INTERNATIONAL STANDARD

ISO 17776

Second edition
2016-12-15

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

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

Reference number
ISO 17776:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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
measureable 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.

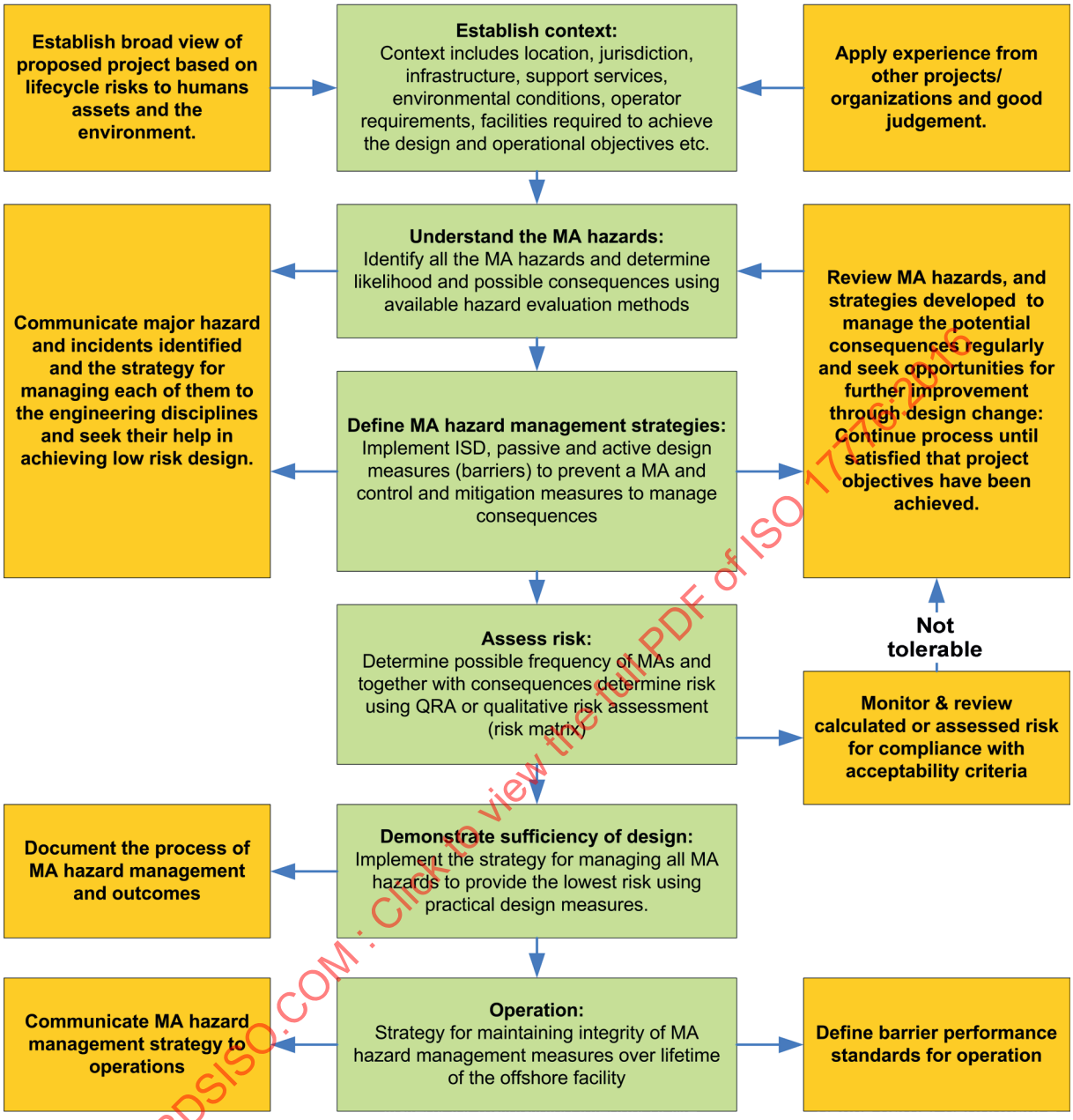

Figure 1 — Overview of managing MA hazards

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.

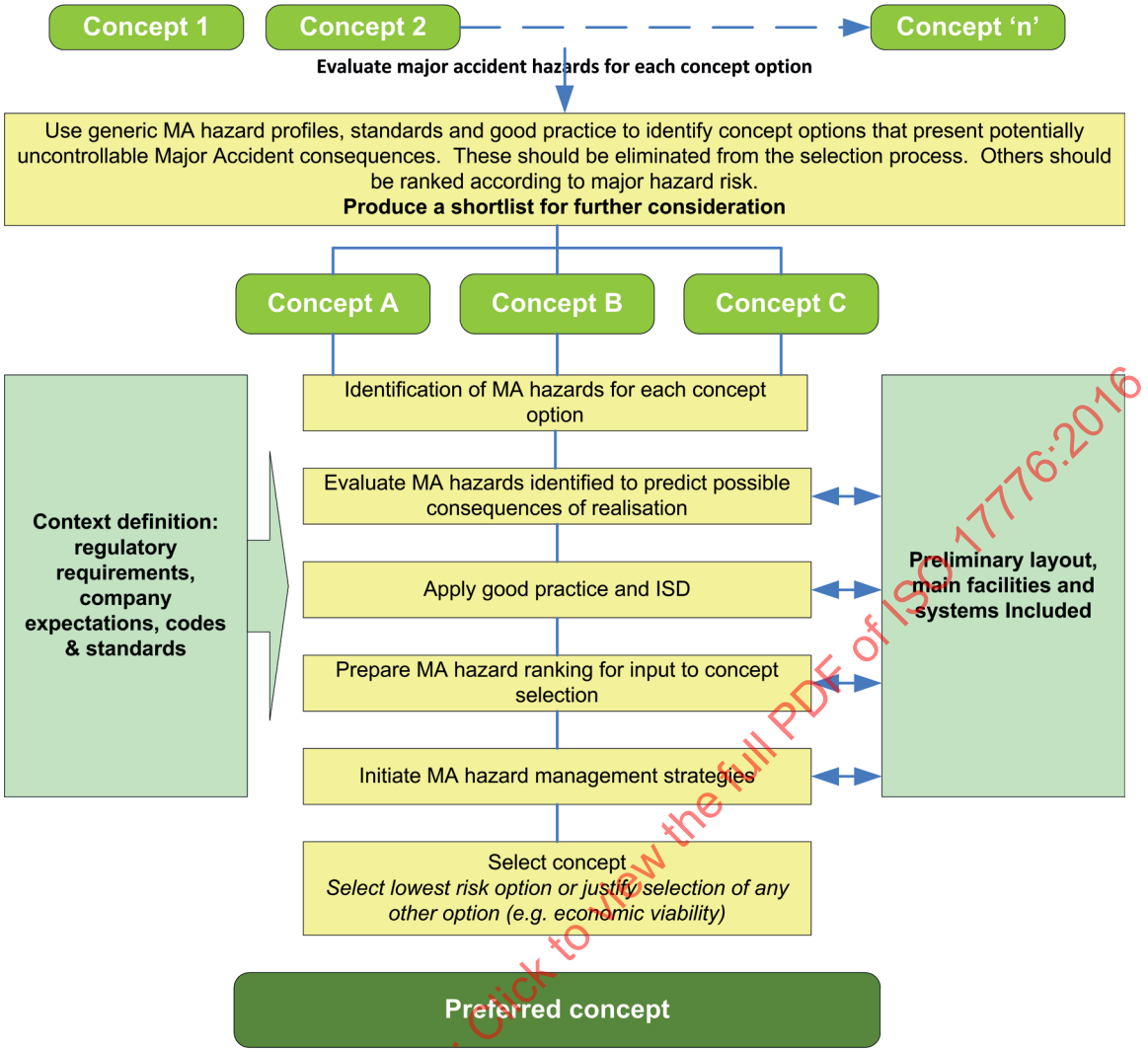

Figure 2 — Screening and concept selection process

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.

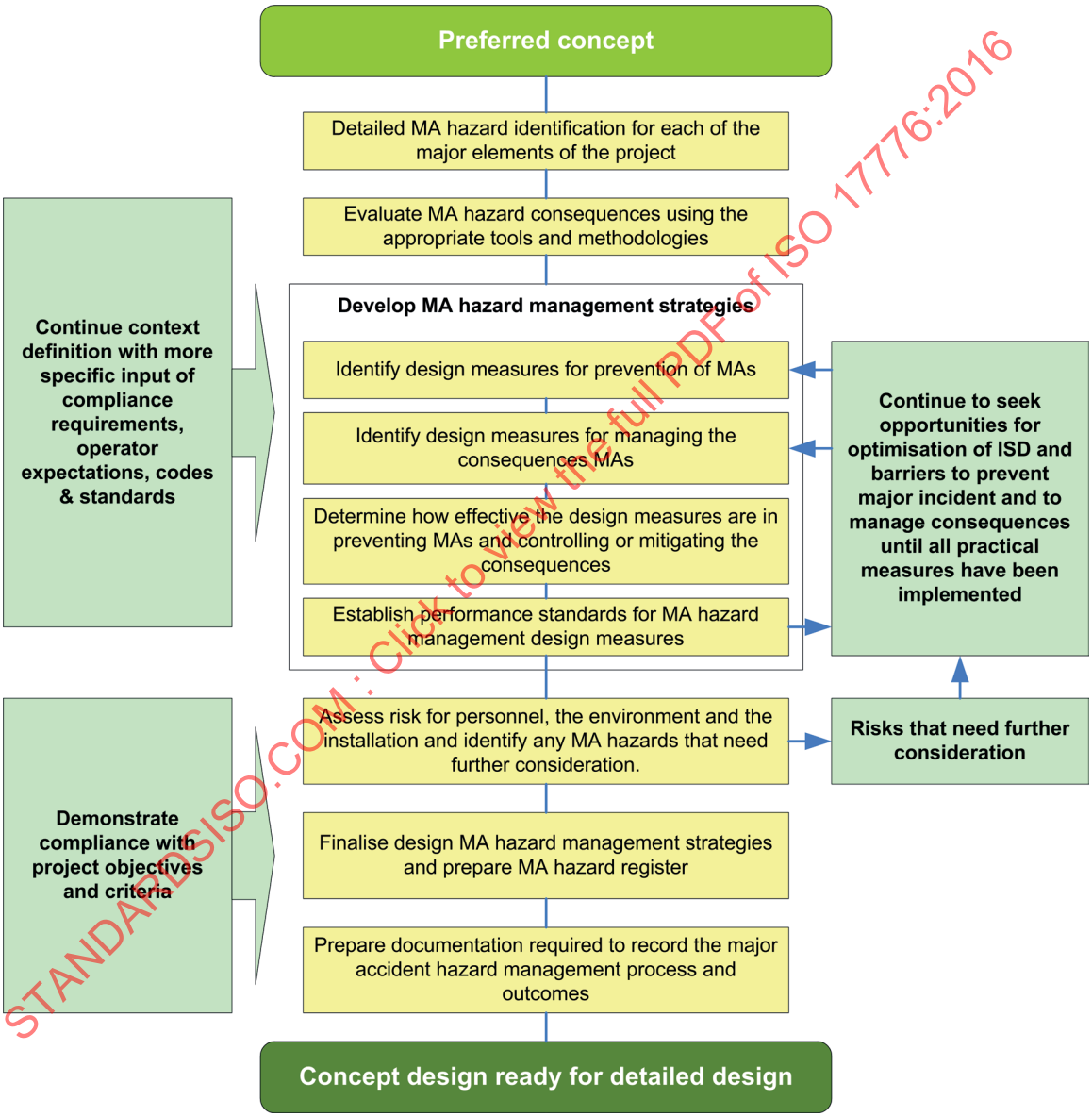

Figure 3 — Outline of concept definition and optimization

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.

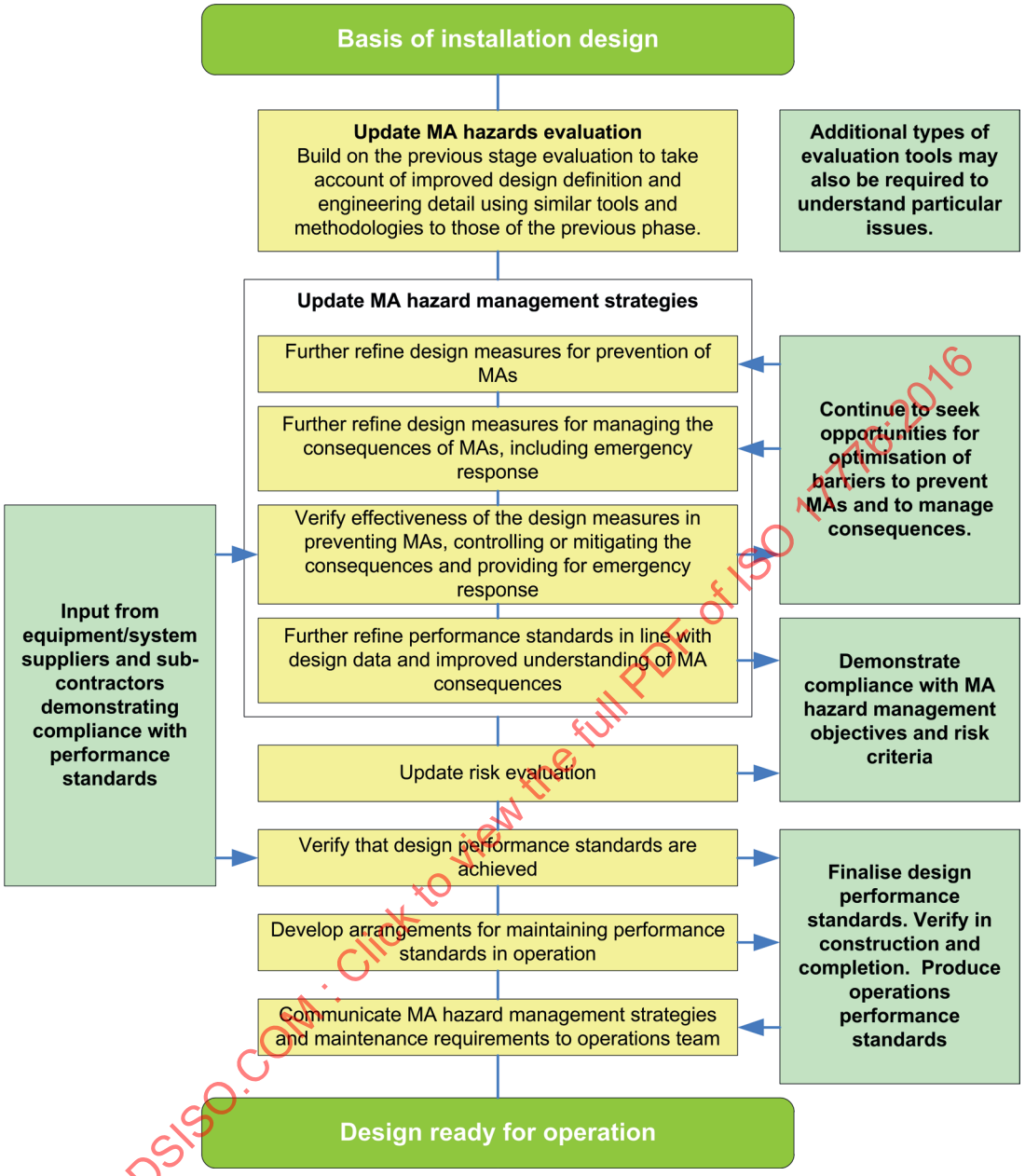

Figure 4 — Outline of detailed design and construction

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

have not been completed or have been rejected, this shall be recorded with the demonstration that the overall hazard management objectives will still be achieved.

