

BS EN ISO 17776:2016



BSI Standards Publication

**Petroleum and natural gas
industries - Offshore
production installations -
Major Accident hazard
management during the
design of new installations
(ISO 17776:2016)**

bsi.

AVA Documents
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN ISO 17776:2016. It supersedes BS EN ISO 17776:2002 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PSE/17/-/6, Processing equipment and systems for petroleum and natural gas industries.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 81227 9

ICS 75.180.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 **January 2017**.

Amendments/Corrigenda issued since publication

Date	Text affected
------	---------------

English Version

**Petroleum and natural gas industries - Offshore
production installations - Major Accident hazard
management during the design of new installations (ISO
17776:2016)**

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 17776:2016)

Erdöl- und Erdgasindustrie - Offshore-
Produktionsanlagen - Management der Gefährdungen
durch schwere Störfälle bei der Konstruktion neuer
Offshore-Anlagen (ISO 17776:2016)

This European Standard was approved by CEN on 19 October 2016.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

This document (EN ISO 17776:2016) has been prepared by Technical Committee ISO/TC 67 "Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries" in collaboration with Technical Committee CEN/TC 12 "Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries" the secretariat of which is held by CYS.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2017, and conflicting national standards shall be withdrawn at the latest by June 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 17776:2002.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 17776:2016 has been approved by CEN as EN ISO 17776:2016 without any modification.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	4
4 Major accident hazard management overview	5
4.1 General	5
4.2 Project management commitment	5
4.3 Project management accountability	6
4.4 Project plan to manage major accident hazards	6
4.5 Objectives of major accident hazard management	6
4.6 Selection of hazard evaluation and risk assessment methods	7
4.7 Good engineering practice	7
4.8 Documentation	8
4.8.1 General	8
4.8.2 Register of major accident hazards	9
4.9 Actions management	9
4.10 Management of change	9
5 Management of major accident hazards in design	10
5.1 Overview of MA hazard management	10
5.2 Key concepts	11
5.2.1 Understanding the MA hazards	11
5.2.2 Inherently safer design (ISD)	12
5.2.3 Design strategies for managing MA hazards	13
5.2.4 Barriers	13
5.2.5 Performance standards	14
5.2.6 Communication with technical and operational teams	15
6 Screening and concept selection process	15
6.1 General	15
6.2 Objectives	16
6.3 Functional requirements	17
6.3.1 Screening	17
6.3.2 Hazard identification	17
6.3.3 Major accident hazards evaluation	17
6.3.4 ISD and barriers	18
6.3.5 Performance standards	18
6.3.6 Sufficiency of measures	18
6.3.7 Documentation	18
7 Concept definition and optimization	19
7.1 General	19
7.2 Objectives	20
7.3 Functional requirements	20
7.3.1 Hazard identification	20
7.3.2 Major accident hazard evaluation	20
7.3.3 Risk assessment	20
7.3.4 Inherently safer design (ISD)	20
7.3.5 Barriers	21
7.3.6 Performance standards	21
7.3.7 Sufficiency of measures	21
7.3.8 Documentation	21

8	Detailed design and construction phase	22
8.1	General	22
8.2	Objectives	23
8.3	Functional requirements	23
8.3.1	Overview	23
8.3.2	Hazard identification	24
8.3.3	Major accident hazards evaluation	24
8.3.4	Risk assessment	24
8.3.5	Inherently safer design (ISD)	24
8.3.6	Barriers	24
8.3.7	Performance standards	25
8.3.8	Sufficiency of measures	25
8.3.9	Register of major accident hazards	25
8.3.10	Documentation	25
8.3.11	Procurement of equipment	26
8.3.12	Construction, completion and commissioning	26
8.3.13	Transfer to operation	26
8.3.14	Actions management	26
9	Major accident hazard management in operation	27
9.1	General	27
9.2	Objectives	27
9.3	Functional requirements	28
9.3.1	Barrier management	28
9.3.2	Revalidation	28
9.3.3	Safety-critical tasks	28
9.3.4	Temporary changes	29
9.3.5	Non-availability of barrier performance	29
9.3.6	Management of change (MOC)	29
	Annex A (informative) Example of a framework for risk-related decision support	31
	Annex B (informative) Plan to manage major accident hazards	32
	Annex C (informative) Major accident hazard management identification and evaluation tools	41
	Annex D (informative) Strategy for managing major accident hazards	71
	Annex E (informative) Barrier system performance standards	77
	Annex F (informative) HAZID guidewords	80
	Bibliography	94

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 (see 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 (see 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.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is 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 document 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 petroleum 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 the 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 recognized codes and standards.

This document covers the following main elements:

- establishing general requirements for identifying MA hazards and their causes;
- assessing 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 all credible MAs;
- maintaining the measures throughout the life of the installation.

The technical content of this document is arranged as follows:

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

This document 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 document describes processes for managing major accident (MA) hazards during the design 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 limit the possible consequences. It also contains some requirements and guidance on managing MA hazards in operation.

This document 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 credible MA hazards with the potential to have a material effect on people, the environment and assets.

This document is intended for the larger projects undertaken to develop new offshore 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.

Mobile offshore units as defined in this document are excluded, although many of the principles can be used as guidance. The design of subsea facilities are also excluded, though the effects of mobile and subsea facilities are considered if they can lead to major accidents that affect an offshore installation. This document does not cover the construction, commissioning, abandonment or security risks associated with offshore installations.

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

2 Normative references

The following documents are referred to in text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, *Risk management — Principles and guidelines*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1 barrier

functional grouping of safeguards or controls selected to prevent a major accident or limit the consequences

Note 1 to entry: Barriers can be subdivided into hardware barriers or human barriers and are supported by management system elements.

Note 2 to entry: Adapted from IOGP Report No. 415.

