Draft for Public Comment

PRIVATE CIRCULATION
PSE/17/-/6_15_0021
For comment - Action Due Date: 2015/11/24

Form 36

DPC: 15 / 30328952 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: + 44 (0)20 8996 9000
Fax: + 44 (0)20 8996 7400
www.bsigroup.com

Date: 24 September 2015
Origin: European

Latest date for receipt of comments: 24 November 2015 Project No. 2015/02077

Responsible committee: PSE/17/-/6 Processing equipment and systems for petroleum and natural gas industries

Interested committees:

Title: Draft BS EN ISO 10418 Petroleum and natural gas industries - Offshore production installations - Process safety systems

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard
i) has any issues related to 3rd party IPR, patent or copyright
ii) affects other national standard(s)
iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 24 November 2015

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop **http://shop.bsigroup.com** or from BSI Customer Services, Tel: + 44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from **http://standardsdevelopment.bsigroup.com**

Responsible Committee Secretary: **Mr Bernard N Shelley (BSI)**
Direct tel: **020 8996 7217**
E-mail: **bernard.shelley@bsigroup.com**

Introduction

This draft standard is based on European discussions in which the UK has taken an active part. Your comments on this draft are welcome and will assist in the preparation of the consequent British Standard. Comment is particularly welcome on national, legislative or similar deviations that may be necessary.

Even if this draft standard is not approved by the UK, if it receives the necessary support in Europe, the UK will be obliged to publish the official English Language text unchanged as a British Standard and to withdraw any conflicting standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with reasons) or positive vote on this draft.

Submission of Comments

- The guidance given below is intended to ensure that all comments receive efficient and appropriate attention by the responsible BSI committee. **Annotated drafts are not acceptable and will be rejected.**

- All comments must be submitted, preferably electronically, to the Responsible Committee Secretary at the address given on the front cover. Comments should be compatible with version 6.0 or version 97 of Microsoft Word for Windows, if possible; otherwise comments in ASCII text format are acceptable. **Any comments not submitted electronically should still adhere to these format requirements.**

- All comments submitted should be presented as given in the example below. Further information on submitting comments and how to obtain a blank electronic version of a comment form are available from the BSI website at: **http://drafts.bsigroup.com/**

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: **ISO/DIS xxxx**

1	2	(3)	4	5	(6)	(7)
MB	**Clause No./ Subclause No./Annex** (e.g. 3.1)	**Paragraph/ Figure/ Table/Note**	**Type of comment**	**Commend (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations on each comment submitted**
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '…so that the mains connector to which no connection…'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

EXAMPLE ONLY

Microsoft and MS-DOS are registered trademarks, and Windows is a trademark of Microsoft Corporation.

DRAFT INTERNATIONAL STANDARD

ISO/DIS 10418

ISO/TC **67**/SC **6**

Secretariat: **AFNOR**

Voting begins on:
2015-09-24

Voting terminates on:
2015-12-24

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

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

ICS: 75.180.10

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 10418:2015(E)

© ISO 2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2015 – All rights reserved

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 third edition cancels and replaces the second edition (ISO 10418:2003), which has been technically revised including the following:

— the risk based methods of analysis as specified in edition 2 are included as a basis of design but details of the analysis method based on the use of safety analysis tables (SATs) and safety analysis checklists (SACs) have been deleted and replaced by references to the analysis methods included in API RP 14C

— a screening process is included in a revised Annex B to simplify the setting of safety integrity levels for fire and gas and ESD systems.

© ISO 2015 – All rights reserved

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.

© ISO 2015 – All rights reserved

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 references standards such as IEC 61511 and 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.