8.3.11 Procurement of equipment

The specifications for procurement of equipment and materials shall include a clear definition of requirements necessary to achieve the ISD measure and hardware barrier performance standards. Although some requirements can be included in the specifications directly, for example a maximum acceptable passing/leakage rate for a valve or its accessibility requirements, some standards will need to be translated into measures that the vendors and contractors can understand. In general, vendors and contractors might not have the knowledge of MA hazards management necessary to interpret the barrier performance standards.

When conducting pre-delivery acceptance (factory acceptance tests), it is important that the parameters specified for meeting performance standards are included.

8.3.12 Construction, completion and commissioning

Clear definition of requirements for the ISD features of the installation and the barrier performance standards shall be provided to the contractor executing the construction work. This information shall be supplied in time for the construction contractor to make the necessary arrangements to meet these requirements during the construction programme. Construction contracts which are placed before such information is available shall specify that the construction contractor shall meet the requirements for ISD and hardware barrier performance standards once this information is available.

As part of commissioning, meeting of the performance standards shall be verified through inspection and testing. The inspection and test schedules shall include the activities necessary to verify that the as-built facilities meet the performance standards.

8.3.13 Transfer to operation

Knowledge transfer to the operations team is essential in preparation for the operational phase. Any assumptions made during design about how specific facilities will be operated, and expectations regarding human performance or error potential, shall be made available to the operations team in a form that facilitates their understanding and use of the information.

Part of the information transfer shall be requirements on the appropriate periodic inspection and testing of measures for MA hazard management (ISD and hardware barriers). If the operations team wants to change these requirements, then the design strategies for managing MA hazards shall be reviewed and changed as necessary to account for the changes.

Any failure of ISD measures or barriers shall be assessed for their significance to MA hazard management. Remedial measures necessary to restore the performance of barriers in the operational phase is outside the scope of this document.

A review of any temporary activities planned during the pre-operation phase or after operation has begun shall be conducted to determine whether there is an impact on MA hazard management and risk (e.g. installing risers after production has started). Considerations shall include the possible increase in risk associated with construction activity, possibly heavy lifting, and other hazards close to an operating plant. In addition, there is likely to be an increase in manpower requirements that need to be managed within the limitations of emergency response provisions. The outcome of this review shall be used to propose operational limitations or extra protection as necessary.

8.3.14 Actions management

Actions that relate to design shall be closed prior to completion of this stage. Actions that can only be managed by the operations team shall be handed over to them as early as possible, in order to get their agreement to complete the action. On completion of this stage, a handover report shall be prepared

to record the actions completed, any actions rejected with the reasons for rejection, and any actions accepted by the operations team.

9 Major accident hazard management in operation

9.1 General

Managing MA hazards and seeking risk reduction measures shall continue throughout the life of the installation.

Planned inspection and testing shall continue to demonstrate the performance of MA hazard management measures, and any failures or trend towards reduced performance shall be recorded. Remedial work shall be done in a timely manner to prevent significant increase in risk.

Any changes to the installation or to operating conditions shall be evaluated and managed through a MOC process, with the appropriate update of design strategies for managing MA hazards.

Field data needed to verify MA hazards management shall be collected and subject to further analysis if necessary to allow judgement on the effectiveness of the arrangements provided for MA hazards management.

Figure 5 illustrates the process of MA hazard management in operations.

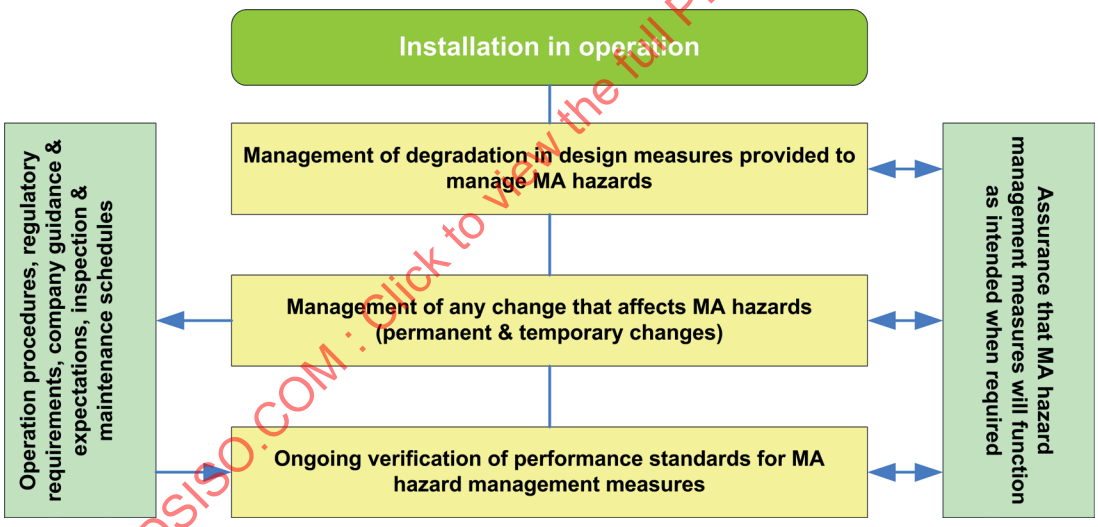

Figure 5 — Outline of operation

9.2 Objectives

The primary objective shall be to ensure that risk to people, the environment and assets is not increased over time. To achieve this, it will be necessary to

— maintain barriers such that the overall cumulative performance of barriers is sufficient to manage the risk,

— avoid progressive increase in risk resulting from changes to the operating parameters or degradation of barrier performance, and

— avoid increase in risk as a result of design or operational changes to the installation.

The process for continuous improvement in managing MA hazards is outside the scope of this document.

9.3 Functional requirements

9.3.1 Barrier management

Barrier management in the operations phase shall require that the performance standards for the ISD measures and hardware barriers are regularly inspected and/or tested, and appropriate actions are taken to re-establish performance of degraded barriers or implement compensating measures. This shall initially be in accordance with a schedule produced by the design team, but may be modified after experience in operations providing that there is no impact on the MA hazard management strategy.

The schedule of periodic inspections and tests for barriers shall be managed through the operations inspection, testing and maintenance system, and shall include the following:

— Periodic inspection and testing of hardware barriers, carried out in accordance with the schedules and activities defined in the operation maintenance management system.

— Timely maintenance or other remedial work necessary to restore any failure or impairment of barriers to their full functionality. Assessments shall be made of the impact of failure, unavailability or degradation, and ensure that overall barrier performance is maintained.

— Means to recognize and record creeping changes in performance, in order to identify potential failure to meet design intent (creeping changes are, e.g. successive minor changes that occur over a period of time and that, if taken individually, are not sufficient to trigger an MOC process).

People involved in the inspection and maintenance of barrier performance shall be competent to perform the tasks, and have a good understanding of the role of the barrier in managing MA hazards and the significance that any deviations in performance will have on safe operation.

9.3.2 Revalidation

Revalidation of design strategies for managing MA hazards shall be carried out periodically, with a suggested interval of no longer than every 5 years, to include review of the following:

— register of MA hazards, to verify continuing validity or to identify any changes that have occurred;

— record of reliability/availability of hardware barriers during the intervening period, to identify equipment that is not as reliable as expected;

— changes in manning profile that result in more or fewer people located in hazardous areas;

— changes resulting from creeping, or other changes in composition of process fluids;

— changes to equipment and facilities, either permanent or temporary.

— changes affecting human barriers, the potential for error and expectations regarding reliable human performance.

The results of this revalidation shall be used to identify if any changes are needed to the arrangements for managing MAs such as the emergency response strategy, training requirements, safety critical equipment, safety critical tasks/activities, mechanical integrity activities and operational procedures.

9.3.3 Safety-critical tasks

The tasks required to maintain barrier performance standards shall be identified and their significance in the overall MA hazard management shall be clearly defined. This information shall be included in the operational procedures, training and competency requirements and updated as necessary as an integral part of the location MOC process.

Safety-critical tasks shall be assessed using an appropriate task analysis method.

9.3.4 Temporary changes

Planning for temporary changes shall include a review of the likely impact of the change on the design strategies for managing MA hazards. Significant temporary changes or activities shall be reviewed and managed through an MOC process.

Examples of temporary changes and their impacts are listed below:

— introduction of temporary process equipment which can

  1) increase the risk of a hydrocarbon release;

  2) increase the risk of ignition of hydrocarbon releases;

  3) cause obstruction to explosion vent paths or to escape and evacuation routes.

— scaffolding, habitat and other temporary structures which can cause obstruction to natural ventilation or block the view of surveillance equipment;

— temporary structures which increase congestion that can potentially increase explosion overpressure;

— temporary equipment and/or structures which obstruct access to critical control, mitigation emergency response equipment;

— storage of chemicals which introduce a hazard not expected when developing the design strategies for managing MA hazards;

— overall increase in the number of people on board to beyond that assumed in the design strategies for managing MA hazards.

9.3.5 Non-availability of barrier performance

If failure to meet barrier performance standards occurs, and early remedial measures are not possible, an immediate evaluation of the implications for MA hazard management strategy shall be carried out, including the following:

— implement guidance provided in the performance standards specification for operation;

— if such guidance is not applicable or available, assess the consequences of the failure and determine whether the plant should be shut down or continue to operate in a limited form while remedial work is carried out;

— notify the appropriate operations management and put in place suitable measure(s) for mitigation;

— conduct a review as soon as practicable to assess the change in MA hazard management and risk, and identify additional measures that shall be implemented to mitigate any increase in risk;

— develop an action plan to include the change in design strategy for MA hazard management, the measures implemented to mitigate additional risk and the expected time to remedy the failure.

Failure of a hardware barrier to meet its performance standards is most often caused by failure of one or more components. Guidance provided in the performance standards specification (produced during the preparation for operation stage) shall provide information on the significance and practical measures that can be implemented to mitigate any additional risk.

9.3.6 Management of change (MOC)

The general principles for managing change given in 4.10 shall be fully applied in the operational phase to both physical and organisational changes. All proposals for change that can cause a material change shall be assessed for possible impact on MA hazards, the design strategies for managing them and any change in the potential for human error. Where necessary to ISD measures and barriers shall

be implemented to maintain the MA hazard management strategy at least comparable to current strategies.

All proposals for change shall be recorded, made available for review by the appropriate people and approved or rejected in accordance with the installation decision-making process. This process shall be fully documented.

Annex A
(informative)

Example of a framework for risk-related decision support

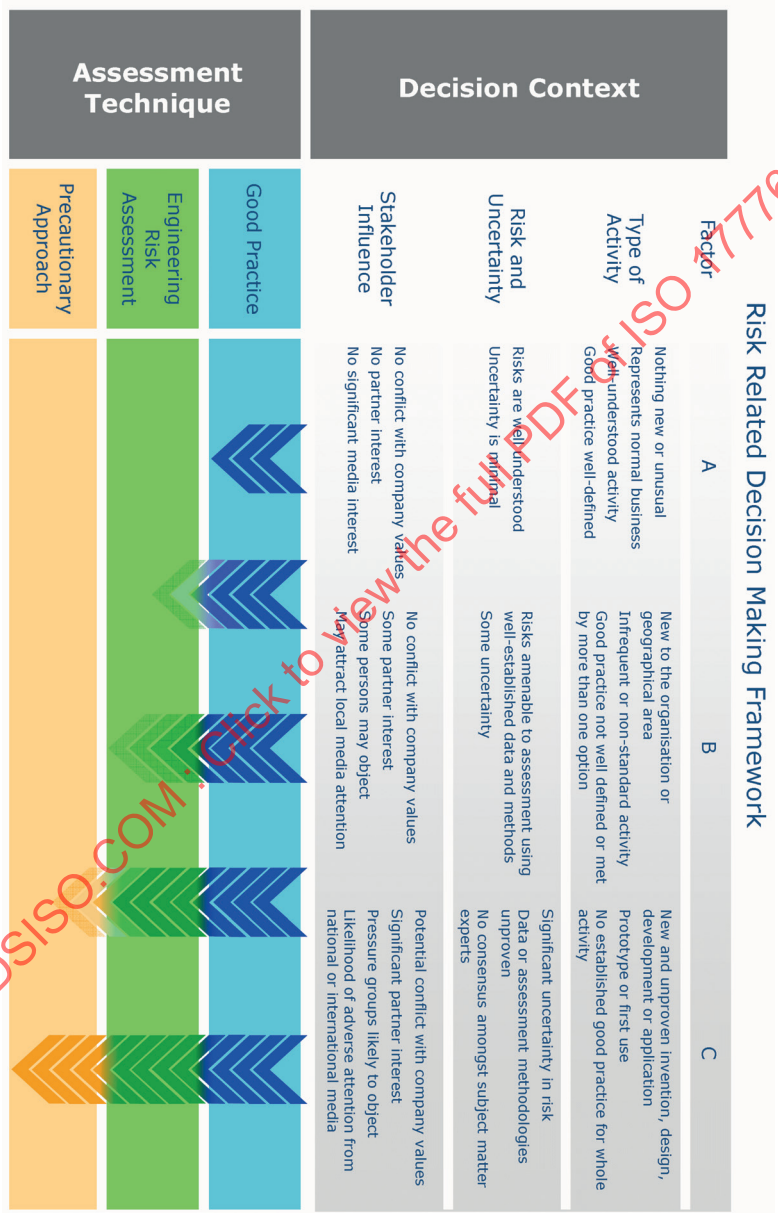

Figure A.1 — Framework for risk-related decision support

Annex B
(informative)

Plan to manage major accident hazards

B.1 General

The plan to manage MA hazards during the various design phases of an offshore installation should provide a consistent framework for defining the activities necessary to effectively manage potential incidents. It should set out the requirements in advance of each phase, in order to raise awareness of the process to be implemented and define accountability. It should be targeted towards the whole project engineering community, including contractors and significant system and equipment suppliers. The plan can be combined with an overall project plan covering other aspects such as general safety, health, security and environmental requirements.

