INTERNATIONAL STANDARD

ISO 10418

Third edition
2019-05

Petroleum and natural gas industries — Offshore production installations — Process safety systems

Industries du pétrole et du gaz naturel — Plates-formes de production en mer — Systèmes de sécurité des procédés

Reference number
ISO 10418:2019(E)

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

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 5
4 Symbols and identification for protection devices **5**
4.1 Objectives 5
4.2 Functional requirements 6
5 Safety analysis concepts **6**
5.1 Objectives 6
5.2 General functional requirements 6
5.3 Functional requirements for analysis using structured review techniques 7
6 Process safety system design **8**
6.1 Objectives 8
6.2 Functional requirements 8
Annex A (informative) **Support systems** **12**
Annex B (informative) **Toxic gases** **15**
Bibliography **17**

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 of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document 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 third edition cancels and replaces the second edition (ISO 10418:2003), which has been technically revised. It also incorporates the Technical Corrigendum ISO 10418:2003/Cor.1:2008. The main changes compared to the previous edition are as follows:

— safety analysis tables (SATs) and safety analysis checklists (SACs), which previously were reproduced from API RP 14C, have been deleted and replaced by references to the analysis methods included in API RP 14C;

— simplification of annexes to avoid duplication of API RP 14C content.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Effective management systems are required to address health and safety aspects of activities undertaken by companies associated with offshore recovery of hydrocarbons. These management systems are applied to each stage in the lifecycle of an installation and to related activities.

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

Selection of risk-reduction measures entails the use of sound engineering judgement informed by recognition of the particular circumstances, which can prompt variation to past practices and previously applied codes and standards.

Risk reduction measures include those to minimize and eliminate hazards by design (i.e. use of inherently safer designs), to prevent incidents (i.e. reducing the probability of occurrences), to control incidents (i.e. limit the scale, intensity and duration of a hazardous event), and to mitigate effects (i.e. reducing the consequences).

Extent of hazard identification and risk assessment activities will vary depending on the stage in the installation lifecycle, as well as process conditions, degree of standardization, complexity, number of persons on board and the installation's overall estimated level of risk.

For installations in the early design phases, the evaluations will necessarily be less detailed than those undertaken during later design phases. Design assumptions developed during these early stages are normally verified before the installation becomes operational.

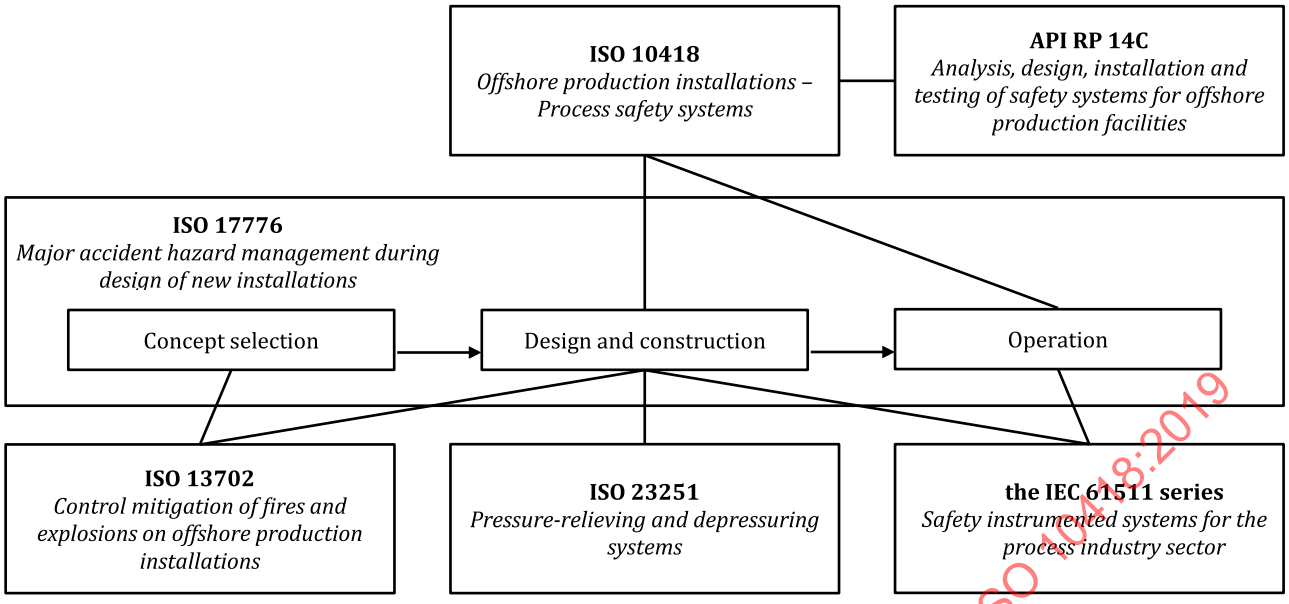
Process safety systems are provided to prevent, detect, control or mitigate undesirable events in process equipment.