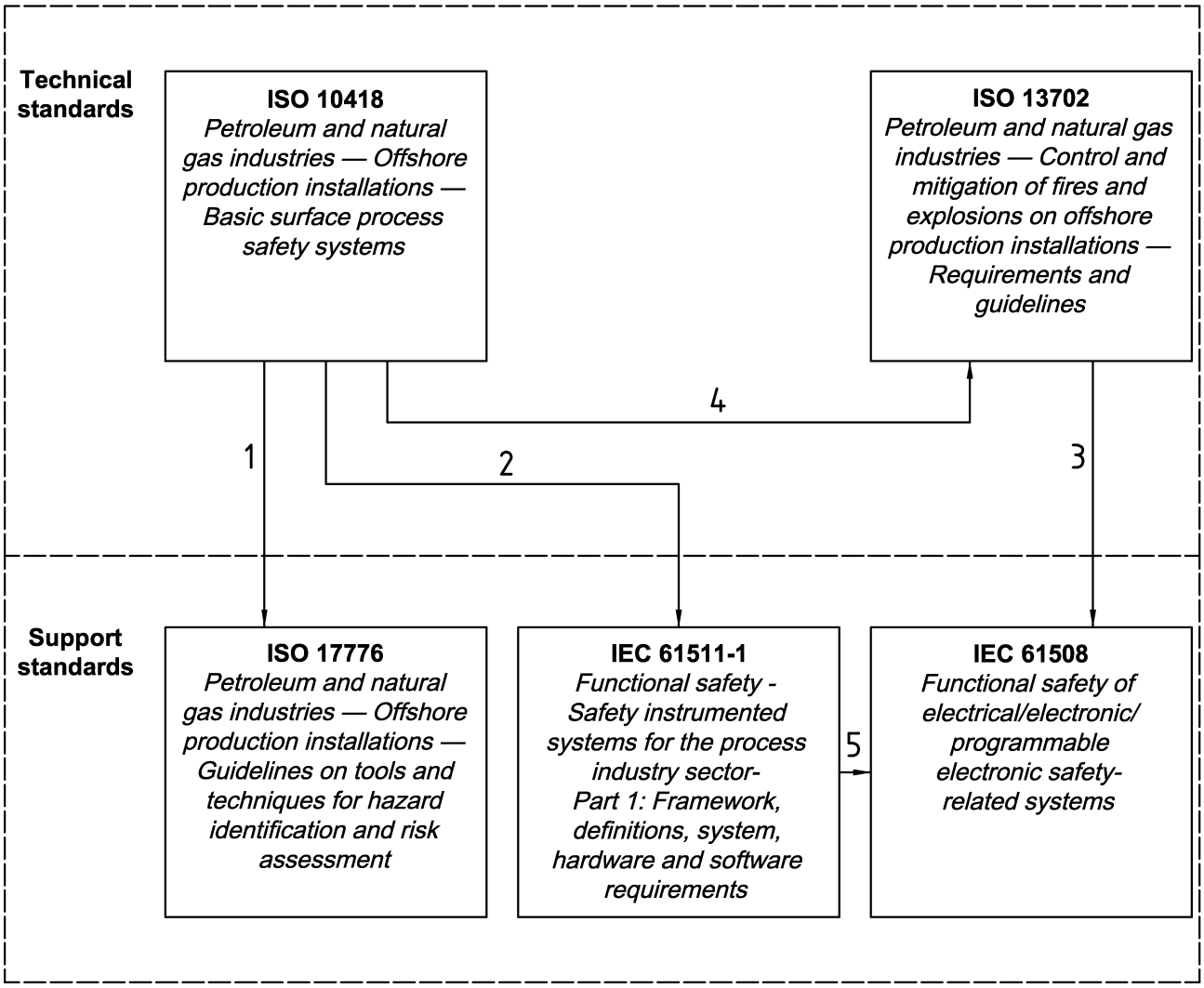
This International Standard and ISO 13702 reference new standards on functional safety of instrumented systems. This International Standard refers to IEC 61511-1, which is the process sector implementation of the generic standard IEC 61508 that is referred to in ISO 13702. The relationship between the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

© ISO 2015 – All rights reserved



Key – The numbered arrows explain purpose of the references to the other ISO standards

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

© ISO 2015 – All rights reserved

Petroleum and natural gas industries — Offshore production installations — 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. The scope of this International Standard is limited to specifying the methods by which the asset is protected against loss of containment of hydrocarbon material. Requirements for how the systems are selected, implemented and managed throughout the detailed design and subsequent operation of the facility are not included in this 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

© ISO 2015 – All rights reserved

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
bypass
temporary disablement of a protective measure for the purpose of operation outside the normal limits e.g. for proof testing or start up

3.1.8
detectable abnormal condition
abnormal operating condition which can be detected by a sensor

3.1.9
direct ignition source
any source with sufficient energy to initiate combustion

3.1.10
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

3.1.11
excess temperature
in a process component, temperature higher or lower than the rated working temperature

3.1.12
fail-closed valve
valve which will move to the closed position upon loss of the power medium or signal

3.1.13
failure
improper performance of a device or equipment item that prevents completion of its design function

3.1.14
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

© ISO 2015 – All rights reserved

3.1.15
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

3.1.16
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: Examples of temperature-sensing elements are: fusible plugs, synthetic tubing, etc.