Specific requirements should be defined at the outset of the project, and then periodically updated as the work progresses and requirements change. The plan adopted for each project can vary in format and content depending on many factors, including company standards, legislative requirements in different regions of the world and the type of project. The following clauses provide examples of the range of information commonly included.

B.2 Scope of the plan

The scope describes the period covered by the plan and the elements of the overall project covered, for example:

— design and procurement;

— construction, integration, completion;

— transportation;

— hook-up, commissioning and handover.

B.3 Basis for the plan

The plan can be based on the company policy regarding safety and the environment, regional legislative requirements or a policy determined by the project management team.

B.4 Regulatory compliance

The primary regulations applicable to the operating location should be listed.

B.5 Primary codes and standards

The codes and standards that are the overarching basis for the project should be given. This includes, for example, ISO standards, company engineering standards, certifying authority requirements, etc. The specific standards to be applied for the MA hazard management process should also be included.

B.6 Goals and criteria

The MA hazard management goals and criteria for the project should be defined in terms that can be measured or demonstrated.

For example:

a) Qualitative goals:

   1) MAs should be minimized by inclusion of ISD measures and passive hardware barriers where practicable;

   2) people should be able to survive the identified MA consequences within the temporary refuge and achieve successful evacuation to sea when necessary.

b) Quantitative goals:

   1) individual risk should be defined for those people most exposed to MAs;

   2) group individual risk/fatal accident rate, etc. should be defined for all people on board;

   3) frequency of safety function impairment from all sources (immediate and delayed) should be defined;

   NOTE Safety functions cover those functions that need to be intact in order to ensure the safety for people and/or to limit pollution, e.g. escape routes, temporary refuge, central control room and others rooms of significance.

   4) estimated frequency of environmental damage, such as oil spills, should be defined.

Various industry standards give guidance on conducting quantitative evaluations (e.g. NORSOK Z-013, Lloyd's Register Guidance Notes for the Calculation of Probabilistic Explosion Loads[53]) and on risk-related decision-making (e.g. Oil and Gas UK guidance[64]).

B.7 Project organization

The organization of the project for each of the stages should define the relationships of key functions and people, including relationships between the company and contractor teams. There should be a clear indication of the organization required to provide the necessary authority and support for conducting effective MA hazard management.

B.8 Responsibilities, leadership and commitment

Responsibilities and accountabilities for MA hazard management for each of the key functions and people should be clearly set out. As a minimum this should include:

— the project manager;

— the engineering manager;

— the lead design safety manager or engineer;

— the lead discipline engineers.

B.9 Contracting arrangements

The requirements for MA hazard management for any contractor appointed to carry out work for any phase of the project should be defined.

Primary design and procurement contractors are expected to demonstrate a good understanding of the requirements and competency to develop and implement design strategies for managing MA hazards, in order to meet the stated objectives. The same applies to subcontractors employed to design and supply significant subsystems (e.g. integrated process control and safety systems). For this reason it is important to agree with the contractor how these expectations will be achieved in advance of contract award.

Prospective contractors are normally expected to demonstrate competency and agree the arrangements for MA hazard management prior to the final award of the contract.

B.10 Procurement

Arrangements for specification and verification of the quality and reliability of systems and equipment that form part of a hardware barrier system should be defined.

B.11 Study programme and timing

The study programme should be defined and updated where necessary to ensure that studies are carried out at the appropriate time and to an agreed scope, or terms of reference. Examples of studies that can be required are included in Annex C.

B.12 Arrangements for action management

The arrangements for transferring actions arising from the hazard identification and other safety reviews and studies should be defined, along with details of how each of these actions will be formally approved, tracked and closed out.

B.13 Arrangements for assurance and verification

The plan should detail the arrangements for tests and checks to verify performance of ISD measures and barriers during procurement of equipment and systems and final completion of construction and commissioning.

B.14 Overview of timing of key deliverables

Table B.1 provides an overview of timing of key deliverables for MA hazard management.

Table B.1 — Timing of key deliverables for MA hazard management

Managing major accident hazards activity/ deliverables[a]	Project phase				Notes
	Screening and concept selection	Concept definition and optimization	Detailed design and construction	Operations[b,c]	
Plan to manage MA hazards	First issue	Updated	Updated		Issued specific to each phase, and details requirements for next phase
Register of MA hazards	First issue	Updated	Updated	Maintained	
Summary of MA hazard management	First issue	Updated	Updated	Maintained	May be a safety case/ major hazards report in some jurisdictions
Action management	Process followed	Process followed	Process followed	Process followed	
Management of change	Process followed	Process followed	Process followed	Process followed	
ISD report	First issue	Updated	Updated	Maintained	
MA hazard management design strategies	First issue	Updated	Updated	Maintained	See ISO 13702 for fire and explosion strategy and ISO 15544 for emergency response strategy
Design performance standards		First issue	Updated		Design performance standards are converted into operation performance standards during DD&C phase
Operational performance standards			First issue	Maintained	See Annex D
Review of MA hazard management process applied		First issue			
HAZID review	First issue	Updated	Updated	Maintained	HAZID is primarily to allow comparison of the different development options during operations performed, if any significant changes occur
Concept risk assessment	First issue				Ranking of concepts
Active geological processes	First issue	Updated			Geological issues can have a significant impact and need to be identified as early as possible. See ISO 19900:2013, 5.13.2
HAZOP review		First issue	Updated	Maintained	

[a] The scope and amount of activities to be performed should be dependent on the complexity of the installation being designed.

[b] Documents listed to be reviewed for impact as a result of Brownfield modifications.

[c] Documents listed as maintained to be available for each installation, and revalidated at least every 5 years.

Table B.1 *(continued)*

Managing major accident hazards activity/ deliverables[a]	Project phase				Notes
	Screening and concept selection	Concept definition and optimization	Detailed design and construction	Operations[b,c]	
Explosion hazard analysis		First issue	Updated	Maintained	
Fire hazard analysis		First issue	Updated	Maintained	
Smoke and gas dispersion/ ingress analysis		First issue	Updated	Maintained	
Escape, evacuation and rescue (EER) analysis		First issue	Updated	Maintained	
TR integrity analysis		First issue	Updated	Maintained	
Dropped object assessment		First issue	Updated	Maintained	
Ship collision assessment		First issue	Updated	Maintained	
FMECA		First issue	Updated	Maintained	
Emergency system reliability/ survivability analysis		First issue	Updated	Maintained	
Risk assessment		First issue	Updated	Maintained	
Integrity of instrumented systems analysis		First issue	Updated	Maintained	
Human factors analyses		First issue	Updated	Maintained	In particular, the identification of safety-critical and barrier-related tasks, and the necessary design requirements to support them.
Task risk analysis			First Issue	Maintained	Safety-critical tasks should be assessed using task risk analysis. See Reference [56].
Environmental risk assessment		First issue	Updated	Maintained	

[a] The scope and amount of activities to be performed should be dependent on the complexity of the installation being designed.

[b] Documents listed to be reviewed for impact as a result of Brownfield modifications.

[c] Documents listed as maintained to be available for each installation, and revalidated at least every 5 years.

B.15 Summary of key activities in the design phases

Table B.2 provides the screening and concept selection activities. Table B.3 provides the concept definition and optimization activities. Table B.4 provides the detailed design and construction activities

Table B.2 — 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 or complex 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 all credible MA hazards; — conduct a high-level assessment of concept options, mainly to identify credible MA 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 hazard identification 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 functions for reducing the impact of MA consequences; — assess whether potential MA 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 the major hazards that potentially could lead to a high risk.
ISD and barriers	— identify ISD measures that could reduce the likelihood of MAs and the possible consequences; — identify any unusual or high criticality barriers required to manage potentially severe but credible MAs; — propose a generic range of barriers to support a multilayer design strategy for MA hazard management; — 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 optimization phase.

Table B.3 — Concept definition and optimization activities

Hazard identification	— identify the MA hazards for each of the major elements of the installation development (e.g. production facilities, pipelines and sub-sea systems, marine facilities and systems); — review the identification and evaluation of MA hazards from the previous phase and update as necessary to ensure that all credible MA hazards are identified; — increase confidence that no further MA hazards will be identified in detailed design.
MA hazard evaluation	— use improving design definition to deepen understanding of those aspects of the design that are important to managing MAs (e.g. layout, process design, risers and their hazardous inventories); — conduct a programme of reviews and analyses of credible MAs, to understand their causes and the potential consequences, using appropriate tools and methodology; — use results to test the beneficial effect and sufficiency of ISD measures, barriers and other proposed design strategies for managing hazards; — revise and update assessment and analyses as necessary to provide ongoing improvement in understanding of credible MAs and their potential consequences; — make allowances for possible increase in severity of MAs as a result of likely increase in equipment and congestion during the detailed design phase; — demonstrate that understanding of MAs is sufficient to support the related strategies, and that they are suitable to be carried forward for detailed design.
Assess risk	— use risk assessment or analyses methodologies to develop predictions of frequency with which credible MAs could occur; — combine with results of the evaluation of the possible consequences of MAs, to assess the risk for people, the environment and assets; — take account of the developing design strategies for managing credible MAs; — predict the contribution to risk made by each of the MAs identified and identify those contributing the most for further review and reduction; — provide a high level of confidence that the operation risk management objectives will be achieved following detailed design.
ISD	— seek opportunities for ISD and implement ISD measures that will provide effective and reliable design strategies for managing credible MAs and reduce the need for human barriers; — ensure that ISD measures are identified and implemented early in this phase and before key aspects of the design definition become fixed; — define the range of ISD measures required for managing MAs by the end of this phase; — identify remaining detailed specifications to be completed in the next phase.
Barriers	— develop a range of barriers, in addition to ISD measures, required to support a multi-layer design strategy for MA hazard management for each of the identified MA hazards; — include hardware barriers designed to reduce the likelihood of a MA arising from identified MA hazards (prevention); — include hardware barriers designed to provide control and mitigation of the major accident consequences predicted by the MA hazard evaluation process; — identify where human barriers are required or necessary; — relate the number and type of barriers to the severity of consequences predicted; — define the range of barriers required for managing MAs by the end of this phase; — identify remaining detailed specifications which need to be completed in the next phase.

Table B.3 *(continued)*

Performance standards	— define the role of each hardware barrier in managing MAs; — define performance criteria for functionality, reliability/availability and survivability; — evaluate the effect of failure or impairment of each hardware barrier, and how that could change the design strategies for managing MAs that rely on that barrier; — ensure performance standards for all barriers and ISD measures have been defined, at least in a preliminary form, by the end of this phase, leaving only some of the detail specification for the next phase; — identify remaining detailed specifications to be completed in the next phase; — make a preliminary assessment of assurance activities to be performed in next phase (detailed design, procurement, construction and commissioning).
Sufficiency of measures	— demonstrate that design strategies for managing MAs are sufficient to provide effective prevention, control and mitigation of each identified major hazard; — demonstrate that emergency response arrangements are sufficient for the credible MAs on the installation. — identify remaining uncertainty, particularly where there can be a sensitivity to detail design changes; — evaluate the likely impact of failure or impairment of barriers when in service, to determine any dilution of design strategies for managing MAs; — provide assurance that the design strategies for managing MAs are sufficient to achieve the project objectives and criteria.
Register of MA hazards	— prepare or update previous-phase register of MAs as early as reasonable in this phase, and include the design strategy for MA hazard management developed for each MA identified; — define uncertainty remaining and the action required during detailed design to address any uncertainty.
Documentation	— produce approved reports for all activities for managing credible MAs, including evaluation and risk analysis; — prepare documentation that describes the status of managing MA hazards at the end of this phase; — explain the reasoning used to develop the design strategies for managing MA hazards and further development work required in the next phase. — prepare a plan for managing the MA hazard management activities needed during the detailed design and construction phases.

Table B.4 — Detailed design and construction activities

Hazard identification	— hazard identification is only likely to be required if there are major changes during detailed design or if there are inputs from equipment/suppliers and subcontractors that impact the previous hazard identification work; in these cases, the impact on hazard management strategies need to be assessed by first updating the hazard identification work.
MA hazard evaluation	— use detailed design definition to refine design aspects that relate to the MA hazard management (e.g. layout, process design, risers and their hazardous inventories); — conduct a programme of review, analysis and assessment of credible MA hazards using the appropriate tools and methodologies to improve and finalize understanding of them, their causes and the potential consequences; — use results to update barrier performance standards and to verify that ISD measures and hardware barriers implemented are capable of achieving the performance throughout the life cycle of the installation; — conduct specific reviews and studies where necessary to address significant increases in severity of consequences of MAs as a result of detailed design.
Assess risk	— use risk assessment or analysis methodologies to refine and finalize assessment of frequency with which credible MAs could potentially occur; — combine with results of MA consequence evaluation to predict the risk for people, the asset and the environment; — provide a final risk analysis report that predicts the overall risk to people, the environment and assets and the contribution made by each of the MA hazards identified.
ISD	— although ISD measures will largely have been implemented in previous phases, continue to seek opportunities for implementing further ISD measures.
Barriers	— use detailed design data to finalize the design of barriers for MA hazard management.
Performance standards	— use detailed design data and updated evaluation results of MAs to finalize the operational barrier performance standards for functionality, reliability/availability and survivability; — verify that the design, specification and quality of equipment used, are consistent with their performance standards; — develop a suitable methodology for inspection or test of barrier performance standards during procurement (e.g. factory acceptance tests) and during construction and commissioning; — identify those hardware barrier performance standards that require inspection, testing and maintenance during operation for inclusion in the operations maintenance systems.
Sufficiency of measures	— provide a final demonstration that design strategies for managing MA hazards will be effective for each identified major hazard including a final assessment of the potential for human error; — finalize demonstration that emergency response arrangements are sufficient for the credible MAs on the installation. — finalize the evaluation of the likely impact of failure or impairment of hardware barriers through individual failure of component parts, or failure of the complete barrier; — provide assurance that design strategies for managing MA hazards are sufficient to achieve the project objectives and criteria.
Register of major accident hazards	— finalize the register of MA hazards for handover to the operations team.
Documentation	— produce reports for all activities supporting the management of MA hazards, including hazard evaluation and risk analysis; — record any MA Hazard Management actions that have been rejected with the reasons for rejection and any actions not completed, — prepare documentation that explains MA hazard management both for operations and for any subsequent change to the installation.