This document sets out three options for identifying appropriate process safety systems. The first option is to adopt the prescriptive approach specified in API RP 14C. The second approach is to use structured review techniques to identify hazards and evaluate risk, with process safety systems being provided based on the results of this more specific analysis. The third option is to use a combination of the first two. The use of the structured review techniques is likely to be of benefit for more complex, novel or higher hazards systems.

Figure 1 illustrates the relationship of this document to other documents that play a key role in designing offshore process safety systems. Under the overarching risk management principles of ISO 31000, ISO 17776 provides a framework for managing major accident hazards throughout the facility lifecycle. This document provides requirements and guidelines for process safety systems with more detailed and specific guidance and requirements for particular elements provided in other documents, most notably ISO 13702, ISO 23251 and the IEC 61511 series.

The approach described in this document is intended to be applied in an iterative way. As the design proceeds, hazards that are introduced or changed are systematically identified and the need for additional risk-reduction measures evaluated.

This document has been prepared primarily to assist in the development of new installations. It is not always appropriate to apply certain requirements to an existing installation. During the planning of a major modification to an installation, there can be greater opportunity to implement the requirements.



NOTE The lines between the standards illustrate the main relationships.

Figure 1 — Relationship between offshore-relevant standards

Petroleum and natural gas industries — Offshore production installations — Process safety systems

1 Scope

This document provides objectives, functional requirements and guidelines for techniques for the analysis and design of surface process safety systems for offshore installations used for the recovery of hydrocarbon resources.

It also provides recommendations and requirements on support systems which complement the process safety systems in reducing risk.

NOTE These are not intended to be exhaustive.

The scope of this document is limited to specifying the methods by which the asset is protected against loss of containment of hydrocarbon or other hazardous materials.

This document is applicable to

a) fixed offshore structures, and

b) floating offshore production installations

for the petroleum and natural gas industries.

This document is not applicable to mobile offshore units and subsea installations.

NOTE Nevertheless, many of the principles contained in this document can be used as guidance.

2 Normative references

The following documents are referred to in the 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 13702, *Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines*

IEC 61511 (all parts), *Functional safety — Safety instrumented systems for the process industry sector*

API RP 14C, *Analysis, Design, Installation, and Testing of Safety Systems for Offshore Production Facilities*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
abnormal operating condition
condition which occurs in a *process component* (3.1.21) when an operating variable ranges outside of its normal operating limits

3.1.2
alarm
audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response

[SOURCE: IEC 62682:2014, 3.1.7]

3.1.3
blowdown
emergency depressuring
system discharging gas to flare or other disposal system

3.1.4
containment
situation in which the hazardous material is held safely in a pressurized system

3.1.5
control
<of hazards> limiting the extent or duration of a hazardous event

3.1.6
ESD system
emergency shutdown 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

3.1.7
emergency support system
ESS
portion of the overall facility safety system consisting of the ESD, fire detection, gas detection, ventilation, containment systems, sumps, blowdown system, and *SSSVs* (3.1.28)

3.1.8
fail-closed valve
valve which will move to the closed position upon loss of the power medium or signal

3.1.9
failure
improper performance of a device or equipment item that prevents completion of its design function

3.1.10
fire loop
pneumatic control line containing temperature-sensing elements which, when activated, will initiate control actions in response to a hazardous situation

Note 1 to entry: Fusible plugs and synthetic tubing are examples of temperature-sensing elements.