3.1.17
flame failure
flame which is inadequate to instantaneously ignite combustible vapours entering the firing chamber of a fired vessel

3.1.18
flowline
piping which directs the well stream from the wellhead to the first downstream process component

3.1.19
flowline segment
any portion of a flowline that has an operating pressure different from another portion of the same flowline

3.1.20
gas blowby
discharge of gas from a process component through a liquid outlet

3.1.21
gas detection system
system which monitors spaces on an offshore installation for the presence and concentration of flammable and/or toxic gases and initiates alarm and may initiate control actions at predetermined concentrations

3.1.22
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

3.1.23
hazardous event
incident which occurs when a hazard is realised

EXAMPLES Release of gas, fire, gas blowby.

3.1.24
high liquid level
in a process component, liquid level above the normal operating level but less than the maximum allowable working level

3.1.25
high pressure
in a process component, pressure in excess of the normal operating pressure but less than the maximum allowable working pressure

Note 1 to entry: For pipelines, the maximum allowable working pressure is the maximum allowable operating pressure.

© ISO 2015 – All rights reserved

3.1.26
HP/LP interface
point in a process plant where operating pressure changes from high pressure to low pressure

Note 1 to entry: A change in system design pressure or piping class is often associated with the HP/LP interface.

3.1.27
high temperature
in a process component, temperature in excess of the normal operating temperature but less than the maximum allowable working temperature

3.1.28
indirect heated component
vessel or heat exchanger used to increase the temperature of a fluid by heat transfer from another hot fluid

Note 1 to entry: Examples of hot fluids are steam, hot water, hot oil, or other heated medium.

3.1.29
installation safety system
arrangement of safety devices and emergency support systems to effect installation shutdown

Note 1 to entry: The system can consist of a number of individual process shutdowns and can be actuated by either manual controls or automatic sensors.

3.1.30
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

3.1.31
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

3.1.32
integrity
probability of a system satisfactorily performing the required function under all the stated conditions within a stated period of time

3.1.33
leak
accidental escape from a process component of liquid and/or gaseous hydrocarbons to atmosphere

3.1.34
liquid overflow
discharge of liquids from a process component through a gas (vapour) outlet

3.1.35
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

3.1.36
low flow
in a process component, flowrate lower than the normal operating flowrate but higher than the lowest allowable working flowrate

© ISO 2015 – All rights reserved

3.1.37
low liquid level
in a process component, liquid level below the normal operating level but above the lowest allowable working level

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

3.1.39
low temperature
in a process component, temperature less than the normal operating temperature but more than the lowest allowable working temperature

3.1.40
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

3.1.41
maximum allowable operating pressure
highest operating pressure allowable at any point in a pipeline system during normal flow or static conditions

3.1.42
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

3.1.43
overpressure
in a process component, pressure in excess of the maximum allowable working pressure

Note 1 to entry: For pipelines, the maximum allowable working pressure is the maximum allowable operating pressure.

3.1.44
pipeline
piping which directs fluids from subsea manifolds to an installation, between installations or between an installation and a shore facility

3.1.45
pneumatic power system
system which supplies pressure to operate pneumatic actuators

3.1.46
pressure safety valve
self-actuated valve that opens when pressure is higher or lower than a set value

3.1.47
process component
single functional piece of production equipment and associated piping used on processing and injection facilities

EXAMPLES Separator, heater, pump, tank.

3.1.48
process shutdown
isolation of a given process station from the overall process by closing appropriate shutdown valves

© ISO 2015 – All rights reserved

3.1.49
process station
one or more process components performing a specific process function such as separation, heating, pumping

3.1.50
protection device
instrument or item of equipment used within a protection system

3.1.51
safety instrumented system
instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s)

Note 1 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.

3.1.52
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 1 to entry: SIL 4 has the highest level of safety integrity; SIL 1 has the lowest. Applications which require the use of a single safety instrumented function of safety integrity level 4 are rare in the process industry. Such applications should be avoided where reasonably practicable because of the difficulty of achieving and maintaining such high levels of performance throughout the safety life cycle. (ref IEC 61511-1 section 9.3.1).