3.1.2 emergency response

action taken by personnel on or off an installation to limit the consequences of a major accident or initiate and execute abandonment

[SOURCE: ISO 15544:2000, 2.1.8]

3.1.3 environment

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

Note 1 to entry: Surroundings can extend from within an organization to the local, regional and global system.

Note 2 to entry: Surroundings can be described in terms of biodiversity, ecosystems, climate or other characteristics.

[SOURCE: ISO 14001:2015, 3.2.1]

3.1.4 ergonomics

scientific discipline concerned with study of human factors and understanding of interactions among human and other elements of a system

Note 1 to entry: Adapted from ISO 6385:2004.

3.1.5 escape route

route from an area of an installation leading to a muster area, temporary refuge (TR), embarkation area, or means of escape to the sea

[SOURCE: ISO 15544:2000, 2.1.15]

3.1.6 evacuation

planned method of leaving the installation in an emergency

[SOURCE: ISO 15544:2000, 2.1.17]

3.1.7 harm

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

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.1.8 hazard

potential source of harm

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

3.1.9

hazardous event

event that can cause harm

[SOURCE: ISO/IEC Guide 51:2014, 3.3]

3.1.10

individual risk

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

3.1.11

inherently safer design

design which eliminates or reduces major accidents through measures that are permanent and inseparable from the design

3.1.12

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 document, a major accident is the realization of a major accident hazard.

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

3.1.13

major hazard

hazard with the potential, if realized, to result in a major accident

3.1.14

mobile offshore unit

mobile platform, including drilling ships, equipped for drilling for subsea hydrocarbon deposits and mobile platforms for purposes other than production and storage of hydrocarbon deposits

Note 1 to entry: Includes mobile offshore drilling units, drill ships, accommodation units, construction and pipe-lay units, well servicing and well stimulation vessels.

3.1.15

muster area

designated area to which personnel report when required to do so in an emergency

[SOURCE: ISO 15544:2000, 2.1.29]

3.1.16

performance standard

measurable statement, expressed in qualitative or quantitative terms, of the performance required of a system, item of equipment, person or procedure, and that is relied upon as a basis for managing a hazard

Note 1 to entry: Hardware performance standards address the functionality, reliability, survivability and interdependency of barriers under emergency conditions.

[SOURCE: IOGP Report No. 415]

3.1.17

risk

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

Note 1 to entry: A more general definition of risk is given in ISO Guide 73:2009 and is “effect of uncertainty” where:

- an effect is a deviation from the expected, and
- uncertainty is a state of having limited knowledge where it is impossible to exactly describe the existing state and future outcomes.

[SOURCE: ISO/IEC Guide 51:2014, 3.9, modified, Note 1 to entry has been replaced with another note.]

3.1.18

risk criteria

terms of reference against which the significance of risk is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and [external](#) and [internal context](#).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.1.19

risk tolerance

organization's readiness to bear the risk after risk [treatment](#) in order to achieve its objectives

Note 1 to entry: Risk tolerance can be influenced by legal or regulatory requirements.

Note 2 to entry: Qualitative or quantitative criteria can be used to help the organization decide if a risk is tolerable

[SOURCE: ISO Guide 73:2009, 3.7.1.3, modified – Note 2 to entry has been added.]

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

[SOURCE: ISO 15544:2000, 2.1.37, modified, Note 1 to entry has been omitted.]

3.2 Abbreviated terms

CFD computational fluid dynamics

EER escape, evacuation and rescue

ESD emergency shutdown

FMECA failure mode, effects, and criticality analysis

HAZID hazard identification study

HAZOP hazard and operability study

IOGP International Association of Oil and Gas Producers (previously: OGP)

ISD inherently safer design

JHA job hazard 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 31000 and shall

- establish the context prior to starting or executing any of the elements of the process,
- update the context throughout the process, and
- 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 an 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 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 document 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 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, shall be used 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. An example of a framework to support decision making is given in [Annex A](#).

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 all credible 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 objectives can be written into legislation);
- define the decision-making process related to managing MA hazards, including who is authorized 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, including the lead discipline engineers;
- make available to the project team competent and sufficient engineering resources to deliver the MA hazard management objectives (including safety and other technical disciplines);
- 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 all credible MA hazards;
- define how the process for managing all credible 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 person in the project organization accountable for safety engineering shall be capable of specifying and commissioning work necessary for evaluating MA hazards and performing risk assessments. Where appropriate, that work can 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 all credible 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 B](#).

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 person accountable for the safety engineering 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, testing or maintenance activities;
- reducing the likelihood of MAs by providing facilities that can meet the full operational envelope, including foreseeable upset conditions and the potential for human error;
- reducing the likelihood of MAs by providing the functionality to safely allow all foreseeable operational, inspection, testing 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 people on board while emergency response is undertaken and, if necessary, evacuation is completed.

4.6 Selection of hazard evaluation and risk assessment methods

The person accountable for safety engineering shall be responsible for selection of the approach and the appropriate methods for MA hazard evaluation and risk assessment. The methods chosen shall be dependent upon factors such as the size and complexity of the installation, the credible MA hazards, the severity of the MA consequences, the degree of uncertainty, the level of risk, the number of people exposed to the risk and the proximity of environmentally sensitive areas.

The approach to MA hazard evaluation and risk assessment can 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 can 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 can be used providing they meet current objectives, standards and criteria, new knowledge and technology and they adequately cover any significant differences which affect the management of MA hazards (e.g. environment, fluid composition, shut-in pressure). In some cases, the earlier hazard management work may be deemed sufficient or may need only limited new work.
- Complex installations, such as production platforms with processing facilities and accommodation, shall always use a structured approach for MA hazard management to ensure that no MA hazards are overlooked. Within a structured approach there may be areas of the installation where previous relevant MA hazard management work can be used to limit the amount of new work needed.
- For installations in the early design phase, evaluations will necessarily be less detailed than those undertaken during later design phases.