3.1.11
functional requirements
minimum criteria which shall be satisfied to meet the stated health, safety, and environmental objectives

[SOURCE: ISO 13702:2015, 3.1.24]

3.1.12
gas blowby
discharge of gas from a *process component* (3.1.21) through a liquid outlet

3.1.13
gas detection system
system which monitors spaces on an offshore installation for the presence and concentration of flammable and/or toxic gases, initiates *alarms* (3.1.2), and might initiate control actions at predetermined concentrations

3.1.14
leak
accidental escape from a *process component* (3.1.21) of liquid and/or gaseous hydrocarbons or other hazardous materials to atmosphere

3.1.15
liquid overflow
discharge of liquids from a *process component* (3.1.21) through a gas (vapour) outlet

3.1.16
malfunction
condition of a device or equipment item that causes it to operate improperly, but does not prevent the performance of its design function

3.1.17
maximum allowable working pressure
highest operating pressure allowable at any point in any *process component* (3.1.21), other than a pipeline, during normal operation or static conditions

3.1.18
mobile offshore unit
mobile platform, including drilling ships, equipped for drilling for subsea hydrocarbon deposits, and mobile platform for purposes other than production and storage of hydrocarbon deposits

Note 1 to entry: Includes mobile offshore drilling units, drillships, accommodation units, construction and pipelay units and well servicing and well stimulation vessels.

3.1.19
overpressure
pressure in a *process component* (3.1.21) in excess of the *maximum allowable working pressure* (3.1.17)

Note 1 to entry: For pipelines, refer to relevant design code for the definition of the maximum allowable working pressure.

3.1.20
PRD
pressure relief device
device actuated by inlet static pressure and designed to open during emergency or abnormal conditions to prevent a rise of internal fluid pressure in excess of a specified design value

Note 1 to entry: The device can be a pressure-relief valve (pressure safety valve), a rupture disk device, or a buckling pin device.

3.1.21
process component
single functional piece of production equipment and associated piping used on processing and injection facilities

EXAMPLE Separator, heater, pump, tank.

3.1.22
process safety system
system consisting of devices used on a facility to prevent or mitigate the potentially *undesirable events* (3.1.32) that can occur within the process

3.1.23
protection device
instrument or item of equipment used within a protection system

3.1.24
safety instrumented system
instrumented system used to implement one or more safety instrumented functions

Note 1 to entry: A safety instrumented system is composed of any combination of sensor(s), logic solver(s), and final element(s).

Note 2 to entry: The primary function of a safety instrumented system is to detect and initiate control or mitigation action when there is a potentially hazardous situation.

3.1.25
safety integrity level
discrete level (one out of four) allocated to the safety instrumented function (SIF) for specifying the safety integrity requirements to be achieved by the *safety instrumented system* (3.1.24)

Note 1 to entry: Further details (including definition of SIF) are given in IEC 61511-1:2017.

3.1.26
sensor
device which automatically detects an operating condition and transmits a signal to initiate/perform a specific control function

Note 1 to entry: Process component shutdown is an example of a control function initiated by a sensor.

3.1.27
SDV
shutdown valve
automatically operated, *fail-closed valve* (3.1.8) used for isolation

3.1.28
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

3.1.29
SSCSSV
subsurface-controlled subsurface safety valve
SSSV (3.1.28) actuated by the pressure characteristics of the well

3.1.30
SCSSV
surface-controlled subsurface safety valve
SSSV (3.1.28) controlled from the surface by hydraulic, electric, mechanical or other means

3.1.31
surface safety valve
automatically operated wellhead valve assembly which will isolate the reservoir fluids upon loss of the power medium

3.1.32
undesirable event
adverse occurrence or situation in one or more *process components* (3.1.21) performing a specific process function which poses a threat to safety

EXAMPLE Overpressure, under pressure, gas blowby, liquid overflow.

3.1.33
vacuum
<in a process component> pressure less than atmospheric pressure

3.1.34
vent
pipe or fitting on a vessel or pipework that opens to the atmosphere

Note 1 to entry: A vent system can contain a pressure and/or vacuum relief device.