Annex C
(informative)

Major accident hazard management identification and evaluation tools

C.1 Introduction

IEC 31010:2009 provides a general overview of good practices in selection and use of risk assessment techniques that are relevant to many industries and types of system. This annex provides guidance on a number of the specific tools that are commonly applied in the design of offshore production installations.

C.2 Hazard identification (HAZID)

C.2.1 Objectives

The objectives of HAZID are to use structured review techniques to identify all hazards associated with a particular concept, design, operation or activity, including the likely initiating causes and possible consequences or safeguards.

C.2.2 Typical input information

Dependent on the selected HAZID technique and on the phase of development or level of maturity input information typically includes the following:

— details of the installation layout and equipment arrangement (e.g. from design drawings and/or project computer-aided design model);

— process flow diagrams (PFDs);

— details of the inventories of hazardous materials;

— piping and instrumentation diagrams (P&IDs);

— operating/control/shutdown philosophies/procedures;

— details of any unusual features (e.g. hostile environment);

— experience of other, similar facilities in the area, or generally.

C.2.3 Description/Narrative

Various techniques are available for HAZID. Most techniques involve a team approach, with the team having a mix of expertise and involving all relevant disciplines and stakeholders.

A HAZID technique appropriate to the complexity of the installation, the stage of the installation in its life cycle, and the scale and nature of the MA hazards on the installation should be employed, e.g.:

— structured brainstorming (guideword-based), generally termed HAZID;

— preliminary hazard assessment (see IEC 31010);

— checklists;

— “what-if” analysis.

A structured approach should be taken to ensure that no hazards, initiating events or sequences of events, are overlooked. A comprehensive process for identifying these hazards would normally include consultation with the workforce and if appropriate, contractors and suppliers.

Identification of MA hazards generally requires a structured, guideword-based approach (usually termed a HAZID), as it is able to cover low-frequency events and hence relates better to MA hazards (and QRA) than other techniques.

Guidewords are an important element of a HAZID, and should be sufficiently comprehensive to stimulate identification of hazards and discussion, while avoiding the possibility of being too onerous for the stage of development. The HAZID facilitator is usually charged with adapting the guidewords to the specifics of each HAZID. Example guidewords are given in Annex F.

A hazard identification exercise can also involve qualitative or semiquantitative risk assessment/ranking of the hazards.

The HAZID should be fully documented, using HAZID worksheets showing clear linkages between hazardous events, hazards, underlying causes and control measures/safeguards, where appropriate, as well as capturing actions. The HAZID worksheets are normally used by the scribe to record the meeting proceeds and outcomes live as the meeting progresses.

In general, the approach should be applied to each area and hazard guideword, for example asking the following questions:

a) Is the guideword hazard-relevant, or is there something similar that should be identified?

b) Is the type of hazard well understood in this context, or new/uncertain?

c) What are the likely causes that could lead to realization of hazard consequences (major accident)?

d) What are the credible and worst-case potential consequences?

e) What are the ISD measures and barriers already specified (or expected)?

f) Are there any additional ISD measures or barriers that could be proposed?

g) Are there human barriers or expectations regarding reliable human performance and are they reasonable?

h) Is further analysis required to understand the consequences of the hazard?

i) What recommendations should be made (actions for follow up)?

Actions arising from the HAZID should be managed and closed out in an auditable manner.

HAZID should be carried out throughout the life cycle of any installation, but is particularly important in the early stages of design so that, where practicable, hazards can be eliminated through the application of ISD principles.

Plant/process modifications should be subject to HAZID, to ensure that changes to existing hazards, or the introduction of new hazards, are appropriately managed.

C.2.4 Use of output

HAZID forms the basis of all activities related to MA hazards management, and is thus used as input to:

— the evaluation of incidents related to MA hazards;

— risk assessments;

— the development of MA hazard management strategies [e.g. identifying, evaluating, defining and justifying the selection (and rejection) of ISD measures and barriers];

— the definition of performance standards;

— the register of MA hazards.

C.3 Job hazard analysis (JHA)

C.3.1 Objective

The objectives of a job hazard analysis is to use a qualitative method to assess risks associated with a particular job in order to decide upon the precautions and contingency provisions that should be taken to reduce the risks.

NOTE JHAs are broadly similar to activity hazard analysis (AHA), job safety analysis (JSA) and task hazard analysis (THA).

C.3.2 Typical input information

Typical input information is dependent on the specific JHA to be undertaken, but typically would include:

— relevant experience of the work including any incident history (internal and external);

— the task description and job steps;

— location and environment where the work will be undertaken;

— the skills and experience of those who will be involved with the work;

— the tools, equipment and resources that will be involved with the work.

C.3.3 Description/Narrative

The exact format of the evaluation can differ from company to company, but the general approach involves breaking the job or activity down into a number of logical steps needed to accomplish the task. For each step, a number of questions are asked in order to identify hazards, consequences and risks associated with that particular step and the precautions and contingency measures that can be taken.

For each step in the job, typically the following approach would be adopted:

— Identification of hazards:

  — What exactly is going to be done?

  — What materials will be dealt with?

  — What tools and equipment will be used?

  — When will the job be done (daytime, night-time, time of year, etc.)?

  — Where will the job be done (at height, in confined space, etc.)?

  — How might the task affect people, activities or equipment close by?

— Assessment of the consequences of the identified hazard. This is usually done using a scale of high, medium or low. In this context, the following questions are useful:

  — What is the effect of the hazard?

  — Is it a short-term or long-term effect?

  - Does it affect the equipment or people?
  - How much damage can it cause?
  - How many people can be hurt?
  - Is the effect immediate or is there a time delay allowing escape?
- Assessment of the probability of occurrence of the hazard. This is, again, usually done using a scale of high, medium or low. In this context, the following questions are useful:
  - Is it likely that the hazard will arise every time the job is done or will it be less frequent (once in 10 times, or 100 times or once in a lifetime)?
  - If the unsafe situation arises is it certain the worst will happen?
  - Do the characteristics of the job, the people doing it or the equipment being used have any effect on the probability?
- Determination of the risk associated with the action. Again, often carried out using a scale of high, medium or low, calculated using the product of the probability of occurrence and the consequences. The following logic is usually applied: high × high = high, high × medium or medium × high = high, high × low or low × high = medium, medium × medium = medium, medium × low or low × medium = medium, low × low = low.
- Determination of precautions that can be taken to guard against the risks identified. Precautions can be identified by the following types of questions:
  - Would rescheduling the work reduce the risk?
  - Can concurrent activities be phased apart?
  - Are there physical actions possible to reduce the probability of occurrence?
- Assessment of the residual risk after feasible precautions have been taken. This involves identifying contingency measures that would reduce the consequence in the event of a hazardous situation. The normal form of such questions is "What if ...?" In order to ensure uniformity of approach and a systematic evaluation, it is normal to use a standard form to undertake JHA. This allows the precautions and contingency measures to be clearly identified and can then act as a checklist to ensure implementation.

JHA is best undertaken by a small team of people who are fully conversant with the equipment, systems and procedures to be used during the job, and can approach the analysis using logical thought and common sense.

C.3.4 Use of output

The primary output from the study is changes to how the job will be executed in order to reduce the risk so far as is reasonable. The results of the work also indicate the residual risk that will remain and this can be helpful when assessing those activities that are part of a human barrier in the management of MAs.

C.4 Explosion hazard analysis

C.4.1 Objectives

Explosion hazard analysis applies recognized analysis tools (e.g. CFD or phenomenological tools) to develop the design accidental loads (overpressure and drag) for structure, equipment and piping systems. See Reference [62].

C.4.2 Typical input information

Input information for explosion hazard analysis typically includes the following:

— details of the layout and equipment arrangement (e.g. from design drawings and/or project computer aided design model);

— the areas of the installation where explosion hazards have been identified;

— definition of inventory isolation and depressurization (blowdown) and likely release scenarios identified (e.g. location, release rate, gas volume, composition, ignition source location, wind conditions);

— elements of the installation that should be designed to withstand explosion loading to allow them to perform their function.

C.4.3 Description/Narrative

There are various levels of sophistication that are available for explosion modelling. Whichever approach is used, the models should have been validated against large scale explosion tests.

The basic steps in the analysis are as follows:

a) Define any critical assumptions to be used in the modelling (e.g. models to be used, areas to be considered, release scenarios to be used, initial degree of turbulence, elements of the installation to be designed to withstand explosion loads).

b) Develop the scenarios to be considered. This can be dynamic, based on modelling the gas build-up for various release rates and locations, or static, i.e. based more on fixed gas volumes in different parts of the area.

c) Determine the explosion loads for the various scenarios.

d) Repeat the modelling if there is any significant change or increase in detail for the areas being considered.

Conservative assumptions should be used in explosion modelling to reflect the uncertainty in the study basis, especially in the early stages of a project when the definition of layout and equipment arrangement is not finalized.

A sufficient range of explosion scenarios should be modelled to provide a good level of confidence that an appropriate design accidental load can be established.

For areas which are not open, loading from both the internal and external parts of the explosion should be considered. An external explosion can cause significant loads on enclosures and equipment away from the area of ignition.

For CFD modelling of explosions, it can be possible to develop a three-dimensional geometric model of the installation by an automatic conversion from the project computer-aided design model. For analyses conducted before the final detailed model is available, additional congestion in the form of “typical” piping and equipment should be added to try to reflect the finished installation. The geometric models to be used for explosion analysis should be checked for accuracy before analysis begins.

If is not reasonable to design for the estimated explosion loads, QRA or other frequency assessment tools (e.g. Monte Carlo simulation) should be used to assess the frequency that the loads will exceed the resistance of critical equipment and structure. This allows a judgement to be made on the realistic design loads for the installation and in some jurisdiction this is call the dimensioning accidental load.

The benefit of potential hardware barriers to protect against high consequence, low probability MAs, which significantly exceed the design resistance should be assessed when deciding whether to implement a hardware barrier. For example, activation of water deluge on gas detection can only have a limited impact on the design load, but in a large gas cloud, there can be a potential for deflagration-to-

detonation-transition leading to severe damage. In this case, if water deluge is activated before ignition, it can prevent the strong flame acceleration and thus significantly reduce the consequences.

It can be possible to reduce the estimated explosion loads by providing explosion relief devices (e.g. vents), though care is needed if flow towards a vent will increase turbulence leading to higher overpressures.

C.4.4 Use of output

The results of explosion analysis are given as

a) overpressure: transient increases in pressure due to the expanding combustion products of an explosion, and

b) drag: directional loading due to the passing air/gas flow.

The load imposed by an explosion can be expressed in terms of

— elastic limit: maximum load which structure and facilities can withstand without permanent deformation or loss of function (sometimes referred to as "strength level blast"), or

— ductile limit (above the level of 1): load causing permanent deformation of structure or damage to facilities but without leading to failure or further loss of containment integrity (sometimes referred to as "ductile level blast"), or

— failure load: load causing failure of structure or containment integrity.

The results of explosion analysis should be used to define the structural strength to be provided by those elements of the installation required to provide resistance to blast and drag loads as part of the MA hazard management strategy. These loads should be included in the relevant performance standards. Elements of the installation to be considered include:

a) structure (primary and secondary);

b) boundaries (floors, walls, ceilings) to the area involved in an explosion;

c) process containment (e.g. risers, large vessels, piping, etc.) to prevent escalation by release of additional inventory;

d) enclosures (e.g. local equipment rooms, switch rooms, control rooms, etc.), particularly those considered critical under MA conditions;

e) emergency response provisions (e.g. escape routes, TR, and evacuation facilities).

The design load used for equipment and structures may be either the maximum calculated over pressure load or the load that the function or system needs to withstand to meet some defined risk tolerability criteria (dimensioning accidental load).

C.5 Fire hazard analysis

C.5.1 Objectives

Fire hazard analysis should apply recognized fire-modelling tools to predict potential fire load effects on structure and equipment, particularly ISD measures and barriers. See also ISO 13702.

C.5.2 Typical input information

Input information for fire hazard analysis typically includes the following:

— details of the layout and equipment arrangement (e.g. from design drawings and/or project computer-aided design model);

— wind rose/wind data if there are wind-exposed areas;

— areas of the installation where fire hazards have been identified;

— definition of inventory isolation and depressurization (blowdown) and likely release scenarios identified (e.g. location, release rate, composition, wind conditions), including release rate over time;

— types of release scenarios (e.g. pressurized liquid or gas, non-pressurized liquid pool) that should be modelled to provide the likely fire loads;

— elements of the installation that should be designed to withstand fire loading, and to what level of severity (often referred to as design accident load) that can be less than the maximum for some elements, if it is demonstrated that

  — failure of an element can be tolerated without causing harm to emergency response provisions or leading to uncontrolled escalation of an MA, and/or

  — that the frequency of severe fire load is low.

C.5.3 Description/Narrative

There are many different tools and levels of sophistication available for fire modelling. No matter which approach is used, the tools should be validated against fire tests.

The following basic types of scenario should be considered:

— Pressurized jet fire: fire due to flammable gas or vaporized liquid spray or a combination of both. The heat load on structure and equipment can be very high, but can reduce over time if the pressure falls (e.g. as a result of isolation and blowdown).

— Liquid pool fire: fire due to flammable liquid forming a pool with an open surface area that allows vaporization and burning of the vapour. Depending on location and ventilation, a pool fire can produce a large quantity of toxic smoke. The heat load is less than that of a jet fire, but still significant.

— Boiling liquid expanding vapour explosion (BLEVE): most commonly occurs when a pressure vessel containing flammable liquid is heated, possibly by a fire in another area nearby, and the combination of heat and increased pressure causes catastrophic failure of the vessel structure. The liquid released expands and vaporizes very quickly, leading to a rapidly expanding ball of fire. A catastrophic failure of a vessel with a significant hydrocarbon vapour volume at pressure (e.g. a separator) would lead to much of the same consequences as a BLEVE, with strong pressure waves, projectiles, and a large flameball followed by a major pool fire.

In the fire hazard analysis, the following basic steps should be carried out:

a) Define any critical assumptions to be used in the modelling fires, e.g. models to be used, areas to be considered and loss of containment scenarios to be used, elements of the installation to be designed to withstand pool fires or jet fire loads.

b) Develop the scenarios to be considered. This should include isolatable release cases and un-isolatable releases cases used to model the likely effect of isolation failure under MA conditions.

c) Determine the fire loads on nearby structure, equipment and piping for the various scenarios.

d) Conduct sensitivity modelling to provide confidence that the maximum realistic design case has been determined.

e) Repeat the modelling if there is any significant change or increase in detail for the areas being considered.