4.7 Good engineering practice

An integral part of MA hazard management is the application of recognized and accepted good engineering practice by 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 recognized 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 risk-related decision-making is available in Reference [64]. 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

- develop the strategies for managing MA hazards and how they reduce risk, and
- 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 credible MA hazards and evaluate the potential consequences of any relevant 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, including the potential for human error, have been taken into account;
- e) report the risk assessed, and when necessary calculated, for the design detailing 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 MA hazards and related MAs.

The documentation shall be subject to formal review by the project 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 summarize the following:

- all the MA hazards identified;
- the identified initiating mechanisms (i.e. failure modes or causes);
- the potential consequences of all credible MAs, including the escalation potential;
- the primary design measures for inherently safer design;
- the hardware barriers provided for MAs;
- the primary design measures for protection of escape routes, the temporary refuge, muster locations, evacuation facilities and the associated structural supports;
- 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 authorization for verification of close-out or rejection.

Requirements for managing actions shall also be applied to the primary contractors, 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 accepted by operations prior to start-up.

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 detailed requirements for MOC are outside the scope of this document, 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 shall 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. Once this stage is reached, all changes that significantly affect the design strategies for MAs shall be managed through an MOC process. This requires:

- assessment of the impact of the proposed change on the MA hazards;
- identification and evaluation of any new MA hazards introduced by the proposed change;
- assessment of whether the barrier's performance will be sufficient to maintain the MA hazard management strategy following the change;
- definition and implementation of changes to ISD measures and barriers which are required to provide MA hazard management strategy at least comparable to current strategies;
- definition of changes required to the documentation that demonstrates that MA hazards have been managed in a way that satisfies the objectives and criteria for the installation.

5 Management of major accident hazards in design

5.1 Overview of MA hazard management

[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.

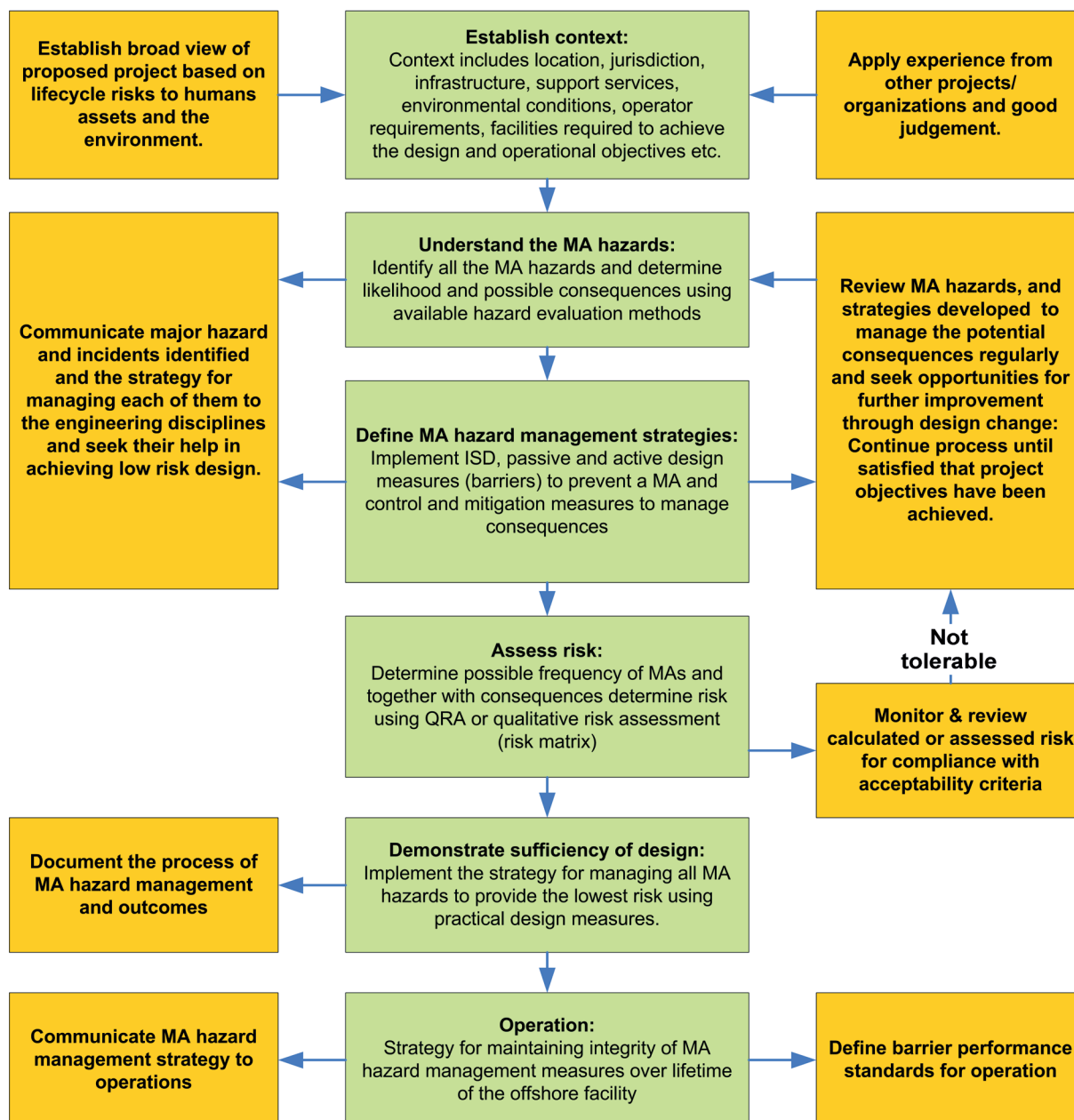


Figure 1 — Overview of managing MA hazards

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.