3.2 Abbreviated terms

AFP	active fire protection
ESD	emergency shutdown
FES	fire and explosion strategy
ISA	International Society of Automation
ISD	inherently safer design
OEL	occupational exposure limit
PFD	process flow diagram
P&ID	piping and instrumentation diagram
PSH	pressure safety high
PSV	pressure safety valve
SAC	safety analysis checklist
SAT	safety analysis table
SIL	safety integrity level
SSC	sulfide stress cracking

4 Symbols and identification for protection devices

4.1 Objectives

The purpose of graphical symbols and identification of protection devices is to

a) uniquely identify safety devices,

b) facilitate the recognition of safety devices throughout an installation and between installations, and

c) aid the systematic design and analysis process.

4.2 Functional requirements

A unique system shall be employed for identifying and symbolizing process safety devices and process components. Individual process safety devices and process components shall be described by a unique identifier (tag). This unique identifier shall be used during the development of design drawings, such as PFDs and P&IDs.

5 Safety analysis concepts

5.1 Objectives

Objectives of a safety analysis are to

a) identify undesirable events that pose a safety risk, and define reliable protective measures that will prevent such events or minimize their effects if they occur,

b) establish a firm basis for designing and documenting a process safety system, and

c) enable verification that the arrangements provided for the protection of process components form an integrated system covering the entire platform through the application of proven analysis technics.

5.2 General functional requirements

5.2.1 An analysis shall be carried out for each process component in order to determine the arrangements provided to prevent, detect, mitigate or control undesirable events which can develop within or external to a process component. The analysis shall be based on scenarios that are selected to represent all reasonably foreseeable hazardous events.

5.2.2 The analysis procedure shall provide a structured method to develop a process safety system and provide supporting documentation.

5.2.3 The analysis shall

a) identify those undesirable events which can compromise the integrity of the process component,

b) identify the safety measures required to prevent, detect, mitigate such events, and

c) establish a firm basis for designing and documenting the provisions of a process safety system.

5.2.4 The safety analysis, system design and protection concepts used shall be in accordance with one of the following:

a) the approach specified in API RP 14C;

b) the approach involving the use of structured review techniques as described in 5.3;

c) a combination of both approaches.

The use of structured review techniques is likely to be of benefit for more complex, novel or higher hazard systems. A combined approach whereby structured review techniques are used for these types of systems, with API RP 14C being applied to simpler or lower hazards systems, is an option that can potentially offer both effective risk reduction and resource efficiency.

5.2.5 Factors to evaluate when selecting the analyses approach, include the following:

a) severity of operating conditions, quantities of hazardous inventories, potential personnel exposure;

b) novelty and complexity of the process to be used;

c) requirements of the regulation authority having jurisdiction over the facility;

d) company requirements in excess of the applicable regulations;

e) skills, experience and competency of those undertaking the analysis;

f) in the case of analysis of a modification, the consistency with the original method of analysis.

5.2.6 If process components that are not included in API RP 14C are used, or if process components are used in a novel way, then use of the structured techniques as described in 5.3 shall be applied or new SAT and SAC, as described in API RP 14C, shall be developed.

5.3 Functional requirements for analysis using structured review techniques

5.3.1 A risk management process shall be applied for

a) identification of hazards,

b) assessment of the risk (this may be qualitative or quantitative), and

c) control of risks.

Use of ISD should be applied to reduce the risk, if practical.

Guidance on application of ISD is in ISO 17776:2016, Annex D.

5.3.2 Structured review techniques shall be selected based on factors including but not limited to the particular features of the installation and its process. Guidance on the selection of tools and techniques is in ISO 17776:2016, Annex C.

5.3.3 A strategy for managing process hazards shall be developed based on the results of the risk management process. The following elements shall be included or referenced in the strategy:

a) application of inherently safer design philosophy;

b) process control, plant start-up and shutdown philosophy;

c) ESD philosophy including plant segregation philosophy;

d) relief and blowdown philosophy;

e) flare and vent philosophy.

5.3.4 A systematic study shall be made to determine those credible undesirable events (such as, but not limited to, overpressure, over filling) in the process that would result in hazardous events. The study shall cover all anticipated modes of operation and assess the adequacy of protection systems for these undesirable events. Guidance for relief is contained in ISO 23251 or API Std. 521.