In general, conservative assumptions should be used in fire modelling, especially in the early stages of a project when the definition of layout and equipment arrangement is not finalized.

A sufficient range of fire scenarios should be modelled to provide a good level of confidence that the design accidental loads have been determined.

C.5.4 Use of output

Results of fire hazard analysis are used to estimate the heat loads imparted by fire on structure, equipment and piping systems over time, in order that suitable passive and/or active protection can be developed.

Output is given as:

— the fire and radiated heat loads on emergency response provisions, including whether escape routes remain passable, TR remains capable of protecting people for the defined period and evacuation facilities remain available for use;

— the fire loads on structure, piping, vessels and enclosures (e.g. local equipment rooms, switch rooms, etc.), particularly those considered critical for the function of hardware barriers under MA conditions;

— passive fire protection requirements for TR, escape routes, enclosures, critical structural, piping, vessels, etc. in order to meet the design strategies for managing MA in the event of a fire;

— identification of the passive fire protection requirements for the areas and facilities identified (e.g. B, H or J rating);

— identification of the areas and facilities that require active fire protection;

— active fire protection requirements for the areas and facilities identified (e.g. type and density of coverage).

C.6 Smoke and gas dispersion and ingress analysis

C.6.1 Objectives

Smoke and gas dispersion and ingress analysis should apply recognized modelling tools to predict:

— dispersion of gas (toxic or flammable) following accidental release;

— dispersion of smoke produced by an identified fire hazard;

— potential ingress of gas and/or smoke to utility enclosures (e.g. equipment rooms) and the TR.

C.6.2 Typical input information

Input information for smoke and gas dispersion and ingress analysis typically includes the following:

— Details of the layout and equipment arrangement (e.g. from design drawings and/or project computer-aided design models).

— Areas of the installation where gas or liquid release sources have been identified and evaluated, and a nominated release location within these areas for the purposes of smoke and gas dispersion (e.g. open deck or within a module).

— Release characteristics (e.g. composition, mass flow rate over time) and the type of fire (e.g. gas jet fire, pool fire). For pool fires, the likely surface area of liquid is required, particularly if bounded by deck size or bunding (for the purposes of MA pool fire evaluation, drip trays under equipment are not normally able to contain a large liquid release).

— Key target areas for results (e.g. gas or smoke concentration at the TR boundary, air intakes, evacuation facilities, etc.)

C.6.3 Description/Narrative

There are many different tools and levels of sophistication available for modelling of gas and smoke dispersion, depending on the level of detail required. Due to the complexity of air flow around an offshore installation, CFD-based tools provide the highest level of resolution. Whichever approach is used, the tools should be validated.

In the smoke and gas dispersion/ingress analysis, the following basic steps should be carried out:

a) Evaluate the dispersion of smoke and un-ignited flammable gas using release-source analyses produced as part of the explosion and fire hazard evaluations. Toxic gas concentration at source is calculated independently from its concentration in the fluid stream. Before starting, it is necessary to define the conditions, including:

   — Location of gas-release sources to be analysed, and the orientation of release direction (e.g. up, down, east, west, etc.).

   — Wind speeds and directions to be evaluated, taking into account the installation orientation and the prevailing wind conditions. The worst-case wind condition should also be evaluated (this can be towards the TR and evacuation facilities).

   — Data points for which the gas concentration is required (e.g. escape routes, enclosure boundaries, TR, air intake points, etc.).

b) Define any critical assumptions to be used in the modelling.

c) Take account of failure of internal pressurisation under MA conditions, which can be caused by isolation of air intakes on detection of smoke or gas, damage to the system components or failure of power supplies. Enclosure leakage integrity is the primary protection against ingress.

d) Conduct sensitivity modelling to provide confidence that the maximum realistic design case has been determined.

e) Repeat the evaluation with updated model if there is any significant change or increase in detail for the areas being considered.

C.6.4 Use of output

Results of smoke and gas dispersion analysis are used to develop understanding of how any MA can impact people, either directly or indirectly through impairment of working areas, escape routes, TR and evacuation facilities.

Output is given as:

— Flammable or toxic gas concentrations at nominated points on the installation, based on the initial release composition and mass flow rate. Measurement criteria are usually based on the percentage of lower explosive limit for flammable gas, and on concentration, expressed in parts per million, for toxic gas.

— Concentration of smoke at nominated points on the installation, relative to concentration at the fire source. Measurement criteria can be based on obscured visibility, CO_2 concentrations or other parameters depending on the analysis method.

Flammable gas, toxic gas or smoke concentrations, and the length of time present around utility enclosures and TR or air intakes, should be used to guide the design of enclosure leakage rates as well as detection requirements and the actions to be taken when smoke or gas is detected (such as isolation of air intake ducts, isolation of equipment inside an enclosure not rated for the presence of gas, transfer of control of the MA to a location not affected by smoke or gas, etc.).

C.7 Escape, evacuation and rescue (EER) analysis

C.7.1 Objectives

Escape, evacuation and rescue analysis involves assessment of the facilities provided, in order to determine whether they meet the emergency response strategy and project goals under MA conditions. In this context, the following actions should be evaluated:

— escape to the TR from any area where people may be working or off-duty;

— protection of people in the TR or muster area for the pre-defined period;

— controlled evacuation of all people, and recovery or rescue, if necessary.

The assessment is followed by identification of any shortcomings in EER arrangements and measures for their improvement.

See also C.8, ISO 15544 and References [48], [63] and [64].

C.7.2 Typical input information

Input information for escape, evacuation and rescue analysis typically includes the following:

— emergency response, escape and evacuation strategy, and supporting documents (e.g. philosophy, procedures);

— project and regulatory requirements (e.g. regulations, standards, operating procedures);

— details of the layout and EER-related systems (e.g. alarm system, escape/egress routes, muster points/TR, primary evacuation facilities, other means of evacuation or escape to sea, internal and external search and rescue arrangements);

— MA scenarios identified and their evaluation outcomes (e.g. toxic release, fire, explosion, smoke, ship collision, loss of stability, earthquake, etc.);

— results of the TR integrity analysis;

— key input data and assumptions (e.g. manning levels, impairment criteria, EER decision model, evacuation success probabilities).

To avoid any misunderstanding, a clear definition of each of the following terms should be included:

a) escape to the TR/muster location;

b) controlled evacuation;

c) primary evacuation means;

d) secondary evacuation measures or escape to sea;

e) recovery and rescue.

C.7.3 Description/Narrative

The EER analysis evaluates the performance of the emergency response facilities and procedures under major accident scenarios. The evaluation is performed for each element of emergency response against the performance standards in term of functionality, adequacy, availability and survivability.

In EER analysis, the following basic steps should be carried out.

a) Define and document any critical assumptions to be used in the analysis. These typically include:

— evacuation and rescue strategy to be established, if not already available;

- manning levels for the range of predictable activity levels likely during operation;
- criteria for impairment of emergency response facilities due to physical effect of heat radiation, toxic/flammable gas concentration, explosion, smoke;
- (for quantitative study) fatality probability during the process of escape/egress, mustering, embarkation, evacuation and rescue.

b) Set performance goals for each element of emergency response. These typically include:

- emergency alarm/communication;
- escape/egress/access routes;
- TRs/mustering facilities;
- primary evacuation facilities (e.g. lifeboats, lifeboat embarkation points);
- secondary/tertiary evacuation/escape to sea facilities (e.g. helicopters, heli-deck, life rafts, escape chutes, sea-entering devices);
- personal protective equipment;
- search and rescue arrangements (e.g. helicopters, stand-by vessels).

c) Develop scenarios to be considered at various locations of the facility. The locations should encompass the entire facility and the scenarios should capture the complete range of MA scenarios identified.

d) At each location, based on MA consequence analysis (e.g. flammable or toxic gas, fire, explosion, smoke, ship collision), determine how the ER facilities could be impacted by the consequences and whether the EER performance standards can be met.

e) If shortcomings are identified, propose improvement options and re-evaluate until EER performance standards can be met. Practicable alternative EER arrangements should be identified and similarly evaluated for additional benefits and incurring cost.

f) Determine time required for:

- People to escape from the impacted location and all other areas of the installation to a TR or muster location, taking into account identified impairment potential.
- The on-scene commander to evaluate the MA, account for all people at muster or in defined ER positions, conduct on-facility search and recovery of any casualties and assess the need for controlled evacuation. This should take into account the availability of feedback information from the hazardous areas (e.g. fire and gas detection, confirmation of ESD, etc.).
- Controlled evacuation if considered necessary (e.g. loading of lifeboats and launching).

C.7.4 Use of output

Results of EER analysis are used to develop understanding of how any MA can impact people while escaping to the TR or muster locations, sheltering in the TR/muster location and during controlled evacuation, if that proves necessary.

This understanding should be used by the project to

- improve the EER arrangements in order to meet the required performance under MA conditions, or
- provide assurance that the facilities are sufficient for the required task and meet the performance standards.

Taking into account the range of ISD measures and barriers implemented for MAs, EER analyses should result in:

a) identification of those MA hazards that could cause impairment of the escape routes, and whether some or all people could be prevented from reaching the TR within the time specified in the performance standards (e.g. maximum 15 min);

b) implications for the protection of people if TR integrity analysis predicts that some MA hazards could lead to impairment within the time specified, and whether early controlled evacuation could be successful;

c) identification of those MA hazards that could cause impairment of the evacuation facilities and prevent controlled evacuation;

d) sensitivity analysis to assess the aspects considered to be deficient, and what measure are required for their remedy;

e) confirmation that performance standards for time required for evacuation of the facility and rescue of people from lifeboats or the sea have been achieved (or not);

f) risks to people during escape, muster, evacuation and rescue.

C.8 Temporary refuge (TR) integrity analysis

C.8.1 Objectives

A TR integrity analysis involves the use of recognized fire and explosion evaluation, smoke and gas dispersion analyses and impact analyses to demonstrate that TR structural integrity and functionality of emergency response barriers are capable of supporting the survival of people within for a predetermined period under MA conditions (e.g. explosion, fire, heat, smoke). See also ISO 15544.

A TR impairment analysis is a calculation of impairment frequency based on modelling of barrier failure probabilities.

C.8.2 Typical input information

Input information for TR integrity analysis typically includes the following:

— details of the layout and equipment arrangement (e.g. from design drawings and/or project computer aided design model);

— the pre-determined period for which the TR should remain able to perform its emergency response role (e.g. 1 hour) under MA conditions;

— definition of the TR boundary, entrance and exit points, external air intakes, exhaust ducts and associated dampers;

— identification of

  — ISD measures, structural measures and other passive hardware barriers for the management of MA hazards that could cause TR impairment (e.g. fire and blast barriers), and

  — hardware barriers for protection of people inside the TR following an MA (e.g. enclosure leakage integrity, ventilation and internal pressurization).

C.8.3 Description/Narrative

In TR integrity analysis, the following basic steps should be carried out.

a) From the various outputs from MA evaluation, identify those that could cause impairment of the TR or of the services that provide for the protection of people inside. These include:

   — fire and explosion hazards, including direct explosion effects (e.g. overpressure, structural deformation and missile damage), fire at the boundary and radiated heat from fire elsewhere;

   — ingress of smoke or gas (see C.6);

   — impact from marine vessels or helicopter crash (including possible fire);

   — other source of direct damage (e.g. impact energy from rotating machinery).

b) Determine whether the TR/muster locations are those least likely to be impaired by the effects of the identified MA hazards, including direct impact, structural failure, explosion or fire, heat, gas (toxic or flammable) or smoke.

c) Define any critical assumptions to be used in the analysis, such as what constitutes impairment.

d) Under the identified MA conditions for possible TR impairment, assess whether, for the predetermined period:

   — the boundary of the TR is likely to remain intact and maintain a low leakage rate (e.g. 0,3 air changes per hour);

   — emergency access doors are likely to remain available for all people who survive the immediate effects of the incident to gain entry;

   — systems that provide support for the survival of people within the TR are capable of continuing to function;

   — systems required to provide incident control feedback to the control room, allowing an informed judgment to be made about evacuation, are capable of continuing to function;

   — barriers are capable of preventing escalation from causing impairment of the TR within the predetermined period;

   — evacuation provisions remain capable of performing their designated function when required, and are not impaired by the identified MA effects (unless that is addressed as part of an EER analysis; see C.7);

e) Conduct sensitivity modelling to provide predictions of the time scale for impairment of the TR, should the identified MA not be controlled within the predetermined period.

C.8.4 Use of output

Results of TR integrity analyses are used for

— identification of those MA hazards that could cause impairment of the TR or the services that provide for the protection of people inside, either immediately or over time,

— confirmation of (or deficiencies in) the location and/or structural integrity necessary to provide the required emergency response role for the predetermined period, and

— confirmation of (or deficiencies in) the design of supporting systems.

This information is used to guide design improvement to reduce the likelihood of MA impairment of the TR, or to provide assurance that people will be protected from the effects of the MA for the predefined period.

C.9 Dropped object assessment

C.9.1 Objectives

The objectives of dropped object assessment are to

— identify and evaluate MA hazards associated with dropped or swinging objects from lifting and mechanical handling activities, and

— provide inputs to the philosophy of mechanical handling and to the design of dropped object/swinging load protection of facilities considered necessary to mitigate the potential risk of an MA.

See also References [37] and [47].

C.9.2 Typical input information

Input information for dropped object assessment typically includes the following:

— mechanical handling philosophy;

— 2D and 3D (if available) layout of surface and subsea facilities;

— description of loads and lifting or handling routes [dimensions and shape, mass (full and empty), lifting routes, lifting height and lift frequency];

— description of lifting appliances [type of crane, lifting potential and operating limits (e.g. mass, height, distance, lifting rates), design and operational safety controls (e.g. alarms, lock-out zone)];

— generic and site-specific mechanical lifting failure data;

— impact strength criteria for decks and other structures that exist to provide protection for vulnerable systems and equipment;

— nature, scale and consequence of MAs associated with vulnerable systems and structures (e.g. loss of containment, structure collapse).