5.2 Key concepts

5.2.1 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, people 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. An analysis of human factors should be used to identify all reasonable improvements that can be made to the installation design to strengthen human barriers, reduce the potential for error and to help the operations team manage the operation of the installation. As a minimum, safety-critical tasks shall be identified and assessed systematically, including the effect of errors or unreliable human performance.
- Limitations in the validity of the results due to lack of availability of relevant data and models.
- 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.

[Annex C](#) provides an introduction to many of the identification and evaluation tools that are commonly used in the development of new offshore installations.

5.2.2 Inherently safer design (ISD)

ISD shall be used either to eliminate credible MAs 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 optimization phases to eliminate MAs. Where MAs cannot be eliminated, ISD shall focus on passive rather than active means for preventing and managing the MA.

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 minimize the impact of a release of hazardous material or energy;
- simplify: reduce complexity and make operating errors less likely.

5.2.3 Design strategies for managing MA hazards

Strategies shall be developed to identify how the credible MA hazards will be managed in order to meet the overall project objectives. The strategies shall describe the approach to be used to manage the MA hazards in sufficient detail to guide the design and operation of the installation. They shall cover:

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

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 D](#).

5.2.4 Barriers

All reasonable options to eliminate or avoid MA hazards shall be applied before consideration is given to the provision of barriers. For the MA hazards that remain, a robust MA hazard management strategy is likely to need barriers to:

- prevent MAs, or reduce the likelihood of occurrence;
- limit the extent and duration of any MAs that do occur;
- limit the effects of any MAs that to occur;
- allow effective emergency response.

Barriers can be hardware or human and are supported by management elements. Hardware barriers are the engineered systems provided to prevent MAs and limit the potential consequences. Human barriers are the actions of people to prevent MAs and limit the potential consequences.

Passive hardware barriers shall be preferred over active hardware barriers which, in turn, shall be preferred over reliance on human barriers.

Design accidental loads shall be specified for those hardware barriers that need to withstand an MA in order to perform their role. The preference shall always be to design a barrier to withstand the worst credible design accident load. If this is not reasonable, lower loads may be specified providing it can be demonstrated that the overall project objectives will still be met. In this case, the consequences of failure of a barrier, or an element of a barrier, shall be fully assessed.

NOTE The design accidental loads specified to achieve numerical risk criteria which have been set for the installation are sometimes called the dimensioning accidental loads.

Hardware barriers provided for a particular MA can affect the likelihood and consequences of other MAs (e.g. fire walls provided to limit fire spread can reduce ventilation and increase the likelihood of gas accumulation and explosions). When selecting hardware barriers, the full effect of providing the

barrier shall be assessed to confirm that provision of the barrier will not jeopardize the overall project objectives.

Some barrier performance can be dependent on human actions, and therefore prone to unreliable human performance and potential error. When considering reliance on a human barrier, the design requirements necessary to support the barrier and the associated tasks shall be specified.

Additional guidance on barriers is provided in [D.2](#).

5.2.5 Performance standards

5.2.5.1 General

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

Performance standards for each barrier or barrier element shall specify:

- a) function — a high level description of what the barrier or barrier element is intended to achieve;
- b) scope — extent of the barrier;
- c) functional requirements:
 - specific standards or criteria that the barrier shall meet in order to perform its role;
 - the required availability or reliability of the barrier;
 - the type and severity of MAs that the barrier shall survive and continue to function.

Multiple but linked performance standards can be needed to support a complete barrier function (e.g. ignition control).

Any critical dependency or interaction between barriers shall be evaluated to ensure this does not jeopardize 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.

NOTE ISO/TR 12489:2013, Annex A lists a number of safety functions (hardware barriers) that can require reliability analysis, as part of the MA hazard management process.

Further information on barrier performance standards is given in [Annex E](#).

5.2.5.2 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 hardware 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 hardware barrier to perform its role.

5.2.5.3 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 the operator.

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 hardware barrier, and how that can change the design strategies for managing MA hazards, should be evaluated to determine the reliability or availability required.

5.2.6 Communication with technical and operational teams

Technical and operational teams in the operating entity are accountable for the ongoing maintenance of hardware 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.