3.1.53
sensor
device which automatically detects an operating condition and transmits a signal to initiate/perform a specific control function

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

3.1.54
shutdown valve
SDV
automatically operated, fail-closed valve used for isolating a pipeline or process station

3.1.55
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

3.1.56
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

3.1.57
subsurface-controlled subsurface safety valve
SSCSSV
SSSV actuated by the pressure characteristics of the well

© ISO 2015 – All rights reserved

3.1.58
surface-controlled subsurface safety valve
SCSSV
SSSV controlled from the surface by hydraulic, electric, mechanical or other means

3.1.59
surface safety valve
SSV
automatically operated wellhead valve assembly which will isolate the reservoir fluids upon loss of the power medium

3.1.60
underpressure
in a process component, pressure which is less than the design collapse pressure

3.1.61
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

3.1.62
undesirable event
adverse occurrence or situation in a process component or process station which poses a threat to safety

EXAMPLES Overpressure, underpressure, liquid overflow.

3.1.63
vacuum
in a process component, pressure less than atmospheric pressure

3.1.64
vent
pipe or fitting on a vessel or pipework that opens to the atmosphere

Note 1 to entry: 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

© ISO 2015 – All rights reserved

FSV	flow safety valve
ISA	the International Society of Automation
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
PZV	pressure safety valve
SAC	safety analysis checklist
SAFE	safety analysis function evaluation
SAT	safety analysis table
SCSSV	surface-controlled subsurface safety valve
SDV	shutdown valve
SIL	safety integrity level
SITP	shut-in tubing pressure
SSC	sulfide stress cracking
SSCSSV	subsurface-controlled subsurface safety valve
SSSV	subsurface safety valve
SSV	surface safety valve
TSE	temperature safety element (heat detector)
TSH	temperature safety high
TSHL	temperature safety high and low
TSL	temperature safety low
TSV	temperature safety valve
USH	ultraviolet/infrared safety high (flame detector)

© ISO 2015 – All rights reserved

USV underwater safety valve

YSH smoke safety high

4 Symbols and identification for protection devices

4.1 Objectives

The purpose of graphical symbols and identification on protection devices is:

— to uniquely identify safety devices used in process plants;

— to facilitate the recognition of safety devices throughout an installation and between installations;

— to aid the systematic design and analysis process.

4.2 Functional requirements

On any installation, a unique system shall be employed for identifying and symbolizing all safety devices and process components. This shall result in individual safety devices and process components being described by a unique identifier (tag) which then shall be used during the development of design drawings, such as PFDs and P&IDs.

5 Safety analysis concepts

5.1 Objectives

The objectives of a safety analysis are:

— to 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;

— to establish a firm basis for designing and documenting a production installation safety system;

— to enable verification that safety has been achieved, through the application of a proven analysis technique, and that the arrangements provided for the protection of process components form an integrated system covering the entire platform.

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 detect, prevent, mitigate or control undesirable events which may 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 that could affect the process equipment.

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:

— identify those undesirable events which may compromise the integrity of the process;

— identify the safety measures required to detect, prevent or mitigate such events;

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

5.2.4 The analysis techniques used shall be in accordance with:

© ISO 2015 – All rights reserved

— the approach specified in API RP 14C;

— the approach involving the use of structured review techniques as described in 5.3.

In many instances there are benefits in using a combination of the above techniques.

5.2.5 In selecting the analysis approach to follow, account shall be taken of the following:

— the skills, experience and competency of those undertaking the analysis;

— the novelty and complexity of the process systems to be used;

— the requirements of the Regulation Agency having jurisdiction over the facility;

— the Operator requirements in excess of the Regulation Agencies having jurisdiction;

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

NOTE Further guidance on the selection of hazard and risk assessment methods is given in Clause 4 of ISO 17776:2000.

5.2.6 If process components are used that are not included in API RP 14C, or if process components are used in a novel way, then use of the structured techniques as described in 5.3 shall be considered 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:

— the identification of hazards;

— the assessment of the risk (this may be qualitative or quantitative);

— the control of risks.

The use of inherently safe designs will help to reduce the risk from plant and equipment. Guidance on risk management is contained in Clause 5 of ISO 17776:2000.