C.9.3 Description/Narrative

In dropped object assessment, the following basic steps should be carried out:

a) From operational lifting patterns of equipment, identify structures or areas that could be at risk of

   — a falling load, boom or crane;

   — collision with a swinging load or crane boom.

b) Estimate the level of damage potentially imparted to the above systems or structural elements.

c) Evaluate the consequences and escalation potential from

   — release of hazardous materials and subsequent fire, explosion, etc.;

   — structural damage or progressive collapse;

   — damage to essential safety systems.

d) Identify opportunities to mitigate hazard by design, typically

   — alternative lifting routes, crane/laydown locations;

   — automatic lock-out zones;

— design of vulnerable systems or structural elements against maximum predicted accidental loads, or the provision of protective structures;

— use of cranes designed for high risk application (see NORSOK R-002:2012, Annex K);

— duplication of lifting equipment;

— design for sequence of failure.

Where hazard cannot be engineered out during the design, frequency arguments should be introduced to quantify the risk, and risk mitigations should be tested until risks associated with crane operations are found to be tolerable.

In general, the initial dropped object study is qualitative and forms the basis from which more accurate and specific quantitative evaluation can be carried out.

For surface lifts, basic geometrical considerations should be used to determine the potential for loads, booms or cranes to strike vulnerable items. The influence of atmospheric conditions (wind, swell, waves) on the predicted motion of the load should be taken into account.

Impact energies should be calculated from standard equations of motion. The mechanisms, i.e. bending, displacement, indentation and deformation of the load and the impacted item, by which the impact energy is dissipated should be considered for estimating that portion of it available for causing damage and failure. Detailed finite element analysis can be performed for better accuracy.

The data basis for frequency evaluation of lifting failures should be specified. Internationally recognized statistical data are given in References [37] and [47].

When assessing exposure of subsea systems to dropped objects, various techniques can be employed for predicting the sink trajectory of objects through the water column. The assessment can be approached deterministically or can use generic probabilistic distributions from experimental data/literature. Bespoke hydrodynamic simulations may have to be performed when no published data can be found to determine the fall trajectory with any accuracy, particularly in deep waters. The influence of current on maximum predicted excursions, as well as the initial drift before the object sinks, should be considered. Subsea systems may also need to consider the hazards of over-trawling or anchors and the protection needed to prevent these leading to significant damage or an MA.

The risk should focus on the impact on MAs. Personnel exposure related to non-escalating falling/swinging loads should be covered as an occupational risk.

C.9.4 Use of output

The output of the assessment should be used to allow a judgment on the vulnerability of facilities to dropped object/swung load hazards, the likelihood and consequences of these event and whether design changes or modifications to the mechanical handling philosophy are needed.

When hazard cannot be eliminated at source, risk can be mitigated for example by:

— designing systems or protective structures against reasonably foreseeable impact loads;

— maximizing lifts during plant turnarounds;

— prohibiting lifting above live high-risk equipment;

— using alternative handling methods, such as dual lifting systems;

— observing crane operating limits;

— integrity management of lifting systems (inspection, maintenance, verification);

— competency/training of people involved in the procedures;

— establishing clear sightlines and communication procedures;

— limiting simultaneous operations;

— establishing contingency plans and emergency procedures.

Preference should always be given to passive rather than active means of control/mitigation. Reliance on operational measures should only be considered at the last resort when other more robust risk management options are not possible, not practicable to implement, or not sufficient to meet design MA hazard management targets.

The results of the dropped object assessment should be used to define the credible impact energies that critical systems are required to withstand, and should input into the overall QRA and emergency systems survivability analysis.

C.10 Ship collision assessment

C.10.1 Objectives

The objectives of ship collision assessment are to

— identify credible impact from marine vessels operating within the field or shipping outside the control of the installation and assess the potential impact load and damage potential, and

— predict the probability that impact could cause failure of structure and increased level of risk.

C.10.2 Typical input information

Input information for ship collision assessment typically includes the following:

a) For marine vessels operating under the instruction or the control of the installation owner (e.g. supply vessels, standby vessels, construction/installation vessels, oil-offloading tankers, etc.):

   — predicted frequency and type of marine vessel operations within the exclusion zone around the installation including:

   — properties of the marine vessels including their station-keeping method;

   — duration of marine vessel operations;

   — understanding of ownership and command structure for marine vessels serving the installation.

b) Where relevant, predicted failure rates for dynamic positioning systems.

c) For shipping and other marine activities not under the control of the installation owner:

   — identification and proximity to shipping lanes and frequency of large vessel passage;

   — data relating to potential deviation of these vessels from shipping lanes, or their breakdown.

C.10.3 Description/Narrative

Impact with a large ship or in-field vessel is the cause of many MA hazards, particularly those involving riser or well (conductor) release and significant structural damage.

The basic steps for assessing the potential impact force and their likely consequences for vessels operating within the exclusion zone are as follows:

a) determine whether all vessels are under the direction of the offshore installation manager, and what control measures are in place for those not directly under the offshore installation manager's direction;

b) obtain predictions of expected marine activities of operational support vessels (e.g. supply vessels, standby vessels, accommodation vessels, construction/installation vessels, oil-offloading tankers, etc.);

c) predict the likely severity of possible impact, taking into account the type of vessels involved, their approach speed, and requirements for manoeuvrability and position holding;

d) given the uncertainty of vessel impact evaluation, a predetermined value for impact energy is commonly established and a prediction made as to the circumstances under which this value can be exceeded;

e) where necessary, install hardware barriers to prevent impact leading to structural failure and loss of containment integrity of risers, conductors or process plant.

If information on shipping frequency and vessel size is available, an estimate of collision risk can be calculated using a recognized method of assessing possible ship deviation from its allotted route sufficiently to impact the installation.

Common causes are loss of ship motive power which causes it to drift (a slow approach to the installation), or a rogue ship heading towards the installation under power but with no effective lookout (a rapid approach).

Another important cause of ship collision relate to the operation of dynamic positioning systems of vessels in close proximity to the installation. Assessment of the reliability of dynamic positioning systems is a complex area, but guidance has been prepared by IMCA (see Reference [45]). Design measures to withstand possible impact from a large ship are normally impracticable, and the risk of collision with the installation dependent largely on the frequency, given that any collision is likely to result in severe consequences for the installation.

For some shipping routes, a log of historic ship movements and a prediction of normal traffic are available from coast guard or other regulatory bodies. Also, in areas where existing offshore installations operate there is likely to be a good understanding of shipping movements.

C.10.4 Use of output

The output of the assessment should provide the following:

a) guidance on the possibility of impact from vessels operating within the installation exclusion zone, which can be used for

   — developing design to provide protection measures, where considered necessary and beneficial in terms of reduced potential for impact damage to critical equipment or structure,

   — preparing effective marine movement management procedures, and

   — defining minimum standards for manoeuvrability and position-holding for any vessel operating within the installation exclusion zone;

b) guidance on the possibility of large vessel (ship) impact which is likely to result in severe impact and extensive damage to the installation, which can be used for

   — developing an early warning system for impending ship collision and appropriate emergency response measures (e.g. controlled shutdown and abandonment of the installation before impact), and

   — likely frequency of an impact that exceeds the inherent structural strength of the installation, and associated risk when combined with potential consequences.

C.11 Failure mode, effects and criticality analysis (FMECA)

C.11.1 Objectives

The objectives of FMECA are the following:

— identification of all possible single failure modes within systems or equipment, the likely effects of these failures and any potential consequences in terms of “severity” and “criticality”;

— prediction of the probability that an identified failure mode will result in failure of design measures (barriers) and increased level of risk.

C.11.2 Typical input information

Input information for FMECA typically includes the following:

— The boundaries of the analysis and a clear definition of the system or equipment to be included (e.g. components, sub-assemblies, modules, etc.) at the correct level in the system hierarchy;

— Known failure rate data for system or equipment components. At the design stage, data may be available from suppliers but the most relevant data are that collected from actual equipment on comparable locations. ISO 14224 provides a comprehensive basis for the collection of reliability and maintenance data for equipment and should be used to provide sound input information for this study.

— The purpose of the analysis and the type of output. For example, seek to identify all failures within the system under consideration, or a specified point of concern within the system.

Dependent on the type of information required, select the tools and techniques to be used, which may include the following:

a) Equipment breakdown structure (EBS), which is normally used to describe the hierarchical structure of the system.

b) Reliability block diagrams (RBD), which identify the critical functional paths for a given function and clearly identify any areas of redundancy. These should be developed in accordance with IEC 61078.

c) Functional block diagrams (FBD), which are normally a primary requirement for performing a functional FMECA.

d) Critical failure paths identified from fault trees or event trees. Fault trees should be developed in accordance with IEC 61025 and event trees in accordance with IEC 62502.

C.11.3 Description/Narrative

FMECA is generally used to identify and focus attention on systems or equipment that are critical to MA hazard management and where there is insufficient failure data available to predict reliability in service.

NOTE The OREDA handbook presents reliability data for offshore equipment and provides both quantitative and qualitative information as a basis for reliability, availability, maintainability and safety analyses (see Reference [65]).

FMECA provides a method of identification and assessment of potential design weaknesses through impartial design review, and can be used to highlight areas which should be considered for design change or to support process change.

Various techniques are used to analyse the design of components and products, engineered systems (using commercially available products), manufacturing and assembly processes, services and software design.

The most common FMECA technique for an offshore project is the analysis of engineered systems, including:

— Safety analyses to establish the types of single failure mode possible for any system or equipment, and the criticality in terms of impaired ability to function as intended. When redundancy is implemented, fault tree analysis (see IEC 61025) can be implemented to analyse failure combinations impairing ability to function as intended.

— Reliability analyses to identify where the reliability of design measures for MA hazard management may not be sufficient. There are various approaches available to perform such reliability analyses, e.g. fault trees (see IEC 61025), RBDs (see IEC 61078), event trees (see IEC 62502), application of Markov techniques (see IEC 61165), Petri nets (IEC 62551) and Monte Carlo simulation, etc. ISO/TR 12489 provides requirements for reliability modelling of safety instrumented systems. Maintainability analyses to identify areas of the design which require unusual or onerous maintenance activity, often relate to the reliability required in service.

— Criticality analysis, which defines the significance of each failure mode qualitatively, semi-qualitatively, or quantitatively, depending on the type of input data available.

The analysis should be implemented at the most appropriate stage of the project, depending on the maturity of design definition and the level of detail required for output. If applied too early, there may not be enough information available to produce a meaningful analysis, but late application can result in much greater cost for design change. Generally, a high level of design definition is required.

A high-level functional analysis may be conducted at an early stage. Using functional block diagrams, which identify the main components and appropriate signals and/or functions, early feedback on potential design problems can be obtained.

Later in the design process, a detailed analysis at component level may be conducted using improved levels of design definition and firm data on failure modes and frequencies.

Most systems apply some form of hierarchical structure in order to divide the top-level system into a number of assemblies and sub-assemblies. These levels of hierarchy can be described both graphically and by a numbering system often described as a logistic support analysis.

FMECA is normally presented in some form of spreadsheet format. There are a number of sources for guidance and standards regarding formatting the FMECA. ISO 20815 covers production assurance of oil and gas production, processing and associated activities and covers the analysis of reliability and maintenance of the components.

C.11.4 Use of output

Results of FMECA, alone or in combination with more detailed approaches, are used to

— determine whether a critical safety system or equipment is capable of achieving the required MA hazard management role and function when demanded by a MA, as defined by the performance standards, and

— provide guidance as to whether remedial design measures are required to improve reliability of function and priorities related to criticality against severity. A criticality matrix is often used to provide a graphical means for illustrating the distribution of failure and consequences.

C.12 Reliability/survivability analysis of emergency systems (emergency system survivability assessment)

C.12.1 Objectives

The objectives of reliability/survivability analysis are to identify those systems which are necessary to maintain life support on the installation, and to assess the effects of credible MAs on the capability of the systems to operate as intended during emergency conditions (see NORSOK S-001).

These systems should be assessed in a systematic and consistent manner in order to

— prevent escalating threats to TR escape and evacuation routes,

— protect the TR, and

— enable escape to and evacuation from the TR.

C.12.2 Typical input information

Input information for reliability/survivability analysis typically includes the following equipment:

— fire and gas detection;

— fire protection;

— ESD and depressurising;

— HVAC;

— wellhead intervention;

— pipeline riser ESD valves;

— subsea isolation valves;

— platform safety communication;

— external communication;

— instrument hydraulic systems;

— control room interface;

— emergency power (including UPS);

— emergency lighting;

— navigation aids;

— arrangements for evacuation;

— toxic gas detection and protection.

Arrangements for evacuation are included in this list for completeness, but detailed treatment of these systems is, however, likely to be performed as part of the evacuation, escape, rescue analysis (see C.7).

Assessments of the nature and scale of major accidents that are credible for the installation. This may include for example loss of containment, fires, explosions, ship collision, helicopter crash, dropped objects (strong vibration), external events, environmental risks, etc.

C.12.3 Description/Narrative

Initially, the role and importance the above emergency systems are considered against each of the credible MA events. Any systems or elements that are needed to manage or mitigate the emergency are deemed to be critical.

If a critical system is deemed “fail-safe”, i.e. none of its components is deemed to fail to danger, including the final control element, then further analysis for such a system is not required and the analysis for these systems is complete.

If systems are critical and not “fail-safe”, the vulnerability of their components against foreseen incidents and human intervention should be assessed.

A system is vulnerable if damage/loss is possible which prevents the system operating for the necessary period of time. This period of time is either the endurance time of the TR (minimum 1 h) or the minimum time required for safe evacuation of people as measured from the commencement of the emergency situation.

For those critical systems that need further evaluation, the following are typically assessed:

— purpose of the system;

— system criticality (how important is the system to manage MAs?);

— escalation potential (if the system were not to perform its function);

— TR integrity (impact of the system not performing its function);

— escape/evacuation (impact of the system not performing its function);

— vulnerability (to the MA event for which it has a critical role);

— conclusion.

C.12.4 Use of output

The results of the analysis should be documented so that those operating the installation or involved with future changes are aware of the criticality and any vulnerability.

Should the conclusion of the assessment be that a critical system is vulnerable to the effects of an MA, and could thus jeopardize the life support or emergency systems, then all reasonable measures to improve the ability of the system to operate under the emergency conditions (e.g. relocation, redundancy, protection, redesign) should be undertaken.

C.13 Risk analysis

C.13.1 Objectives

The objectives of risk analysis are to provide a prediction of frequency with which an MA can occur, using recognized and verifiable methodology, and in so doing produce a value for risk (product of consequence × frequency) for people and the environment. See also NORSOK Z-013.