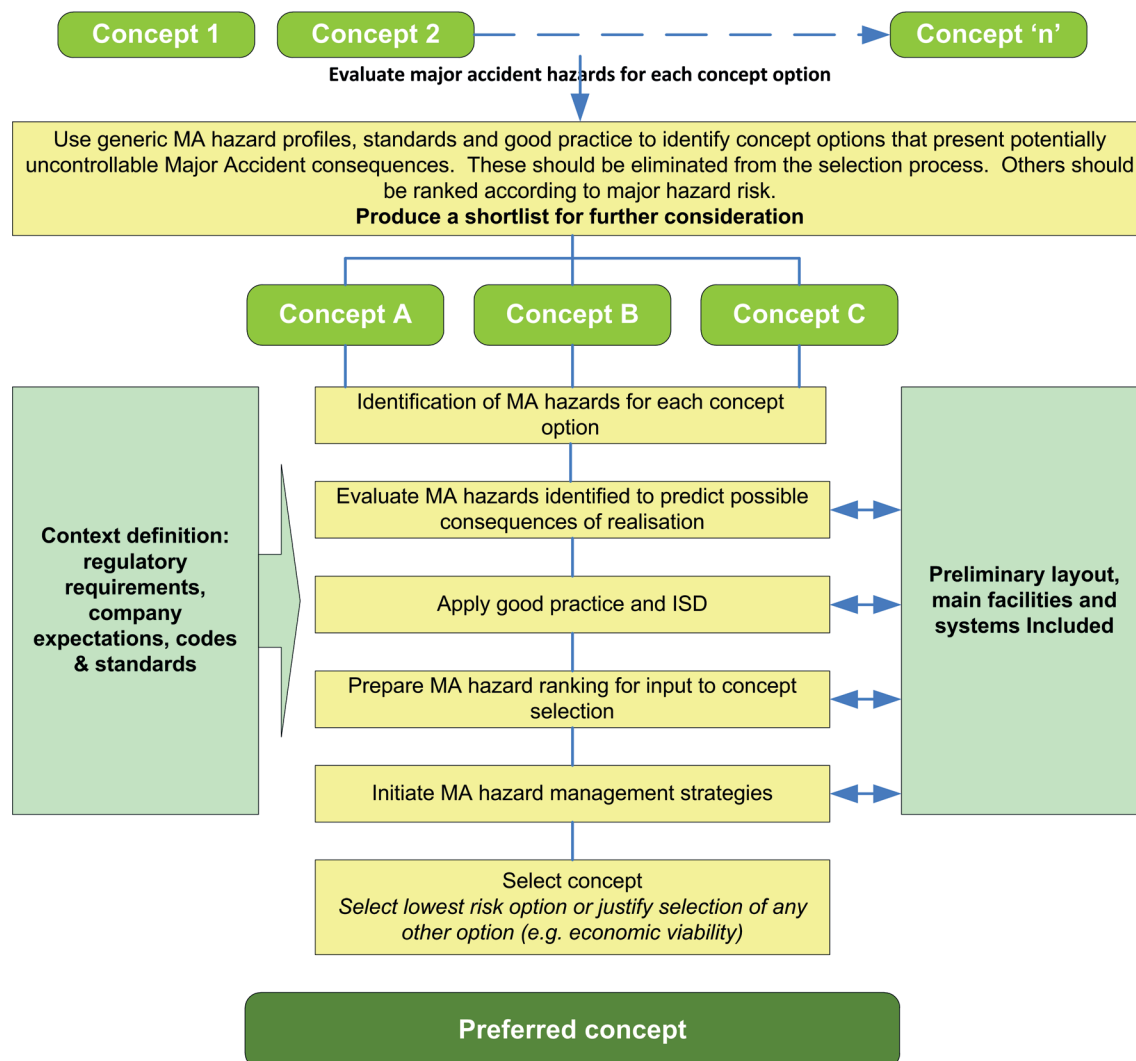


Figure 2 — Screening and concept selection process

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 that could eliminate MA hazards or reduce MA 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 objectives for MA hazard management.

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 Screening

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.

6.3.2 Hazard identification

MA 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 people 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 credible 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.

[Annex F](#) provides an extensive checklist of hazards which can be encountered in the petroleum and natural gas industries.

6.3.3 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. The assessments at this stage of the process shall be robust to uncertainties and lack of knowledge so that there is a high degree of confidence that the project objectives will be met as the design develops.

Where credible MA hazards are unusual, not well understood or there is no suitable design strategy for their management, the concept option shall be eliminated unless there is a very good prospect that further analysis or data will demonstrate that the project objectives will be met.

An outline design strategy for MA hazard management shall be developed, where possible, to explain how the MA hazards should 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.

6.3.4 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.

Multi-discipline knowledge and experience shall be used to identify inherently safer design or specific barriers needed to optimize 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 MAs, and to provide effective emergency response. The aim is to optimize MA hazard management so that a consistent and balanced selection decision can be made.

6.3.5 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.

6.3.6 Sufficiency of measures

Preliminary strategies for managing credible 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 MA 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.

6.3.7 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 credible MA hazards;
- explanation of concept options eliminated due to high risk or perceived difficulty in developing design strategies for managing credible MA hazards;
- explanation of ranking of concept options for credible 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 optimization

7.1 General

The concept definition and optimization process shall be implemented in accordance with the plan for managing MA hazards, as illustrated in [Figure 3](#).