5.3.2 Where a structured review technique is to be used for the risk management process the assessment shall be appropriate to the installation and the activities to be undertaken on the installation. Guidance on the selection of tools and techniques for this process is contained in 4.5 of ISO 17776:2000.

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

— the process control and shutdown philosophy;

— the ESD plant segregation philosophy;

— the ESD philosophy;

— the relief and blowdown philosophy;

— the flare and vent philosophy.

5.3.4 A systematic study shall be made to determine those credible undesirable events in the process that would result in hazardous events. The study shall cover all modes of operation. The study shall assess the

© ISO 2015 – All rights reserved

adequacy of the protection systems for these undesirable events such as overpressure, underpressure and liquid overfill, and shall consider:

— the undesirable events;

— the design capability of the process components;

— relief capacity requirement and the design relief case;

— the relief rate requirements (e.g. control valve maximum throughput);

— the capability of the PSVs to work effectively in all relevant overpressure scenarios;

— adequacy of the relief capacity;

— the assumptions made about the configuration or operation of the let-down stations (e.g. control valves);

— whether the executive action of the instrumented protection devices to enable judgement on whether they will be effective in preventing overpressure in particular scenarios. Spurious trip and partial failure shall be considered when the adequacy of the protection system is being considered.

5.3.7 The operation of the process safety system shall be checked for operability during normal plant start-up and normal plant shutdown conditions.

5.3.8 The design of the process safeguarding system shall be determined including:

— the functional requirements of the process safeguarding system;

— the SIL of each safety instrumented system shutdown loop;

— the inhibits and bypasses required by the system;

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

NOTE Inhibits and bypasses prevent an automatic action, on a temporary basis, to allow continued operation.

5.3.9 The analysis technique shall be applied to all process components, from topside wellhead or boarding valve to the most downstream discharge point.

6 Process safety system design

6.1 Objectives

The objectives of the process safety system are:

— to protect personnel, the environment, and the facility from risks caused by the production process;

— to prevent the release of hydrocarbons or high pressure or toxic fluids from the process, and to minimize the adverse effects of such releases if they occur;

— to shut in the process or affected part of the process to stop the flow of hydrocarbons to a leak or overflow;

— to prevent ignition of released hydrocarbons or other flammable materials;

— to shut in the process in the event of a fire;

— to prevent the release of hydrocarbons or hazardous fluids from other equipment.

© ISO 2015 – All rights reserved

6.2 Functional requirements

6.2.1 The design basis for the process safety system shall include the appropriate contribution of:

— good engineering practice;

— the use of proven analysis techniques to determine the minimum requirement for a process component which shall be valid in the process configuration.

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

NOTE When fully protected process components are combined into a facility, no additional threats to process integrity are created. Therefore, if all process component safety devices are sized to take account of the cumulative needs if an undesirable event has an impact on more than one component and logically integrated into a process safety system, the entire facility is protected.

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

— prevent the uncontrolled release of hydrocarbons or other fluids;

— minimize the consequences of an uncontrolled release.

6.2.4 Protection measures shall be provided to:

— isolate the process as required in order to minimize the consequences of a leak or overflow;

— initiate shutdown or isolation of ignition sources in the event of the release of flammable vapours;

— shut-in the process in the event of a fire or gas accumulation;

— depressurize the inventory, if necessary, by connecting process systems to the system for discharging gas to the atmosphere.

6.2.5 The 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 safety system or impede the safety system from responding to an abnormal event.

6.2.6 The location of SDVs and other final control devices shall be determined from a study of the detailed flow schematic and from a knowledge of operating parameters.

SDV location shall be based on a process segregation/isolation philosophy which considers plant functions, inventories and maintenance/availability requirements.

6.2.7 SSSVs shall be installed below the mudline to prevent uncontrolled well flow in the event of an emergency situation. SSCSSVs shall 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.

NOTE Guidance for the design and installation of SSSVs is covered in ISO 10417[3].

6.2.8 Abnormal operating conditions which may lead to an undesirable event shall be prevented by the provision of an instrument protection system, or self-actuating devices.

6.2.9 If events that are external to the process can affect the process, the safety system shall shut down the process or affected part of the process. If these external events result in fire, the safety system shall shut down all platform activity except that which is necessary for fire fighting and other emergency operations.

© ISO 2015 – All rights reserved

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.