C.13.2 Typical input information

Input to a concept safety evaluation/risk assessment typically includes the following:

— HAZID reports and register of MA hazards;

— design strategies for managing MAs (hazards, and the measures in place to manage them);

— fire and explosion analysis report;

— smoke and gas dispersion and ingress report;

— emergency response analysis report;

— human reliability assessments;

— emergency systems analysis and SIL/risk graph assessments report;

— FMECA report;

— design data on process, risers, layout, etc.;

— isolatable inventories and the identified sources of potential release (e.g. connections between pipes or vessels, valves, instrumentation, etc.);

— agreed sources of historic release data and other factors that affect frequency of MAs (e.g. ignition probability, equipment failure data);

— agreed criteria for impairment, harm to people or the facilities;

— key assumptions forming the basis of the study.

C.13.3 Description/Narrative

Evaluation of MA hazards is combined with historical accident data or other assessments of failure frequency in order to predict the risk associated with each of the identified MA hazards, taking into account the design measures implemented (or proposed) for MAs.

Risk assessment should commence when design definition is sufficiently mature to provide the necessary input data, and when the hazard evaluation studies are sufficiently well advanced to provide useful results. Risk assessment is commonly applied:

— At an early stage (e.g. concept definition and optimization) when the risk analysis results can be used to influence design development, particularly for hardware barriers and the performance standards required. Sufficient time should be allowed for the study to take place and for the feedback of results for improving design.

— At the detailed design stage when the design definition is largely fixed. At this stage it is used to provide assurance that the risks to people and the environment are within acceptable limits and meet the project goals and criteria.

— Interim stages, as required, to provide updated or focused risk values for specific facilities (e.g. frequency of explosion load exceeding structural strength criteria).

The basic steps for the project team in commissioning a quantitative risk analysis (QRA) are as follows:

a) Ensure that the project representative has an understanding of the QRA processes to be employed and whether the models used can be interrogated to provide a clear audit trail from MA hazards to the final risk predictions. This is important when unexpected results are produced and the project needs to trace the process and assess validity of the results.

b) Define risk measures to be calculated and reported (e.g. individual risk, group risk, fatal accident rate, TR impairment frequency, F/N curves, etc.).

c) Specify critical criteria and assumptions concerning the design and operation of the installation (e.g. limits of structural strength or containment integrity under accident load conditions, criteria for impairment of TR/muster location).

d) Agree on assumptions that form the basis of the analysis, and ensure that these are clearly defined in the terms of reference and final reports.

e) Agree on the range of sensitivity analysis required to estimate the level of uncertainty, and predict the sensitivity of the results to variations in the assumptions or to changes to hardware barriers.

f) Specify whether interim results are required to illustrate important characteristics and to aid the design of hardware barriers and performance standards.

g) Define how the final results are to be reported in order to provide an auditable presentation of risk, which includes the models and methodology employed and any uncertainty in the validity of results.

QRA is often conducted by specialists who are not part of the project design team, and it is important therefore to ensure they have a good understanding of the installation design and any unusual features. Arrangements should also be made for a close working relationship between the specialists and the

project team, in order to provide consistency with the MA hazard management work being done by the project team.

Qualitative risk assessment should rely on a competent and experienced team, using a company- or project-approved approach such as a risk matrix. Such an approach is more likely to be relevant for the early stages of a large project or for small, simple installations.

C.13.4 Use of output

Risk analysis is used, in combination with evaluation of MAs, for providing useful and understandable feedback of risk data for design guidance.

Results are given as:

— risk showing overall risk to people and the environment in the form specified (e.g. individual risk, group risk, fatal accident rate, TR impairment frequency, F/N curve, loss of main safety function etc.);

— contribution to the overall risk related to specific areas of the installation and/or types of MA in those areas;

— breakdown of the contribution to overall risk by type of hazard (e.g. hydrocarbon hazards, non-hydrocarbon hazards, occupational hazards);

— assurance that risk to people and the environment is below acceptable limits and meets the project risk tolerance criteria.

C.14 Hazard and operability (HAZOP) study

C.14.1 Objectives

The objectives of a HAZOP study are the application of a structured and systematic review technique to a defined system, carried out by a team, to identify hazards and operability problems, including causes, consequences, safeguards and remedial actions. See also IEC 61882.

C.14.2 Typical input information

Input to a HAZOP study typically includes the following:

— process flow diagrams (PFDs);

— piping and instrumentation diagrams (P&IDs);

— cause and effect (C&E) diagrams;

— operating/control/shutdown philosophies/procedures.

In addition, prior to commencement of the study, the process plant or system should be divided into subsystems or sections, called “nodes”.

C.14.3 Description/Narrative

A HAZOP study is a detailed hazard and operability problem identification process, carried out by a team.

HAZOP deals with the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences.

HAZOP is most suitable in the earlier stages of design for new facilities, and when changes to existing facilities can be made but will likely need to be updated as design definition increases (e.g. P&IDs approved for design and approved for construction).

A HAZOP involves a team of people who have experience of the plant or knowledge of the design that is under review. The sessions are guided by a trained and experienced HAZOP leader, assisted by a recorder/scribe who records identified hazards and/or operational disturbances for further evaluation and resolution.

The approach involves considering each subsystem (or node) of the process in turn, and evaluating the consequences of deviations from the design intent. This examination of deviations is structured around a specific set of guide-words, which ensure complete coverage of all possible problems while allowing sufficient flexibility for an imaginative approach.

The HAZOP proceeds by a series of repeated steps:

1) identify a section of plant on the P&ID(s);

2) establish the design intent and normal operating conditions of this section;

3) identify a deviation from design intent or operating conditions by applying a set of guide-words;

4) identify possible causes for, and consequences of, the deviation;

5) identify existing safeguards and decide what action, if any, is necessary;

6) record the discussion and action.

Steps 3) to 6) are repeated until all the guide-words have been exhausted and the team is satisfied that all meaningful deviations have been considered. The team then goes back to Step 1) and repeats the process for the next section of plant.

There are two basic styles of HAZOP recording: a) full, and b) by exception only. The method of recording should be decided before any sessions take place, and the recorder advised accordingly.

Reports of the study should be produced, both at the end of the HAZOP session(s) and after action closure; all actions should be tracked to closure.

The strengths of HAZOP are that it is widely used and well understood, uses the experience of operating personnel as part of the team, and is systematic and comprehensive.

Its weaknesses are that it depends on the experience of the leader and the knowledge of the team, and documentation can be lengthy (for full recording) or difficult to audit (for recording by exception).

C.14.4 Use of output

HAZOP is a standard tool for process plant design offshore. The results are normally used to generate recommendations to improve the safety and operability of a design, but it is only one of several techniques required for identification of MA hazards.

A HAZOP can provide notes which draw attention to particular points which need to be addressed in operating and maintenance procedures.

The causes and consequences of deviations identified in a HAZOP study can be used in subsequent integrity analysis of instrumented systems [e.g. layer of protection analysis (LOPA)].

C.15 Safety integrity analysis of instrumented systems

C.15.1 Objectives

The purpose of integrity analysis is to ensure that the design, maintenance and operational requirements of safety instrumented functions (SIF) are suitable to meet tolerable risk levels.

C.15.2 Typical input information

Input information for integrity analysis typically includes:

— piping and instrumentation diagrams (P&IDs);

— cause and effect (C&E) diagrams;

— operating/control/shutdown philosophies/procedures;

— HAZOP records/report(s).

NOTE IEC 61511 specifies a life cycle approach with well-defined stages in the process and specific inputs and outputs for the different phases.

C.15.3 Description/Narrative

The term "safety integrity level" (SIL) relates to a "safety instrumented function" (SIF), which typically comprises one or more sensors, a logic solver, and one or more final elements.

The two principle stages in the life cycle described here are:

a) Determination of the necessary risk reduction to be achieved by the SIF and hence the required integrity level (SIL).

b) Confirmation that the design of the SIF meets the required SIL with respect to the average probability of failure on demand (PFD_{avg}) (for demand mode of operation), the frequency of dangerous failures (for continuous mode), architectural constraints and design requirements (as described in IEC 61511-1:2004, Section 11). This activity is often referred to as "SIL verification".

NOTE 1 ISO/TR 12489 and IEC 61508–6 provide guidance on reliability calculations for safety systems.

Determination of the risk reduction to be achieved by the SIF is conducted by a review team of relevant discipline engineers and operations representatives, led by a facilitator. This requires implementation of a defined methodology, e.g. calibrated risk graph, layer of protection analysis (LOPA). See EN 61511 (all parts) for more details on SIL assessments.

The assessment/review should be recorded appropriately to ensure quality and consistency. Correct and transparent recording is important to allow use of the information throughout the life cycle phases of the safety instrumented system (SIS). Recording is typically carried out by a recorder/scribe, assisting the facilitator.

The SIL requirement is derived by taking into account the required risk reduction that is to be provided by the SIF. This leads to the SIL being defined (between SIL1 and SIL4), implying requirements both on probabilistic aspects (PFD_{avg} or frequency of dangerous failures) and on qualitative constraints (e.g. fault tolerance, traceability, systematic capability, etc.). The requirements are more and more stringent as the required risk reduction increases.

SIL verification involves a quantitative analysis to confirm that the SIS meets the required SIL (or PFD), taking into consideration factors such as architecture, required test intervals, common cause failures, etc.

NOTE 2 IEC 61511 relies on IEC 61508–6 in this area and ISO/TR 12489 describes in detail how to perform such quantitative analysis in the oil and gas industry.

The SIL verification should be documented appropriately to ensure quality and consistency.

Software tools can be used to support SIL analysis and verification.

Use of LOPA requires companies to set risk targets to be achieved. For a specified consequence (safety, environmental or commercial), these are referred to as the target mitigated-event likelihood (TMEL).

Modifications to any SIS should be properly managed to ensure that the required safety integrity of the SIS is maintained, despite any changes made.

See IEC 61511-1 for details of each phase of the SIS/functional safety life cycle.

C.15.4 Use of output

The results of integrity analysis can be used to

— contribute to the design of each SIS, to ensure the SIF meets the required SIL,

— define operational and maintenance/test requirements for each SIF, and

— provide a basis for managing modifications to any SIS.

C.16 Analysis of human factors

C.16.1 Objectives

The objective of such analysis is to develop a design which is tolerant to human error.

C.16.2 Typical input information

Input information for the analysis of human factors typically includes the following:

— an initial review to identify the most important issues, and to assist in framing the more detailed work;

— results of other MA hazard management identification and evaluation tools such as HAZID, HAZOP and the results of other;

— initial operations and maintenance philosophies;

— a detailed review of the important issues, in order to describe the environmental, social and health settings of the project, to determine its sensitive characteristics, and to examine the interaction between these component parts.

C.16.3 Description/Narrative

A variety of techniques or methodologies are available. Some (based on the human factors tool of task analysis per Reference [68]) should be focused on the identification of human barriers and safety critical tasks analyses and an assessment of the strength or robustness of those barriers, expectations regarding human performance, and the potential for error in an MA hazard scenario.

Other approaches to ensuring the integration of critical human factors considerations in the design will focus on identifying those points of human interface in the design (i.e. critical valves and field instruments, local controls and the central control room, maintenance-critical equipment items) and ensuring the appropriate design requirements needed to support the tasks are applied.

The objectives of this study can be achieved by identifying the following:

— significant potential human errors;

— factors that make errors more or less likely (e.g. poor design, distraction, time pressure, workload, competence, morale, noise levels, communication systems and other performance-influencing factors)

— and, based on this, to reduce as far as is reasonable the likelihood of human error by redesigning the task or equipment, or by implementing control measures such as HMI redesign, providing redundancy, competence development, updating of procedures, introducing of simulator training, etc.

The key principles in managing human errors are the following:

— it should be recognized that human failure is normal and predictable; it can be identified and managed;

— human error reduction should be addressed in a structured and proactive way from the early stages of a project;

— human error reduction should involve workers in the design of tasks and procedures;

— risk assessment should identify:

  a) where human failure can occur in safety-critical tasks;

  b) the performance-influencing factors which might make it more likely; and

  c) the control measures necessary to prevent it.

The design of control rooms, plant and equipment can have a large impact on human performance. Designing tasks, equipment and workstations to suit the user can reduce human error, accidents and ill health. Failure to observe ergonomic principles can have serious consequences for individuals and for the whole company. Effective use of ergonomics makes workers safer, healthier and more productive.

The earlier that consideration is given to human factors and ergonomics in the design process, the better the results are likely to be. However, human factors and ergonomics expertise should be used appropriately by involving people with knowledge of the working processes involved and the end user. For that reason, user involvement is key to designing operable and maintainable plant and systems.

C.16.4 Key design principles

The key principles in design for human factors include the following:

a) Equipment should be designed in accordance with recognized ergonomics standards (e.g. EN 614-1, EN 614-2, EN 842 and EN 894, ISO 9355-1, ISO 14122 (all parts), NORSOK C-001, and NORSOK S-002).

b) Control rooms should be designed in accordance with recognized standards [e.g. ISO 11064 (all parts)]. Additional guidelines are also contained in EEMUA 191 and EEMUA 201.

c) Different types of users should be involved in the design process, including operators, maintenance and systems support personnel. ISO 9241-210 provides requirements and recommendations for human-centred design principles and activities throughout the life cycle of computer-based interactive systems and ISO 7250 provides basic human body measurements for technological design.

d) Consideration should be given to operator characteristics, e.g. body size, strength and mental capability (e.g. EN 1005 and ISO 9241).

e) Plant and processes should be designed for operability and maintainability, while other elements of the life cycle, e.g. decommissioning, should not be neglected.

f) Consideration should be given to all foreseeable operating conditions, including upsets and emergencies.

g) Consideration should be given to the interface between the end user and the system.

C.16.5 Use of output

Studies/analyses of human factors should be used to identify all reasonable improvements that can be made to the installation design to help the operations team manage the operation of the installation.

It does not consist of one analysis, but several analyses, and should be integrated, as much as possible, into other studies being conducted. In addition, the results should be used to:

— prompt operations to consider options to lower the risk where the study identifies tasks which, if carried out incorrectly, could lead to an MA;

— identify those emergency tasks that need to be practiced so that they can be reliably carried out under emergency conditions;

— provide input to the development of procedures for critical operations or maintenance tasks so that they are clear, up to date and in a form that will actually be used by the operators;

— select, train, and assess as competent employees involved in management of MAs;

— aid in the design, construction and installation of new plant and equipment to avoid any adverse human factors of its operation.

The results of the study should also be reviewed if human factor issues are identified from incidents and near misses, in order to determine if there are any human-factor-related deficiencies that should be addressed.

See also References [49], [70], [74], [79] and [81].

C.17 Environmental risk assessment

C.17.1 Objectives

The purpose of environmental risk assessment is to identify any environmental harm that can arise from an undertaking, and then to decide on any measures needed to reduce the risk of harm to a level that is acceptable to the authorities having jurisdiction for the activity and will meet any internal company standards.