5.3.5 Process safety system shall be designed to cater for all anticipated operating modes including start-up and shutdown.

5.3.6 The design of the process safety system shall include

a) functional requirements of the process safety system,

b) SIL of each safety instrumented system shutdown loop,

c) bypasses required by the system, and

d) reliability, availability and maintainability of the process safety system components.

NOTE Bypasses prevent an automatic action, on a temporary basis, to allow continued operation.

5.3.7 The analysis technique shall be applied to all process components, from and including topside wellhead or boarding valve to the most downstream discharge point and including injection systems, and shall be incorporated into the overall safety system assessment.

6 Process safety system design

6.1 Objectives

The objectives of the process safety system are to

a) protect personnel, the environment, and the facility from process hazards,

b) prevent the release of hydrocarbons or other hazardous materials, and to minimize the adverse effects of such releases, including escalation,

c) shut in the process or affected part of the process to stop the flow of hydrocarbons or other hazardous materials to a leak or overflow,

d) prevent ignition of released hydrocarbons or other flammable materials, and

e) shut in the process in the event of a gas release or a fire.

6.2 Functional requirements

6.2.1 The design basis for the process safety system shall include the following:

a) good engineering practice based on relevant codes, standards and industry guidance;

b) use of proven analysis techniques to determine the minimum requirement for a process component.

6.2.2 Process components on a production platform, comprising the entire process from topside wellhead or boarding valve to the most downstream discharge point and including injection systems, shall be incorporated into the overall safety system assessment.

6.2.3 Protection measures shall be provided to protect each process component in order to

a) prevent the uncontrolled release of hydrocarbons or other hazardous materials, and

b) minimize the consequences of an uncontrolled release.

6.2.4 Protection measures shall be provided to

a) isolate the process in order to minimize the consequences of a leak or overflow,

b) initiate shutdown or isolation of ignition sources in the event of the release of flammable vapours,

c) shut-in the process in the event of a fire, or gas accumulation, and

d) depressurize the inventory, if necessary, based on risk evaluation, by connecting process safety systems to the system for discharging gas to the atmosphere.

6.2.5 The process safety system provided shall be independent of and in addition to the process control devices used in normal process operation. Failure of the normal process control system shall not cause a

dangerous failure of the process safety system or impede the process safety system from responding to an abnormal event.

6.2.6 The location of SDVs shall be determined based on the following:

a) detailed flow schematic and operating parameters;

b) process segregation/isolation philosophy which considers plant functions, inventories and maintenance/availability requirements;

c) fire and explosion studies.

6.2.7 SSSVs shall be installed below the mudline to prevent uncontrolled well flow in the event of an emergency situation. SSCSSVs should shut in if well rate exceeds a predetermined rate that might indicate a large leak. SCSSVs shall shut in when activated by an ESD system and/or a fire loop. Guidance for the design and installation of SSSVs is covered in ISO 10417.

6.2.8 If events that are external to the process result in fire and/or hazardous materials release, the safety system shall shut down all platform activity except that which is necessary for firefighting and other emergency operations.

NOTE Such events can be caused by natural phenomena, ship or helicopter collision, failure of tools and machinery, or mistakes by personnel. These types of events can be prevented or minimized through the implementation of a structured system to manage safety which includes the safe design of tools and machinery, safe operating procedures for personnel and equipment, and personnel training.

6.2.9 The process safety system provides protection in the following ways:

a) automatic monitoring and automatic protective action if an abnormal operating condition, indicating an undesirable event, is detected by one or more sensors;

b) protective action if manually actuated by personnel who observe or are alerted to an abnormal operating condition by an alarm;

c) continuous protection by support systems that limit the volume and effects of escaping hydrocarbons.

ESD system shall be provided for all offshore installations. ESD systems for not continuously occupied installations shall be designed to ensure that personnel are able to actuate the ESD system locally.

6.2.10 When an abnormal condition is detected in a process component (by a safety device or by personnel), all input sources of hazard shall be shut off or diverted to other components if they can be safely handled. If shutoff is selected, process inputs should be shut off at the primary source of energy (wells, pump, compressor, pipeline, etc.).