6.2.10 The operating modes of the safety system shall be:

a) automatic monitoring and automatic protective action if an abnormal condition, indicating an undesirable event, is detected by a sensor;

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

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

NOTE The ESD system is important, even on facilities that are not continuously manned, because most accidents and failures occur during operations that take place when personnel are present. Thus, personnel may be available to actuate the ESD system.

6.2.11 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 shall be shut off at the primary source of energy (wells, pump, compressor, pipeline, etc.).

6.2.12 The safety system shall normally provide two levels of protection to prevent or minimize the consequences of an undesirable event within the process. If practicable, the two levels shall be provided by functionally different types of device.

NOTE 1 Similar devices have the same characteristics and can have the same mode of failure.

NOTE 2 If a structured review as described in 5.3 has been undertaken, it is possible to justify the elimination of some of the primary or secondary protection devices normally required by application of the approach detailed in API RP 14C.

6.2.13 The two levels of protection shall be the first to act (primary) and the next to act (secondary). Judgement is required to determine the best choice of protection devices 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, consideration shall be given to the following:

— the value shall be above the maximum normal operating pressure including appropriate allowance for accuracy of setting and normal process disturbances;

— the value shall be below the relief set pressure, including allowance for accuracy of setting;

— the rate of rise of the process parameter and the speed of response of the system.

6.2.14 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.

EXAMPLE If overpressure protection is required and it is not practicable to provide a relief system an instrument protection system with an appropriate level of redundancy could be used, comprised of a sensor system to detect overpressure, a logic system and shutdown valves to isolate the source of overpressure.

© ISO 2015 – All rights reserved

6.2.15 If instrument-based systems are used as both the primary and secondary methods of protection, and failure would result in serious injury or environmental loss then such systems shall be designed and implemented in accordance with IEC 61511-1.

NOTE 1 If an instrument-based system is used for primary protection, it will not need to comply with IEC 61511-1 provided the secondary protection system is self-actuating and meets the requirements of relevant codes and standards.

NOTE 2 Loss of containment can arise for a number of reasons including overpressure and for some atmospheric tanks, by overfilling. In the case of overfilling, the primary method of protection is likely to be instrument-based (LSH). The secondary method can be an ESS or a second instrument-based system. If both methods are instrument-based, then the systems are designed and implemented to achieve the necessary safety integrity level in accordance with IEC 61511.

6.2.16 An emergency support system (ESS) is required for all emergency situations that result in fire and gas events that could cause a risk to the facility. The ESS shall not be considered as the sole or secondary level of protection for overpressure.

NOTE The ESS does not need to meet the requirements of IEC 61511-1 unless it is required for significant risk reduction. Guidance on requirements for the safety integrity level of ESS is included in Annex B.

6.2.17 The ESS (see Annex A) shall minimize the effects of escaped hydrocarbons and toxic fluids on offshore production platforms. The ESS may include the following:

a) a combustible gas detection system to sense the presence of escaped hydrocarbons and initiate alarms and platform shutdown before gas concentrations reach the LFL;

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

NOTE Annex B provides guidelines and methods of handling sour production.

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) an ESS to provide 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.

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

NOTE Information on how to design and lay out the ESS according to standard methods, as well as means for creating a performance-based design using safety integrity levels, is included in Annex B.

6.2.19 The integrity of a platform system depends on proper operation of several other support systems. These ancillary support systems carry the same degree of importance as other portions of the platform safety system, and shall be equally well maintained.

NOTE Annex A discusses the pneumatic and hydraulic supply systems, electrical power supplies (if actions are energise to trip) and systems for discharging gas to the atmosphere. The pneumatic and hydraulic supply systems are installed to provide power for actuators. The pneumatic system also provides a supply for instruments. Systems for discharging gas to the atmosphere are installed to provide a means for conducting discharged gas from process components to safe locations for final release to the atmosphere. ISO 13702 is referenced for requirements for these systems.

6.2.20 The process safety system design shall include arrangements for managing:

© ISO 2015 – All rights reserved

— inhibits and bypasses on shutdown loops;

— resetting of tripped shutdown loops;

— testing of primary and secondary devices;

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

6.2.21 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.

6.2.22 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.

6.2.23 The design of the process safety systems shall be recorded in data and diagrams, including the following:

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

— records of SIL determination and assumptions made;

— specifications and drawings;

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

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

— index of alarms and trips;

— index of PSVs and associated sizing basis.

6.2.24 The data and documents shall be maintained as live, controlled documents throughout the design and operation of the installation.

