INTERNATIONAL STANDARD

ISO 10418

Second edition
2003-10-01

Petroleum and natural gas industries — Offshore production installations — Basic surface process safety systems

Industries du pétrole et du gaz naturel — Plates-formes de production en mer — Analyse, conception, installation et essais des systèmes essentiels de sécurité de surface

Reference number
ISO 10418:2003(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 10418 was prepared by Technical Committee ISO/TC 67, *Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries*, Subcommittee SC 6, *Processing equipment and systems*.

This second edition cancels and replaces the first edition (ISO 10418:1993), which has been technically revised including the following:

— reference to IEC 61511 is made for instrumentation used as secondary protection;

— risk-based methods of analysis are included as an alternative to the use of safety analysis tables (SATs) and safety analysis checklists (SACs);

— additional guidance is provided on the setting of safety integrity levels for fire and gas and ESD systems;

— additional guidance is provided concerning toxic gases and bypassing and annunciation.

Introduction

Effective management systems are required to address the health and safety aspects of the activities undertaken by all companies associated with the offshore recovery of hydrocarbons[1)]. These management systems should be applied to all stages in the life cycle of an installation and to all related activities. Such a management system, which has been developed for environmental issues, is described in ISO 14001[4] and the principles contained in this International Standard can also be applied to issues relating to health and safety.

One key element of effective management systems is a systematic approach to the identification of hazards and the assessment of the risk in order to provide information to aid decision-making on the need to introduce risk-reduction measures.

Risk reduction is an important component of risk management, and the selection of risk-reduction measures will predominantly entail the use of sound engineering judgement. However, such judgements may need to be supplemented by recognition of the particular circumstances, which may require variation to past practices and previously applied codes and standards.

Risk-reduction measures should include those to prevent incidents (i.e. reducing the probability of occurrence), to control incidents (i.e. limit the extent and duration of a hazardous event) and to mitigate the effects (i.e. reducing the consequences). Preventative measures such as using inherently safer designs and ensuring asset integrity should be emphasized wherever practicable. Measures to recover from incidents should be provided based on risk assessment and should be developed taking into account possible failures of the control and mitigation measures. Based on the results of the evaluation, detailed health, safety and environmental objectives and functional requirements should be set at appropriate levels.

The level and extent of hazard identification and risk assessment activities will vary depending on the scale of the installation and the stage in the installation life cycle when the identification and assessment process is undertaken. For example:

— complex installations, e.g. a large production platform incorporating complex facilities, drilling modules and large accommodation modules, are likely to require detailed studies to address hazardous events such as fires, explosions, ship collisions, structural damage, etc.;

— for simpler installations, e.g. a wellhead platform with limited process facilities, it may be possible to rely on application of recognized codes and standards as a suitable base which reflects industry experience for this type of facility;

— for installations which are a repeat of earlier designs, evaluations undertaken for the original design may be deemed sufficient to determine the measures needed to manage hazardous events;

— for installations in the early design phases, the evaluations will necessarily be less detailed than those undertaken during later design phases and will focus on design issues rather than management and procedural aspects. Any design criteria developed during these early stages will need to be verified once the installation is operational.

Hazard identification and risk assessment activities may need to be reviewed and updated if significant new issues are identified or if there is significant change to the installation. The above is general and applies to all hazards and potentially hazardous events.

---

1) For example, operators should have an effective management system. Contractors should have either their own management system or conduct their activities consistently with the operator's management system.

Process protection system is a term used to describe the equipment provided to prevent, mitigate or control undesirable events in process equipment, and includes relief systems, instrumentation for alarm and shutdown, and emergency support systems. Process protection systems should be provided based on an evaluation that takes into account undesirable events that may pose a safety risk. The results of the evaluation process and the decisions taken with respect to the need for process protection systems should be fully recorded.