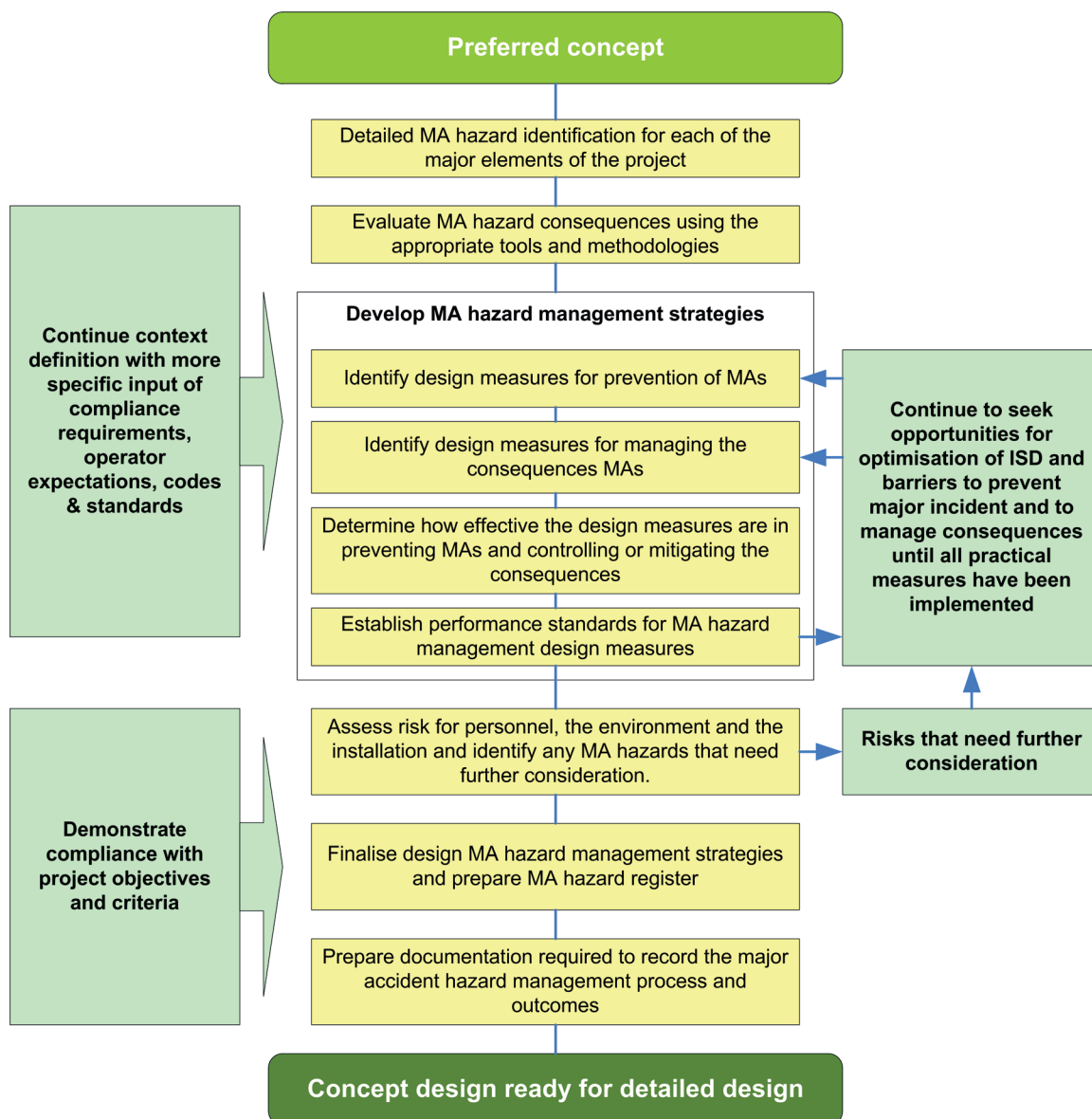


Figure 3 — Outline of concept definition and optimization

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 optimized 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 Hazard identification

MA hazard identification shall be through studies timed to provide input to design development such that design improvements can still be made.

7.3.2 Major accident hazard evaluation

MA hazard evaluation shall be conducted using a range of tools and methodologies.

Studies shall be timed to occur early in the phase and in time to implement design improvements subject to having sufficient design definition.

The studies and analyses shall be used to guide the design of ISD measures and barriers, including the following:

- evaluation of the benefits in terms of hazard management and risk reduction;
- determining the level of reliance placed on each measure within the design strategies for managing MA hazards;
- identifying the vulnerability of the measures to damage from MAs;
- determining the performance standards required to achieve the design strategies for managing MA hazards.

The evaluation of MAs shall be used to define the design accidental loads for the hardware barriers provided to manage MA hazards. The preference shall always be to design to withstand the worst case situation but this may not always be possible. In this case, the consequences of failure shall be evaluated and the impact on the overall project objectives assessed.

The evaluation of the MAs shall include assessing if unreliable human performance and the potential for error could affect a MA scenario.

Although the reliability of evaluation results will improve during this phase, it is possible that growth in potential consequences could occur during detailed design. Good practice and judgment will be required to provide predictions as to how the MAs could change with detail design and what allowances need to be made.

7.3.3 Risk assessment

The overall risks for people, the environment and assets associated with credible MA hazards shall be assessed before the end of this phase, including contributions made by each of the MA hazards identified.

Risk assessment results shall be used in conjunction with hazard evaluation to identify high risks that remain, and to provide inputs to design, particularly for ISD, hardware barriers and their performance standards.

7.3.4 Inherently safer design (ISD)

Development of ISD measures shall continue throughout this phase, and design strategies for managing MA hazards developed accordingly.

Early in this phase, the application of ISD shall focus on major design decisions, such as size and layout, structural barriers, structural strength to withstand credible MA loads, orientation to provide optimum natural ventilation.

Any ISD measures rejected in the screening and concept selection phase shall be reviewed to confirm that they are still not reasonable risk reduction measures.

Consideration of ISD options shall be applied to auxiliary system such as heating and cooling mediums, refrigeration systems, electrical systems, hydraulic and pneumatic systems and other similar utilities.

Performance standards shall be developed for those ISD measures which are defined as hardware barriers, and will need to be monitored for the life of the installation.

By the end of this phase, all the ISD measures shall be implemented, and design strategies for managing MA hazards that rely on them shall be defined in sufficient detail to provide confidence that no major change will be required during detailed design, unless there is a major change in the design concept.

7.3.5 Barriers

Development of the details of barriers shall continue throughout this phase, and the design strategies for managing credible MA hazards developed accordingly.

By the end of the phase, the range of barriers shall be fully established, although more detailed information will be required during detailed design.

7.3.6 Performance standards

Performance standards produced during this phase shall be unambiguous statements specifying the minimum expected performance required of the hardware barriers, using measures that can be verified by design documentation. They shall be defined in sufficient detail to provide confidence that major changes will not be required during detailed design, unless there is a change in the basis of design.

The performance standards shall reflect the likely demand on the hardware barrier, and whether readily available equipment and materials are able to achieve the required performance.

The effect of failure or impairment of each hardware barrier shall be evaluated to determine the performance required. Assessment of the implications of failure or impairment of hardware barriers (e.g. due to individual equipment failure) shall draw on equipment reliability and failure data, operating experience or specific evaluation (e.g. FMECA).

Assurance activities shall be defined in order to ensure that performance standard requirements are verified by relevant discipline engineers or responsible persons. Assurance activities expected in the detailed design, procurement, construction and commissioning shall also be defined, and form part of the contract for the next phase.