© ISO 2015 – All rights reserved

Annex A
(informative)

Support systems

A.1 General

Emergency support systems should be provided in accordance with Annex C of API RP 14C.

A.2 Specific requirements for determination of safety integrity levels 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 and ESD systems are very 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 integrity level requirements for this function should be determined so that it can be used as part of the specification for the systems to be used. The ESS can also be used for additional functions, including the following:

— secondary isolation to segregate sections of the installation;

— initiation of emergency depressurization;

— isolation of electrical equipment to prevent further development of electrical fires;

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

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

— initiation of AFP systems if these have been provided to control or mitigate hydrocarbon fires;

— initiation of muster of personnel.

The criticality of the additional functions should be considered and, if assessed to be critical, they should be included in the function for which the required safety integrity level should be determined.

It should be noted that, as additional functions are included in the functions for which the safety integrity levels are to be determined, it will become progressively more difficult to implement systems and demonstrate that they meet the safety integrity requirements.

A.2.3 General approach

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. The technique applied for such assessment should

© ISO 2015 – All rights reserved

— be systematic;

— be auditable;

— produce consistent results;

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

Furthermore, the system design, maintenance and testing should take into account the results of the safety integrity level determination.

Fire and gas 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 and protective functions in preventing local consequences may be limited because performance is dependent on many factors related both to the capabilities of the devices, the nature of the events that may arise and the environment in which they are located (for more information on the limitations of fire and gas systems see ISA-TR 84.07-2010). Examples of the factors that affect performance and limit the ability to set simple performance targets include:

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

2) 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.

3) Partial failure to initiate planned actions may not always significantly increase the risk to people or to the location.

4) Manual detection may occur and initiate the required functions before the detection system has responded (e.g. by operation of field-mounted shutdown devices).

5) Leak frequencies for each possible source of leak are high for low leakage rates and low for high leakage rates

6) 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.

7) Not all of the actions taken will be necessary for every source of release.

Other protection facilities such as blast and fire resistance, ventilation, the design of the temporary refuge and the escape facilities 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 the location.

This complexity means that a simplified Layer of Protection Analysis normally used to establish the risk reduction requirements for process protection will not normally be adequate for modelling all the factors that contribute to risk. A modified LOPA type approach can be used but the number of leak sources makes the whole process impracticable for evaluation of the requirements in general process areas.

Risk reduction requirements for safety instrumented systems can be determined by using a qualitative or a quantitative approach and this is made clear in IEC 61511-1. Where the reliability of the ESS should be greater than 90 % in order to achieve an acceptable risk level for the location, then the systems should be designed in accordance with IEC 61511-1. For most installations it is sufficient to design, install and maintain the ESS in line with recognised codes and standards, such as ISO 13702 and ISO 15544, providing the selected standard identifies requirements that ESS should meet in order achieve a performance and reliability consistent with industry good practice. For these cases, there is no need to design the systems to comply with the requirements of IEC 61511. However, for some installations, the risk management process, taking into account the relevant factors of the installation such as properties of fluids being handled and the engineering

© ISO 2015 – All rights reserved

design, may set specific targets for the ESS reliability in order to meet the safety objectives for the installation. In these cases, the relevant systems should be designed, installed and maintained to achieve the required SIL level in accordance with IEC 61511.

The general approach to setting the safety integrity level of fire and gas detection systems should comprise the following steps:

a) Undertake a systematic process to identify the hazards and effects that may arise from the location and activities and from the materials which are used or encountered in them.

b) Develop the FES to describe the management of accidental risks by the provision of appropriate measures to mitigate the consequences as and when a loss of containment arises for each of the two application categories. As part of the FES, define the role, integrity and criticality of risk-reduction measures such as the fire and gas detection system. For application in the first category where risk reduction requirements are 10 or less the integrity level requirements will be lower than SIL1. For more details see ISO 13702.

If an ESS (or part of an ESS) has a role in risk reduction with a target reliability of greater than 90 % then an evaluation for each mitigating function of the ESS should be performed in accordance with A.2.4. The evaluation should consider the overall system, comprising detection device, logic solver and output devices that provide the mitigation, and determine the required integrity for the overall system for the safety of people, protection of the asset and protection of the environment. The ESS should be:

a) engineered to achieve the safety integrity target considering the reliability of the system once the appropriate stimulus is provided to the field devices;

b) plan the maintenance, testing and inspection routines to ensure that the required reliability of operation will be achieved in practice;

c) monitor results of inspection and testing, and adjust if necessary.