If an installation and the associated process systems are sufficiently well understood, it is possible to use codes and standards as the basis for the hazard identification and risk assessment activities that underpin the selection of the required process protection systems. The content of this International Standard is designed to be used for such applications and has been derived from the methods contained in API RP 14C[8] that have proven to be effective for many years. Alternative methods of evaluation may be used, for example based on the structured review techniques described in ISO 17776. Having undertaken an appropriate evaluation, the selection of equipment to use may be based on a combination of the traditional prescriptive approach and new standards that are more risk based.

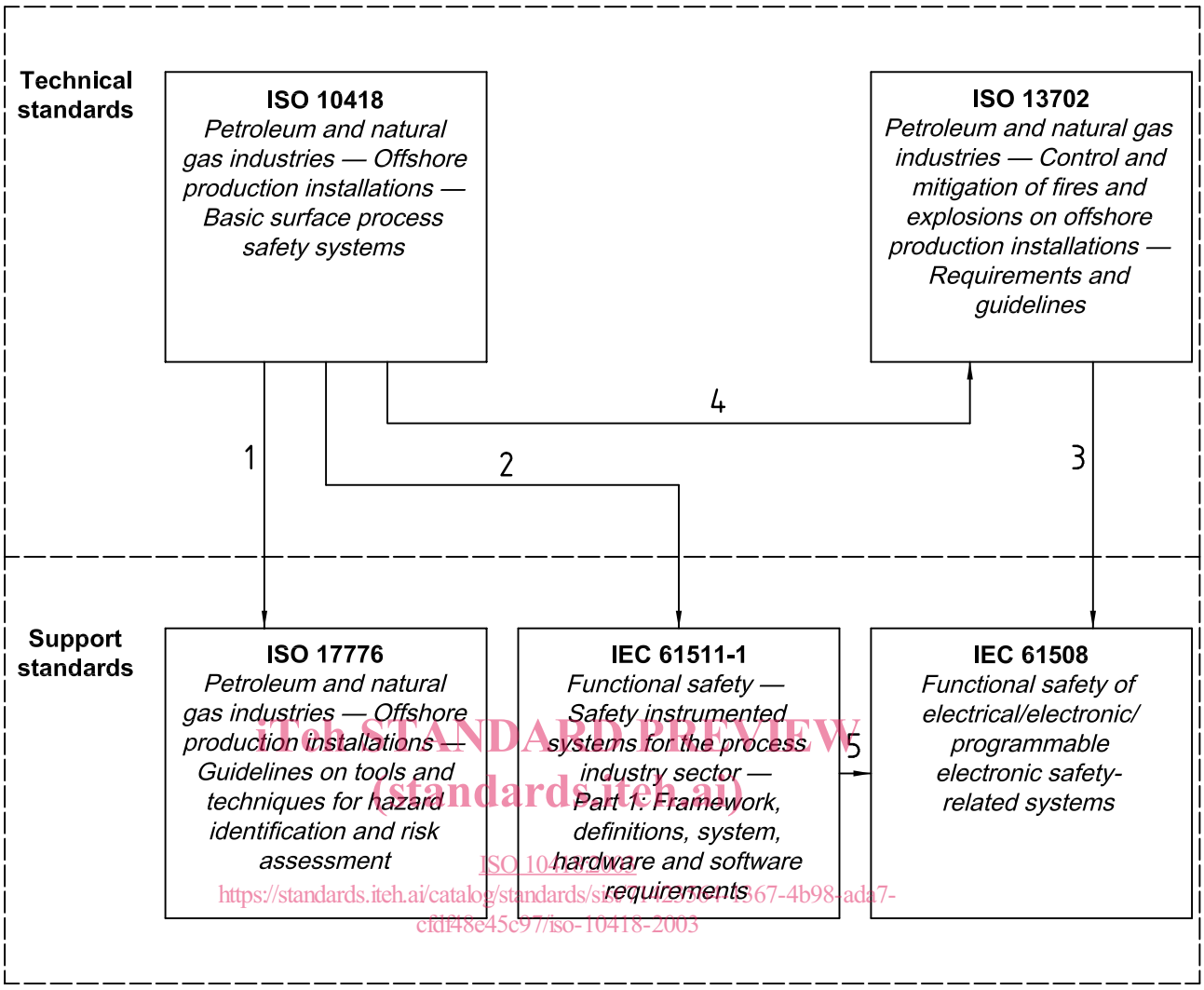
Particular requirements for the control and mitigation of fires and explosions on offshore installations are given in ISO 13702. General requirements for fire and gas and emergency shutdown (ESD) systems are also included in ISO 13702.