6.2.11 The process safety system shall provide two levels of protection to prevent or minimize the consequences of an undesirable event within the process using functionally different types of device. If it is not practicable to provide two functionally different types of protection device, then two sets of the same function safety device may be used, provided it can be demonstrated that they are suitable for the function intended and that the expected demands and common modes of failure have been considered.

NOTE Functionally different types of devices are for example instrumented and mechanical device, as similar devices have the same characteristics and can have the same mode of failure.

6.2.12 The two levels of protection are normally the first to act (primary) and the next to act (secondary). Judgment is required to determine these two levels for a given situation.

NOTE As an example, two levels of protection from a rupture due to overpressure might be provided by a PSH, which could be used to initiate isolation of the affected equipment before rupture can occur, and a PSV, which prevents a rupture by relieving excess volumes to a safe location.

In selecting the setting for the primary level of protection

a) the value shall be above the maximum normal operating pressure including allowance for accuracy of setting and normal process disturbances,

b) the value shall be below the secondary protection level setting, including allowance for accuracy of both level settings, and

c) the rate of rise of the process parameter and the speed of response of the system shall be taken into account.

6.2.13 If instrument-based systems are used as both the primary and secondary methods of protection, SIFs shall be assigned a SIL and designed and implemented in accordance with the IEC 61511 series.

Under the API RP 14C approach, if an instrument-based system is used for primary protection, it will not need to conform with the IEC 61511 series, provided the secondary protection system is self-actuating and meets the requirements of relevant codes and standards.

Under the approach using structured review techniques, each safety instrumented function is assigned a SIL (see 5.3.6) and designed and implemented in accordance with the IEC 61511 series.

6.2.14 An ESS is required for emergency situations that result in fire and gas events that could cause a risk to the facility or to the personnel. The ESS shall not be used as the sole or secondary level of protection for overpressure.

The ESS does not need to meet the requirements of the IEC 61511 series, unless it is part of a safety instrumented function.

Guidance on ESS is provided in Annex A.

6.2.15 The ESS shall minimize the effects of escaped hydrocarbons and toxic fluids on offshore production platforms. The ESS can include the following:

a) a flammable gas detection system to sense the presence of escaped hydrocarbons and initiate platform shutdown;

b) where necessary, a toxic gas detection system to sense the presence of toxic gases and initiate platform shutdown;

NOTE 1 Annex B provides guidelines and methods of handling toxic gases.

NOTE 2 Categorization of the facilities according to toxic gas hazard for personnel access is implemented to indicate areas where specific protective means are required (breathing apparatus, portable and fixed detections, etc.). An example is given in Annex B.

c) a containment system to collect escaped liquid hydrocarbons and initiate platform shutdown;

d) devices to sense the heat or flame from a fire and initiate platform shutdown (e.g. flame detection, heat detection, smoke detection, fire loop);

e) a method to manually initiate platform shutdown by personnel observing abnormal conditions or undesirable events;

f) SSSVs that may be self-actuated (SSCSSV) or activated by an ESD system and/or a fire loop (SCSSV);

g) blowdown process components to divert hydrocarbon gas inventory to a safe location in the case of a fire or leak.

6.2.16 The ESS shall be designed to meet the functional requirements as specified in the FES developed in accordance with ISO 13702.

NOTE The integrity of a platform system depends on proper operation of several other support systems.

6.2.17 The process safety system design shall include arrangements for controlling and managing the following:

a) bypasses on shutdown loops;

b) resetting of tripped shutdown loops;

c) testing of primary and secondary devices;

d) management of change to the process or shutdown loops and shutdown systems.

6.2.18 Each protection measure shall have a functional specification that defines the technical and operational requirements it needs to meet in order to achieve its safeguarding functions.

6.2.19 Where systems have been specified as a result of applying structured review techniques in accordance with 5.3, they shall be installed, maintained and tested to meet the functional and performance requirements determined to be necessary by the analysis techniques used.