C.17.2 Typical input information

Input information for environmental risk assessment typically includes:

— a scoping report, in order to ensure the assessment is focused on the most important issues, and to assist in framing the scope of the baseline studies; and

— a baseline report, in order to describe the environmental, social and health setting of the project, to determine its sensitive characteristics, and to examine the interaction between these component parts.

C.17.3 Description/Narrative

Environmental risk assessment involves four stages:

a) identification of the hazard(s);

b) assessment of the potential consequences to the environment;

c) assessment of the hazard occurrence probabilities; and

d) characterization of the risk and uncertainty.

The evidence required to provide judgements and subsequently characterize a risk in this way can be qualitative, quantitative, or semiquantitative.

Uncertainty is always present when conducting each stage of an environmental risk assessment. The techniques available to analyse, understand and manage these uncertainties include the collection of

further data, the use of trusted sources, probability density functions, Bayes linear methods, and/or sensitivity analysis.

C.17.4 Use of output

Typical outputs from environmental risk assessment include the following:

— identification of issues and the approach to be used to manage the environmental profile of the project;

— a sustainable development plan;

— a biodiversity action plan;

— a water management plan; and

— stakeholder engagement.

The output of this structured process enables a judgement as to the presence, likelihood and significance of environmental harm, along with details on how the risk was assessed and where assumptions and uncertainties exist.

The environmental risk management options available are usually:

a) terminate the source of the risk where possible;

b) mitigate the effects by improving environmental management techniques or engineered systems;

c) transfer the risk through new technology, procedures or investment;

d) exploit the potential benefits of the risk by embracing new opportunities; or

e) accept the risk by not intervening with new or existing situations.

The preferred option is dependent on a range of parameters, such as technical factors, economic factors, environmental security, social issues and organisational capabilities.

However, if a preliminary evaluation shows that there are reasonable grounds for concern that a particular activity might lead to damaging effects on the environment which would be inconsistent with the protection normally provided, the lack of full scientific certainty should not be used to postpone or avoid cost-effective measures to prevent significant environmental harm.

See also ISO 14001 and Reference [43].

C.18 Terms of reference

C.18.1 General

For each study planned, a scope of work (or terms of reference) should be prepared and agreed with the project team and stakeholders. This should be a formal document which sets out the requirements for the activity, including the following:

— study purpose and objectives;

— facilities to be included (e.g. module or other boundary limits) and phase of development (e.g. concept definition);

— type of report and timing (e.g. phase reports to assist ISD and barrier development, plus final report when the studies are complete);

— methodology to be used;

— project input to the study [e.g. documents, drawings, model data (e.g. PDMS) and other information necessary for the study];

— criteria and assumptions to be included;

— schedule and expected deliverables;

— specialist team carrying out the work and responsibilities;

— system for tracking and close-out of actions.

Each study should be recorded in a formal report issued for project use.

C.18.2 Assumptions made

The majority of MA evaluation studies rely on some of the variables which relate to the design or parameters which form part of the analysis being fixed by the use of assumptions (i.e. engineering judgements, best practice, etc.). Any assumptions made should be clearly defined as such in the introduction to the study report, so that the reader is made aware of these and can form his/her own judgement.

Annex D
(informative)

Strategy for managing major accident hazards

D.1 Inherently safer design (ISD)

There are no set rules for implementing ISD. The aim is to develop a design which has an underlying level of MA hazard management through features built into the structure and layout specifications. A list of general principles or approaches is given here for consideration.

a) Review whether the manning levels proposed are appropriate for the operation of the facility, with the aim of identifying measures that would allow them to be reduced.

b) For fixed jacket installations, consider two bridge-linked platforms: one for process plant and the other for TR/living quarters and non-hazardous utilities, etc.

c) Use unmanned or "normally" unmanned facilities, and include measures to minimize the number of visits and the number of people required.

d) Where possible, locate the installation outside known hazardous areas (e.g. shipping lanes, earthquake zones or where foundations can be unstable).

e) Remove the need for oil or gas storage on the installation, and minimize the need to store flammable or hazardous chemicals.

f) Avoid drilling or well workover activities on a production installation (in general, the combined risks associated with drilling and production are greater than for the separate production and drilling activities).

g) Develop structural strength to withstand impact from marine vessels operating in the vicinity and also from dropped or swinging loads.

h) Provide inherent stability to floating vessels under normal conditions and accident conditions, including the prevention of accidental flooding of buoyancy chambers/ballast tanks.

i) For floating vessels, provide mooring facilities designed to withstand extreme environmental loads even after failure of one or more mooring lines.

j) Use simplified, yet robust, design to avoid the need for complicated instrumentation and control systems, thus reducing the number of people required to operate the plant.

k) Employ open modules with low congestion to improve natural ventilation (prevention of explosion or fire by dispersion of flammable gas) and free venting of explosion products in the event of such an accident event (reduce explosion overpressure and drag loads). Avoid enclosed, congested spaces where natural ventilation is limited and a flammable gas release could cause a damaging explosion and escalation.

l) Separate modules by open space where possible, to provide an explosion break (reduced chance of explosion development over a long distance with associated high overpressure).

m) Design layout to provide separation and/or segregation of hazardous areas and non-hazardous areas. Locate the most hazardous functions farthest away from TR/muster locations, living quarters (i.e. where the majority of people are located).

n) Ensure structural strength to withstand explosion or fire loads and to prevent escalation through structural deformation or failure (deformation of supporting structure for process plant is a common cause of further inventory release).

o) Reduce the potential for escalation of an MA by using structural hardware barriers able to protect key facilities such as TR and evacuation facilities, bearing in mind that obstructions like fire and blast hardware barriers can impair natural ventilation and increase the probability of flammable gas cloud development and ignition, and can raise explosion overpressure.

p) Reduce the potential for loss of containment by

— using fully rated pipelines, risers and well fluid reception facilities to remove over-pressurization hazards (piping, valves, vessels, etc.);

— designing specification of materials to reduce the likelihood of loss of containment (e.g. corrosion/erosion/fatigue resistance);

— minimising pipe, instrumentation and equipment connections;

— limiting the severity of any release that could occur through use of high integrity connections and design of connections (e.g. instrument connections of at least 2-inch pipe for mechanical strength, with reduced bore to limit possible release rate).

D.2 Barriers

D.2.1 General

A barrier is a functional grouping of safeguards and controls selected to prevent the realization of an MA. Barriers can be subdivided into the following categories:

a) Hardware barriers — engineered systems designed and managed to prevent MAs and limit any potential consequences.

b) Human barriers — actions of people to prevent MAs and limit any potential consequences.

Barriers are supported by management system elements.

No barrier can be considered completely effective as there is always the potential for problems or defects which reduce the effectiveness. Hence, it is generally necessary to have multiple barriers to reduce the chance that an MA is realized as illustrated in Figure D.1.

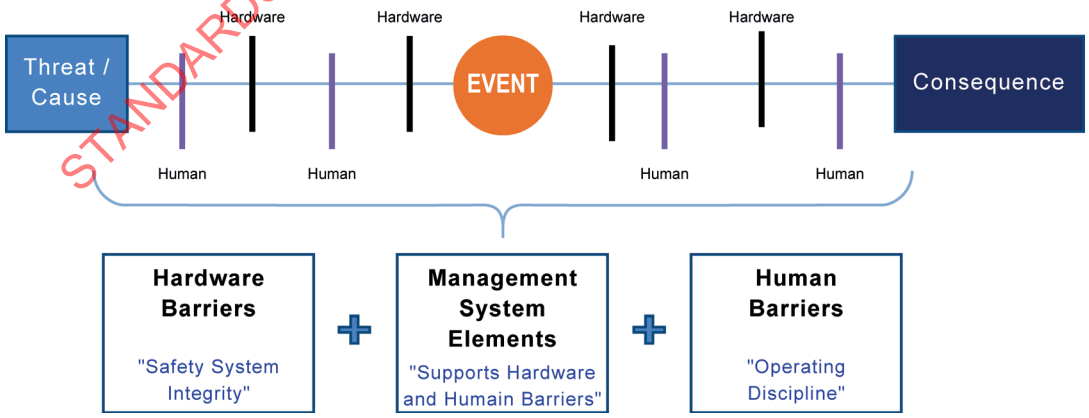

Figure D.1 — Multiple barriers to reduce chance of an MA

The likelihood of an MA is further reduced if multiple barriers are fully functional and independent. If the conditions of independence and full functionality are satisfied, it may be possible to reduce the

number of barriers needed as part of the MA hazard management strategy. A barrier is described as independent if it has no failure modes in common with other barriers.

Reference [46] explains the role of barriers in managing major accidents and Reference [51] provides standard definitions for process safety barriers.

D.2.2 Hardware barriers

The main functional elements of hardware barriers are typically:

— Barriers to prevent or reduce the likelihood of MAs:

  a) structural integrity;

  b) process containment.

— Barriers to limit the consequences of MAs:

  a) ignition control;

  b) detection and monitoring;

  c) protection;

  d) isolation;

  e) emergency response;

  f) lifesaving.

Passive hardware barriers are those that meet the barrier function without the active functioning of any component. Passive barriers are robust if maintained, but some passive devices are still subject to failure. For example, bunds and spill containment are passive barriers but still require the management system elements of inspection and maintenance.

Active hardware barriers are engineered systems that function on demand, without human intervention. Active barriers generally involve multiple active elements: a sensor to detect a hazardous condition, a logic device to decide what to do, and a control element to implement the appropriate action. Active barriers can require many systems and devices to detect and react to multiple potential incident scenarios, and can be costly to design, procure, install, operate and maintain.

Examples of the systems that can be used to meet the various hardware barrier functions are listed in Table D.1.

Table D.1 — Examples of systems to meet hardware barrier functions

Structural integrity	**Process containment**	
Foundations Jacket/hull structure Topsides substructure Mechanical handling equipment Ballast and cargo management Mooring systems Drilling systems	Wellhead/Xmas trees equipment Process equipment Rotating equipment Fired heaters Tanks Piping systems and instrument connections Flowlines and pipelines Relief systems Well containment systems Tanker/loading systems Helicopter refuelling	
Ignition Control	Detection and Monitoring	Protection
Hazardous area ventilation Certified electrical equipment Tank inert gas/blanketing systems Earth bonding Purge systems Electrical tripping systems Flare tip ignition systems	Fire and gas detection Ship/vessel tracking systems Foundation/mooring monitoring Well condition monitoring Collision avoidance monitoring Metocean data collection	Deluge systems Firewater pumps/ring main Fire extinguishing systems Sprinkler systems Fixed fire-fighting equipment Foam systems Explosion relief/suppression Passive fire protection Vessel/ship collision protection
Isolation	**Emergency Response**	**Lifesaving**
ESD and EDP systems Overpressure protection systems Operational well isolations Pipeline isolation valves Subsea isolation valves Well control equipment	Escape and evacuation routes Emergency/escape lighting Temporary refuge Communication systems Emergency power Uninterruptable power supplies Drains systems	Personal survival equipment TEMPSC/lifeboats Rescue facilities Tertiary escape facilities

D.2.3 Human barriers

Human barriers rely to some extent on the actions of people. These may be actions that maintain integrity of plant and equipment or may be the reasoned response to a stimulus indicating a need for action. Examples include:

a) operating within the design envelope of plant and equipment;

b) preparing equipment for isolation and maintenance;

c) reacting to change in equipment status e.g. observed when conducting routine monitoring activities;

d) authorization of temporary and mobile equipment;

e) acceptance of handover or restart of facilities or equipment;

f) response to process alarm and upset conditions (e.g. outside the safe envelope for operation);

g) response to emergencies.

In order for human barriers to be effective amongst other issue there needs to be

— an error-tolerant design,

— sufficient time for operator response,

— appropriate procedures that cover operational actions, and

— operator training in the procedures.

Those providing human barriers should perform the role in accordance with the standards and procedures for the activity. Without this behaviour, the resilience of the barriers is low requiring considerable leadership effort to maintain the barrier effectiveness.

NOTE Human barriers exclude maintenance and inspection activities associated with hardware barriers. These are defined as being management system elements.

When assessing human barriers, consideration should be given to the

— effects of stress,

— workload,

— complexity of reasoning required,

— working environment,

— ease of executing the tasks, and

— interruptions and distractions that can be present when trying to execute safety-critical tasks.

In addition, performance in an emergency can be affected by heat, toxic gas, smoke, gas or other disorientating effects. More guidance on the analysis of human factors of safety critical tasks is provided in C.16.

D.2.4 Management system elements

Management system elements are those parts of the overall management system which are needed to enable the hardware and human barriers to prevent MAs and mitigate the consequences. Management systems typically cover the following:

— commitment and accountability (includes clear accountabilities and resourcing, etc.);

— policies, standards and objectives;

— organization, resources and capability (includes competence, training, contractors, etc.);

— stakeholders and customers;

— risk assessment and control (includes management of change, etc.);

— asset design and integrity (includes the assessment of risk and design and management of hardware barriers, etc.);

— plans and procedures (includes emergency and crisis response management, etc.);

— execution of activities (includes permit to work, etc.);

— monitoring, reporting and learning (includes incident investigation, etc.);

— assurance, review and improvement (includes audit and management review, etc.).

Annex E
(informative)

Barrier system performance standards

E.1 Performance standards for hardware barriers

Performance standards are 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 should be specified for each hardware barrier (including those needed for emergency response). Multiple linked performance standards may be written to support a complete barrier function.

Hardware barrier system performance standards are normally defined in a standard template form (agreed by the project or stakeholder) and comprise several elements, as indicated in Table E.1.

Table E.1 — Example of a performance standard template for a hardware barrier

Reference	**Barrier name**	**Person accountable**
Barrier function	A high-level description of the barrier system function. Some barrier systems provide safety-critical functions as part of a wider role, e.g. the role of the jacket, hull, topsides structure is to support all facilities and equipment through the life of the installation. It also has the safety-critical function of surviving extreme events and accidents without losing its ability to provide support and stability. Other barrier systems are entirely safety-critical, for example the fire and gas detection system.	
Scope	Identifies the equipment and systems that are included in the barrier system and hence subject to the performance standard requirements.	
Excluded items		
PS interfaces		
Functional requirements		
	Requirement	Verification information
F1	Define requirements for how the barrier system should work to perform its stated role and to achieve the MA hazard management and risk reduction required.	
F2		
Availability		
A1	State the required/expected availability of the barrier system in service to achieve the MA hazard management and risk reduction required.	
A2		
Reliability		
R1	State the required level of reliability of the barrier system in service to achieve the MA hazard management and risk reduction required.	
R2		