This International Standard and ISO 13702 reference new standards on functional safety of instrumented systems. This International Standard refers to IEC 61511-1, which is the process sector implementation of the generic standard IEC 61508 that is referred to in ISO 13702. The relationship between the standards referred to above is presented in Figure 1.

The approach described in this International Standard should be applied in an iterative way. As design proceeds, consideration should be given as to whether any new hazards are introduced and whether any new risk-reduction measures need to be introduced.

It should be recognized that the design, analysis and testing techniques described in this International Standard have been developed bearing in mind the typical installations now in use. Due consideration should therefore be given during the development of process protection systems to the size of the installation, the complexity of the process facilities, the complexity and diversity of the protection equipment and the manning levels required. New and innovative technology may require new approaches.

This International Standard has been prepared primarily to assist in the development of new installations, and as such it may not be appropriate to apply some of the requirements to existing installations. Retrospective application of this International Standard should only be undertaken if it is reasonable to do so. During the planning of a major modification to an installation, there may be more opportunity to implement the requirements and a careful review of this International Standard should be undertaken to determine those clauses which can be adopted during the modification.



Key

1 Tools and techniques for systematic hazard identification and risk analysis
2 Requirements for instrument systems used for sole or secondary protection
3 For safety integrity requirements for fire and gas and emergency shutdown systems
4 Requirements for fire and explosion strategy and support systems
5 Requirements for instrument products used for safety that have not been proven by “prior use”

Figure 1 — Relationship between offshore-relevant standards

Petroleum and natural gas industries — Offshore production installations — Basic surface process safety systems

1 Scope

This International Standard provides objectives, functional requirements and guidelines for techniques for the analysis, design and testing of surface process safety systems for offshore installations for the recovery of hydrocarbon resources. The basic concepts associated with the analysis and design of a process safety system for an offshore oil and gas production facility are described, together with examples of the application to typical (simple) process components. These examples are contained in the annexes of this International Standard.

This International Standard is applicable to

— fixed offshore structures;

— floating production, storage and off-take systems;

for the petroleum and natural gas industries.

This International Standard is not applicable to mobile offshore units and subsea installations, although many of the principles contained in it may be used as guidance.

2 Normative references

The following referenced documents are indispensable for the application 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 13702:1999, *Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines*

ISO 17776:2000, *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment*

IEC 61511-1, *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements*

3 Terms, definitions and abbreviated terms

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

3.1 Terms and definitions

3.1.1
abnormal operating condition
condition which occurs in a process component when an operating variable ranges outside of its normal operating limits

3.1.2
atmospheric service
operation at gauge pressures between 0,2 kPa vacuum and 35 kPa pressure

3.1.3
automatically fired vessel
fired vessel having the burner fuel controlled by an automatic temperature or pressure controller

3.1.4
backflow
in a process component, fluid flow in the direction opposite to that of normal flow

3.1.5
blowdown valve
valve used to connect a process system to the system for discharging inventory to the atmosphere

3.1.6
containment
situation in which the hazardous material is held safely in a pressurized system

3.1.7
detectable abnormal condition
abnormal operating condition which can be detected by a sensor

3.1.8
direct ignition source
any source with sufficient energy to initiate combustion

3.1.9
emergency shutdown system
ESD system
system, activated by automatic or manual signals, which undertakes the control actions to shut down equipment or processes in response to a hazardous situation