7.3.7 Sufficiency of measures

A multidiscipline review of MA hazard management shall be conducted before the end of this phase, in order to provide assurance that all credible MA hazards have been identified and subject to appropriate evaluation. The review shall assess whether the ISD and other barriers implemented are sufficient to achieve the project objectives for managing MA hazards and any external criteria defined for the area of operation.

The multidiscipline team shall review the following:

- work done prior to and during the concept definition and optimization stage for MA hazard management;
- how the MA hazard management objectives have been achieved;
- the identified MA hazards and their potential consequences;

- how credible MA hazards are managed by the design;
- summary of the key ISD measures and barriers, and their role in hazard management and emergency response;
- hardware barrier performance standards defined to date and further detail required;
- human barriers and expectations regarding reliable performance;
- readiness of the major hazard management aspects of the design to progress into detailed design, construction and operations;
- level of risk, assessed or calculated, for the design, and the expectation for further risk reduction during detailed design;
- any identified uncertainties and how these will be addressed in subsequent stages;
- basis for emergency response provisions (e.g. the emergency response strategy).

Particular attention shall be paid to areas of uncertainty and to any remaining MA hazards for which the consequences could be severe. The aim is to provide assurance that all reasonable measures have been implemented to reduce uncertainty or limit the severity of MAs, and that the strategies for managing MA hazards are sufficiently mature to provide a good basis for detailed design.

The review output shall be approved by the project management team; in some cases external acceptance can also be required by local legislation.

7.3.8 Documentation

Documentation produced in this phase shall demonstrate that MA hazard management activities have been conducted in accordance with the defined plan. Furthermore, it shall provide evidence that all credible MA hazards have been identified and understood, with effective design strategies for managing them developed.

A key deliverable for completion by the end of this phase is a plan of activities needed to manage credible MA hazards for the detailed design and construction phase.

This plan shall include the following:

- study programme and timetable for detailed design;
- details of specific areas of concern or uncertainty for further investigation or resolution in detailed design;
- actions management approach, including the role of contractors;
- verification schemes required to demonstrate that barrier performance is achieved, either through design documentation or physical inspection and test on site;
- a definition of further MA hazard management required.

8 Detailed design and construction phase

8.1 General

The detailed design and construction phase process shall be implemented in accordance with the plan for managing MA hazards as illustrated in [Figure 4](#).

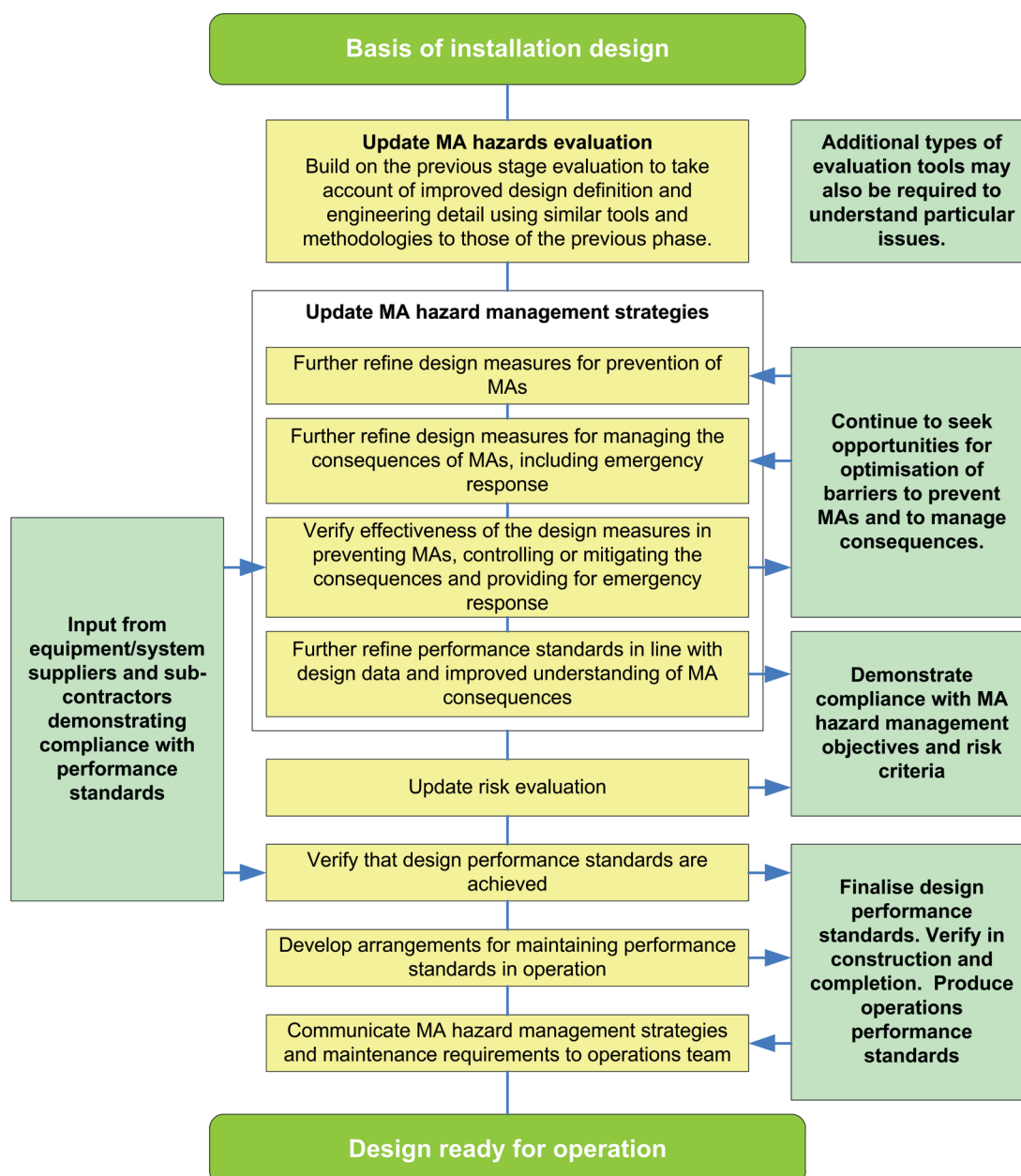


Figure 4 — Outline of detailed design and construction

8.2 Objectives

The primary objective of this phase shall be to build on the MA hazard management achieved during the concept definition and optimization phase through improved understanding of the MA hazards and refining details of the strategies for managing credible MA hazards, such that the installation is ready to operate.

