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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 4

4 Major accident hazard management overview **5**
4.1 General 5
4.2 Project management commitment 5
4.3 Project management accountability 6
4.4 Project plan to manage major accident hazards 6
4.5 Objectives of major accident hazard management 6
4.6 Selection of hazard evaluation and risk assessment methods 7
4.7 Good engineering practice 7
4.8 Documentation 8
4.8.1 General 8
4.8.2 Register of major accident hazards 9
4.9 Actions management 9
4.10 Management of change 9

5 Management of major accident hazards in design **10**
5.1 Overview of MA hazard management 10
5.2 Key concepts 11
5.2.1 Understanding the MA hazards 11
5.2.2 Inherently safer design (ISD) 12
5.2.3 Design strategies for managing MA hazards 13
5.2.4 Barriers 13
5.2.5 Performance standards 14
5.2.6 Communication with technical and operational teams 15

6 Screening and concept selection process **15**
6.1 General 15
6.2 Objectives 16
6.3 Functional requirements 17
6.3.1 Screening 17
6.3.2 Hazard identification 17
6.3.3 Major accident hazards evaluation 17
6.3.4 ISD and barriers 18
6.3.5 Performance standards 18
6.3.6 Sufficiency of measures 18
6.3.7 Documentation 18

7 Concept definition and optimization **19**
7.1 General 19
7.2 Objectives 20
7.3 Functional requirements 20
7.3.1 Hazard identification 20
7.3.2 Major accident hazard evaluation 20
7.3.3 Risk assessment 20
7.3.4 Inherently safer design (ISD) 20
7.3.5 Barriers 21
7.3.6 Performance standards 21
7.3.7 Sufficiency of measures 21
7.3.8 Documentation 22

8 Detailed design and construction phase **22**
8.1 General 22
8.2 Objectives 23
8.3 Functional requirements 23
8.3.1 Overview 23
8.3.2 Hazard identification 24
8.3.3 Major accident hazards evaluation 24
8.3.4 Risk assessment 24
8.3.5 Inherently safer design (ISD) 24
8.3.6 Barriers 24
8.3.7 Performance standards 25
8.3.8 Sufficiency of measures 25
8.3.9 Register of major accident hazards 25
8.3.10 Documentation 25
8.3.11 Procurement of equipment 26
8.3.12 Construction, completion and commissioning 26
8.3.13 Transfer to operation 26
8.3.14 Actions management 26

9 Major accident hazard management in operation **27**
9.1 General 27
9.2 Objectives 27
9.3 Functional requirements 28
9.3.1 Barrier management 28
9.3.2 Revalidation 28
9.3.3 Safety-critical tasks 28
9.3.4 Temporary changes 29
9.3.5 Non-availability of barrier performance 29
9.3.6 Management of change (MOC) 29

Annex A (informative) **Example of a framework for risk-related decision support** **31**
Annex B (informative) **Plan to manage major accident hazards** **32**
Annex C (informative) **Major accident hazard management identification and evaluation tools** **41**
Annex D (informative) **Strategy for managing major accident hazards** **71**
Annex E (informative) **Barrier system performance standards** **77**
Annex F (informative) **HAZID guidewords** **80**
Bibliography **94**

Foreword

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

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

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

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

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

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

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

Introduction

The purpose of this document is to establish requirements and provide guidance for the effective management of major accident (MA) hazards during the design of new offshore installations for the petroleum and natural gas industries.

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

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

This document covers the following main elements:

— establishing general requirements for identifying MA hazards and their causes;

— assessing MA hazards to understand their likelihood and possible consequences;

— developing suitable strategies for managing MA hazards;

— progressively improving the understanding of MA hazards and their consequences to guide design decisions during the development phases of the installation;

— providing the measures needed to manage all credible MAs;

— maintaining the measures throughout the life of the installation.

The technical content of this document is arranged as follows:

a) objectives: the goals to be achieved;

b) functional requirements: specifying requirements considered necessary to meet the stated objectives;

c) annexes: guidelines in support of the functional requirements.

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

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

1 Scope

This document describes processes for managing major accident (MA) hazards during the design of offshore oil and gas production installations. It provides requirements and guidance on the development of strategies both to prevent the occurrence of MAs and to limit the possible consequences. It also contains some requirements and guidance on managing MA hazards in operation.

This document is applicable to the design of

— fixed offshore structures, and

— floating systems for production, storage and offloading

for the petroleum and natural gas industries.

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

This document is intended for the larger projects undertaken to develop new offshore installations. However, the principles are also applicable to small or simple projects or design changes to existing facilities and can also be relevant to onshore production facilities.

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

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

2 Normative references

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

ISO 31000, *Risk management — Principles and guidelines*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
barrier
functional grouping of safeguards or controls selected to prevent a major accident or limit the consequences

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

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

3.1.2
emergency response
action taken by personnel on or off an installation to limit the consequences of a major accident or initiate and execute abandonment

[SOURCE: ISO 15544:2000, 2.1.8]

3.1.3
environment
surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans and their interrelationships

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

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

[SOURCE: ISO 14001:2015, 3.2.1]

3.1.4
ergonomics
scientific discipline concerned with study of human factors and understanding of interactions among human and other elements of a system

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

3.1.5
escape route
route from an area of an installation leading to a muster area, temporary refuge (TR), embarkation area, or means of escape to the sea

[SOURCE: ISO 15544:2000, 2.1.15]

3.1.6
evacuation
planned method of leaving the installation in an emergency

[SOURCE: ISO 15544:2000, 2.1.17]

3.1.7
harm
injury or damage to the health of people, or damage to property or the environment

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

3.1.8
hazard
potential source of harm

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

3.1.9
hazardous event
event that can cause harm

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

3.1.10
individual risk
risk to which an individual is exposed during a defined period of time

3.1.11
inherently safer design
design which eliminates or reduces major accidents through measures that are permanent and inseparable from the design

3.1.12
major accident
MA
hazardous event that results in

— multiple fatalities or severe injuries; or

— extensive damage to structure, installation or plant; or

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

Note 1 to entry: In this document, a major accident is the realization of a major accident hazard.

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

3.1.13
major hazard
hazard with the potential, if realized, to result in a major accident

3.1.14
mobile offshore unit
mobile platform, including drilling ships, equipped for drilling for subsea hydrocarbon deposits and mobile platforms for purposes other than production and storage of hydrocarbon deposits

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

3.1.15
muster area
designated area to which personnel report when required to do so in an emergency

[SOURCE: ISO 15544:2000, 2.1.29]

3.1.16
performance standard
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,