3.1.10
excess temperature
in a process component, temperature higher than the rated working temperature

3.1.11
fail-closed valve
valve which will move to the closed position upon loss of the power medium or signal

3.1.12
failure
improper performance of a device or equipment item that prevents completion of its design function

3.1.13
fire detection system
system which provides continuous automatic monitoring to alert personnel to the presence of fire and to allow control actions to be initiated either manually or automatically

3.1.14
fired vessel
vessel in which the temperature of a fluid is increased by the addition of heat supplied by a flame contained within a fire tube within the vessel

3.1.15
fire loop
pneumatic control line containing temperature-sensing elements which, when activated, will initiate control actions in response to a hazardous situation

NOTE Examples of temperature-sensing elements are: fusible plugs, synthetic tubing, etc.

3.1.16
flame failure
flame which is inadequate to instantaneously ignite combustible vapours entering the firing chamber of a fired vessel

3.1.17
flowline
piping which directs the well stream from the wellhead to the first downstream process component

3.1.18
flowline segment
any portion of a flowline that has an operating pressure different from another portion of the same flowline

3.1.19
gas blowby
discharge of gas from a process component through a liquid outlet

3.1.20
gas detection system
system which monitors spaces on an offshore installation for the presence and concentration of flammable gases and initiates alarm and control actions at predetermined concentrations

3.1.21
hazardous area
three-dimensional space in which a flammable atmosphere may be expected to be present frequently enough to require special precaution for the control of potential ignition sources

3.1.22
hazardous event
incident which occurs when a hazard is realised

EXAMPLES Release of gas, fire, gas blowby.

3.1.23
high liquid level
in a process component, liquid level above the normal operating level but less than the maximum allowable working level

3.1.24
high pressure
in a process component, pressure in excess of the normal operating pressure but less than the maximum allowable working pressure

NOTE For pipelines, the maximum allowable working pressure is the maximum allowable operating pressure.

3.1.25
HP/LP interface
point in a process plant where operating pressure changes from high pressure to low pressure

NOTE A change in system design pressure or piping class is often associated with the HP/LP interface.

3.1.26
high temperature
in a process component, temperature in excess of the normal operating temperature but less than the maximum allowable working temperature

3.1.27
indirect heated component
vessel or heat exchanger used to increase the temperature of a fluid by heat transfer from another hot fluid

NOTE Examples of hot fluids are steam, hot water, hot oil, or other heated medium.

3.1.28
installation safety system
arrangement of safety devices and emergency support systems to effect installation shutdown

NOTE The system can consist of a number of individual process shutdowns and can be actuated by either manual controls or automatic sensors.

3.1.29
installation shutdown
shutting down of all process stations of an installation production process and all support equipment for the process which are not required for emergency response and personnel safety

3.1.30
instrument protection system
system that uses instrumentation to detect a deviation from the normal operating conditions and takes action to return the process to a safe state or prevent environmental damage, injury to personnel or asset loss

3.1.31
integrity
probability of a system satisfactorily performing the required function under all the stated conditions within a stated period of time

3.1.32
leak
accidental escape from a process component of liquid and/or gaseous hydrocarbons to atmosphere

3.1.33
liquid overflow
discharge of liquids from a process component through a gas (vapour) outlet

3.1.34
lower flammable limit
LFL
lower explosive limit
LEL
lowest concentration, by volume, of combustible gases in mixture with air that can be ignited at ambient conditions

3.1.35
low flow
in a process component, flowrate lower than the normal operating flowrate but higher than the lowest allowable working flowrate

3.1.36
low liquid level
in a process component, liquid level below the normal operating level but above the lowest allowable working level

3.1.37
low pressure
in a process component, pressure less than the normal operating pressure but more than the lowest allowable working pressure

3.1.38
low temperature
in a process component, temperature less than the normal operating temperature but more than the lowest allowable working temperature

3.1.39
malfunction
any condition of a device or equipment item that causes it to operate improperly, but does not prevent the performance of its design function

3.1.40
maximum allowable operating pressure
highest operating pressure allowable at any point in a pipeline system during normal flow or static conditions

3.1.41
maximum allowable working pressure
highest operating pressure allowable at any point in any process component, other than a pipeline, during normal operation or static conditions

3.1.42
overpressure
in a process component, pressure in excess of the maximum allowable working pressure

NOTE For pipelines, the maximum allowable working pressure is the maximum allowable operating pressure.