8.3 Functional requirements

8.3.1 Overview

One or more primary contractors can be involved in detailed design, or contractors can be involved in supplying systems or elements that have a significant impact on MA hazard management. Arrangements shall be implemented so that contract boundaries are not an obstacle to seamless development, implementation and verification of design strategies for managing credible MA hazards.

Contractor responsibilities in this respect shall be defined in the contracts and interfaces for MA hazard management and action management defined and accepted by each contractor.

8.3.2 Hazard identification

Changes that are made shall be managed through a formal MOC process so that any requirements for hazard identification and further evaluation of MA hazards will be a part of that process.

8.3.3 Major accident hazards evaluation

Final evaluation of MA hazards shall be conducted using a range of tools and methodologies, with the purpose of further developing understanding of the MA hazards and their potential consequences. Provision shall be made for additional studies in response to issues that arise as a normal part of the detailed design development.

In the early part of this phase, any identified evaluation requirements and uncertainties or specific issues carried forward from the concept definition and optimization phase shall be evaluated, and solutions sought. These early studies shall be timed to allow potential design improvements to be implemented. Studies needed for assurance purposes shall be conducted to meet construction or completion milestones.

By the end of this phase, it shall be possible to verify that the models used to carry out any analysis are an accurate representation of the as-built installation. The models used for the final analyses shall be verified when construction is nearing completion and an on-site inspection of the installation can be conducted, e.g. ensuring that the physical layout, equipment and piping congestion are consistent with the model used to carry out the analysis. Any significant deviation shall be evaluated.

8.3.4 Risk assessment

The risk assessments carried out in the concept definition and optimization phase shall be updated to include detailed design data. These assessments shall define the risk for people, the environment and assets, and shall include contributions made by each of the identified MA hazards to demonstrate that the project will meet the project criteria for risk management.

The results of the detailed risk assessments of MA hazards could prompt changes in detailed aspects of the design. It is therefore necessary to start the process as early as reasonable, to allow the study to take place and feedback into detailed design.

8.3.5 Inherently safer design (ISD)

The scope for development of new ISD measures is likely to be limited during this phase, although opportunities shall continue to be sought. The main focus shall be to preserve the effectiveness of the ISD decisions made in earlier project phases.

Continued engagement of engineering managers and discipline engineers is important for the development and preservation of ISD measures, in order to ensure that they understand and implement the design strategies for managing MA hazards.

8.3.6 Barriers

The definition of barriers shall be developed further to include detailed design information and data from equipment suppliers.

Design strategies for MA hazard management should not change significantly during detailed design, although hardware barrier design definition and performance standards shall be refined to take into account improved design definition, particularly for vendor-supplied equipment. The only reason for significant change should be design changes that require revision of a MA hazard management strategy.

The effect that the failure of key component parts or human error could have on the ability of a hardware barrier to perform its function shall be updated, based on the more detailed knowledge of the barrier design and construction.

By the end of this phase, the hardware barriers shall be complete and shall provide confidence that risk-reduction through design measures has been optimized with sufficient redundancy or allowance for failure of equipment or failure in an MA.

8.3.7 Performance standards

The performance standards developed during the concept definition and optimization phase shall be fully defined during detailed design. The performance standards that require verification during procurement, completion and commissioning activities shall also be defined.

Design documentation that provides verification of performance standards shall be updated so that the basis for each hardware barrier and its performance standards can be traced.

For operations, those hardware barriers that the operations team will be required to monitor, inspect, test and maintain throughout the life of the facility shall be identified and documented.

Where appropriate, guidance shall also be prepared for the operations team to use in the event of failure or impairment of a barrier.

More detailed information about barrier performance standards is included in [Annex E](#).

8.3.8 Sufficiency of measures

The demonstration that sufficient measures are being provided to manage MA hazards shall continue during the design development.

Where further design measures are identified, but considered impractical, these shall be recorded, along with the reasons for rejection.

Construction normally starts before the end of detailed design; the measures for managing MA hazards shall be fully defined prior to the start of the relevant construction phase.

Arrangements shall be made for verification of satisfactory implementation of the measures for managing MA hazards. Self-verification is often acceptable, although a common strategy is to employ an external organization to provide independent verification.

Prior to completion of construction, the modelling used to carry out the evaluation and risk assessments of managing MA hazards shall be verified as an accurate representation of the as-built facility. Significant changes identified at this stage shall be referred to the project management for review and agreement about any remedial action necessary.

8.3.9 Register of major accident hazards

The register of MA hazards shall be updated during detailed design phase to reflect the increased level of design information, results of detailed MA evaluation and the range of ISD measures and barriers implemented.

8.3.10 Documentation

Documentation shall be produced during this phase to demonstrate that the process adopted for managing MA hazards has produced an installation that satisfies the project objectives.

The documentation shall demonstrate that the overall outcome of the process for managing MA hazards is a design which is ready to be carried forward into operation. This means that all the key elements of managing MA hazards are in place and verified. Where planned MA hazard management actions