.1 General

The concept definition and optimisation process shall be implemented in accordance with the plan for managing MA hazards, as illustrated in Figure 3.

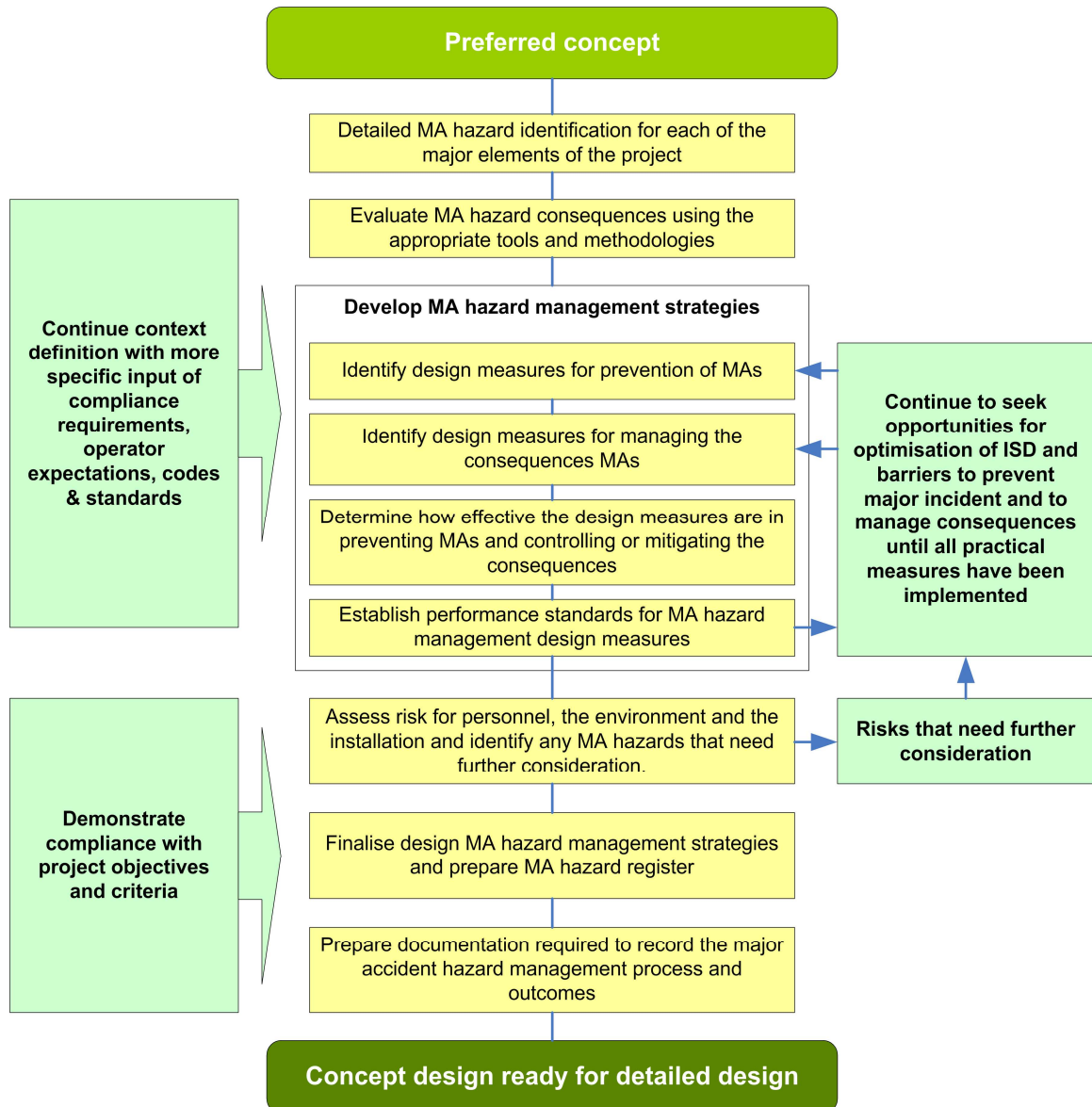


Figure 3 — Outline of concept definition and optimisation

The MA hazard management process in this phase shall involve ongoing iteration of MA hazards review and evaluation, identification of design measures that could provide improved, management of hazards, testing their effect and practicality, and implementing those considered to be of benefit. This shall continue until it can be shown that MA hazard management has been practically optimised and the risk reduced in line with project risk management objectives.

7.2 Objectives

The primary objective is to develop the MA hazard management to a level consistent with entry into the detailed design stage.

7.3 Functional requirements

7.3.1 Overview

The activities required as a minimum during this phase are summarised in Table 2. Further details are found in the subclauses following the table.