3.1.43
pipeline
piping which directs fluids from subsea manifolds to an installation, between installations or between an installation and a shore facility

3.1.44
pneumatic power system
system which supplies pressure to operate pneumatic actuators

3.1.45
pressure safety valve
self-actuated valve that opens when pressure is higher or lower than a set value

3.1.46
process component
single functional piece of production equipment and associated piping used on processing and injection facilities

EXAMPLES Separator, heater, pump, tank.

3.1.47
process shutdown
isolation of a given process station from the overall process by closing appropriate shutdown valves

3.1.48
process station
one or more process components performing a specific process function such as separation, heating, pumping

3.1.49
protection device
instrument or item of equipment used within a protection system

3.1.50
safety integrity level
SIL
discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the safety instrumented system

NOTE SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.

3.1.51
sensor
device which automatically detects an operating condition and transmits a signal to initiate/perform a specific control function

NOTE An example of a control function initiated by a sensor is process component shutdown.

3.1.52
shutdown valve
SDV
automatically operated, fail-closed valve used for isolating a pipeline or process station

3.1.53
shut-in tubing pressure
SITP
maximum pressure that the wellhead could be subjected to as a result of a long-term shut-off of the well

3.1.54
subsurface safety valve
SSSV
automatically operated device installed in a well below the mudline and having the design function to prevent uncontrolled well flow in response to a hazardous situation

3.1.55
subsurface-controlled subsurface safety valve
SSCSSV
SSSV actuated by the pressure characteristics of the well

3.1.56
surface-controlled subsurface safety valve
SCSSV
SSSV controlled from the surface by hydraulic, electric, mechanical or other means

3.1.57
surface safety valve
SSV
automatically operated wellhead valve assembly which will isolate the reservoir fluids upon loss of the power medium

3.1.58
underpressure
in a process component, pressure which is less than the design collapse pressure

3.1.59
underwater safety valve
USV
automatically operated wellhead valve assembly, installed at an underwater wellhead location, which will isolate the reservoir fluids upon loss of the power medium

3.1.60
undesirable event
adverse occurrence or situation in a process component or process station which poses a threat to safety

EXAMPLES Overpressure, underpressure, liquid overflow.

3.1.61
vacuum
in a process component, pressure less than atmospheric pressure

3.1.62
vent
pipe or fitting on a vessel that opens to the atmosphere

NOTE A vent system might contain a pressure and/or vacuum relief device.

3.2 Abbreviated terms

AFP	active fire protection
ASH	combustible gas detector
BDV	blowdown valve
BSL	burner flame detector
CAD	computer-aided design
EDP	emergency depressurization
ESD	emergency shutdown
ESS	emergency support system
F&G	fire and gas system
FES	fire and explosion strategy
FSH	flow safety high
FSL	flow safety low
FSV	flow safety valve
ISA	The Instrumentation, Systems and Automation Society
LFL	lower flammable limit
LSH	level safety high
LSL	level safety low
MAWP	maximum allowable working pressure (rated)
NGL	natural gas liquids
NRTL	nationally recognized testing laboratory
OEL	occupational exposure limit
OSH	occupational safety high (toxic gas)
PFD	process flow diagram
P&ID	piping and instrumentation diagram
PSE	pressure safety element
PSH	pressure safety high
PSHL	pressure safety high and low
PSL	pressure safety low
PSV	pressure safety valve
SAC	safety analysis checklist
SAFE	safety analysis function evaluation