6.2.20 The design of the process safety systems shall be documented, including the following:

a) hazards and hazardous events that have been used as a basis for the design;

b) records of any SIL determination and assumptions made;

c) specifications and drawings;

d) functions required and cause and effect diagrams (including inputs and outputs of the ESS);

e) details of equipment used to prevent hazardous events occurring and mitigate the consequences;

f) index of alarms and trips;

g) index of PSVs and associated sizing basis.

6.2.21 Documentation shall be maintained and controlled throughout the design and operation of the installation.

Annex A
(informative)

Support systems

A.1 General

ESSs should be provided in accordance with Annex G of API RP 14C (8th edition).

A.2 Guidance for emergency support systems

A.2.1 Purpose

The ESS is used as protection against leakage and the performance requirements for the system will need to be determined. For manned installations, fire and gas detection and ESD systems are likely to contribute to reducing risk, and should be engineered to achieve the functional requirements identified in the FES as described in ISO 13702.

A.2.2 Functions of the ESS

The primary function of the ESS is to isolate the installation from the reservoir and pipelines. The ESS can also be used for additional functions, including the following:

a) isolation to segregate sections of the installation;

b) initiation of blowdown;

c) isolation of electrical equipment to prevent further development of electrical fires;

d) initiation of shutdown of ventilation system to minimize ingress of smoke or flammable gas;

e) initiation of isolation of electrical equipment and other potential ignition sources upon detection of flammable gas, to minimize risk of ignition;

f) initiation of AFP systems if these have been provided to control or mitigate fires;

g) initiation of muster of personnel.

The criticality of the additional functions should be considered, assessed and managed accordingly.

A.2.3 General approach

A.2.3.1 General

Irrespective of the design approach adopted, it is important that the risk reduction required from the fire and gas detection and protection functions are assessed to ensure that the system will have adequate integrity to fulfil its role.

A.2.3.2 Fire and gas detection

The technique applied for the assessment of fire and gas detection should

a) be systematic,

b) be auditable,

c) produce consistent results, and

d) take into account the hazards in the areas where detection is provided.

Furthermore, the system design, maintenance and testing should take into account the required reliability.

Fire and gas detection and associated protective functions reduce the risk in the local area where they are installed and also reduce the risk of a local incident escalating into a hazardous event with very severe consequences. The effectiveness of fire and gas detection and protective functions in preventing local consequences can be limited because performance is dependent on many factors related both to the capabilities of the devices, the nature of the events that can arise and the environment in which they are located. ISA-TR 84.07-2010 provides more information on the limitations of fire and gas systems.

Examples of the factors that affect performance and limit the ability to set simple performance targets include the following:

a) there are likely to be a number of hazardous events that can arise in any area, each with potentially many different outcomes;

b) the outcome of the event is a function of the speed of detection, which itself is related to the size of the event and the location within the area;

c) partial failure to initiate planned actions may not always significantly increase the risk to people or to the location;

d) manual detection can occur and initiate the required functions before the detection system has responded (e.g. by operation of field-mounted shutdown devices);

e) leak frequencies for each possible source of leak are higher for low leakage rates and lower for high leakage rates;

f) coverage factors (the probability that a leak will be detected by sensors) for a particular leak source depend on the size of leak and the number and location of detectors;

g) not all of the actions taken will be necessary for every source of release.

A.2.3.3 Safety integrity level approach

Other protection features such as blowdown, blast and fire resistance, ventilation, design of the temporary refuge and the evacuation, escape and rescue features should also be considered when evaluating the contribution of the ESS to the overall risk reduction required to reduce the likelihood of escalation resulting in very severe consequences to people or to the location.

Risk reduction requirements for safety instrumented systems can be determined by using a qualitative or a quantitative approach as described in the IEC 61511 series.

Where the ESS forms part of SIF(s), guidance on assigning a SIL is provided in the IEC 61511 series.

A.3 Blowdown and discharging gas to atmosphere

A.3.1 Purpose

Systems for discharging gas to the atmosphere provide a means for conducting discharged gas from process components under normal conditions (flare, vent) and abnormal conditions (relief) to safe locations for final release to the atmosphere.

As an alternative, discharged gas under normal conditions may be collected and returned to the process. In such cases if there is a need for depressuring, a control valve is normally installed to act as a vent valve and this directs the flow of relieved gas to the flare. A rupture disk is normally included in