A.2.4 Determining the integrity level requirements

A.2.4.1 General

The evaluation discussed in A.2.3 may be undertaken in a number of ways. Recognized methods of risk analysis include quantitative risk analysis (QRA) and layer of protection analysis (LOPA). General advice on the use of such techniques is included in IEC 61511-3. If LOPA is used then the general purpose approach should be modified to include factors such as coverage to be included. More detailed guidance on the application of some of the techniques is given in A.2.4.2and A.2.4.3.

A.2.4.2 Determining the integrity required to meet an overall risk requirement

Evaluation of the criticality of the ESS needs to be undertaken for all fire and gas and protective applications that have not been screened out. This can be undertaken as follows:

a) Applying an effective process to identify and evaluate the hazardous events on the installation.

b) Designing the ESS in line with good industry practice and the requirements and guidelines contained in ISO 13702 to fulfil the role defined in the FES. With this approach fire and gas hazards are actively considered in the hazard management consideration of the overall plant design and layout.

c) Assessing the overall risk and determining whether there are any further risk reduction measures which should be evaluated and applied. In general, alternative measures to the ESS are the most effective means of achieving the necessary safety risk reduction. The hazards together with all methods of risk reduction, both passive and active, should be considered,

d) Establishing the performance required, if the most effective method of risk reduction is to include fire and gas detection systems. Under this approach, a few fire and gas detection functions with higher integrity

© ISO 2015 – All rights reserved

may provide the most cost-effective means of achieving the necessary risk reduction in certain applications. These are the exceptions where fire and gas and related ESD functions require a specified performance within the range of the safety integrity levels defined in IEC 61511-1. Such requirements can arise if hazard studies indicate the presence of a specific major hazard where fire and gas or related ESD functions should reduce the risk significantly. An example of a "safety-critical" fire and gas and related ESD function is the protection of the air supply ducts to the temporary refuge,

e) Implementing and operating the various functions within the ESS to achieve the appropriate integrity levels.

A.2.4.3 Determining the integrity for asset protection

On some installations (e.g. small unattended installations which are infrequently visited), and for some areas of all installations (e.g. under gas turbine hoods), it may be possible to conclude that the fire and gas detection system's main function is asset protection rather than safety. For these applications, it is likely to be sufficient to design the fire and gas detection systems in accordance with recognized practice, adopting the principles within ISO 9001[2].

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. These should be locations where the gas will be diluted with air to below the LFL so it is not a threat to the facility, or where it can safely be burned.

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 depressurization, 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 parallel to the vent valve to ensure that any failure of the valve or associated instrumentation does not lead to a problem.

A.3.2 Description

These systems originate at the normal gas exit or pressure-relief device of a process component, and terminate at the designated safe locations. They can vary from an exit nipple on an individual PSV or control valve to a piping network connected to the outlet of several valves. If gas is discharged from a pressure vessel to flare or vent, a scrubbing vessel should be provided to remove liquid hydrocarbons.

A.3.3 Discharge point

The final discharge point for atmospheric gas may be through a vertical, cantilevered, or underwater pipe. In some cases the discharge point may be remote from the platform. The following should be considered in selecting a safe discharge point:

a) personnel safety;

b) the discharge volume;

c) the location in relation to other equipment, particularly fired vessels or other ignition sources, personnel quarters, fresh air intake systems, and helicopter and boat approaches;

d) prevailing wind direction and, in the case of underwater discharges, the prevailing current.

A.3.4 Design considerations

Atmospheric gas discharge systems should be designed in accordance with API RP 520 Part II[12] and API RP 521[13], API Std 2000[14], and Section VIII of the ASME *Boiler and pressure vessel code*[18] or other

© ISO 2015 – All rights reserved

national or internationally recognized pressure vessel codes. Systems should be designed so that back pressure, including inertial forces developed at maximum instantaneous flow conditions, will not exceed the working pressure of the lowest pressure rated item. Flame arrestors can be used in vent systems to reduce the danger of combustion within the component from an external source. A flare scrubber should be a pressure vessel designed to handle maximum anticipated flow. During blowdown calculations, consideration should be given to hydrate potential, flare capacity and flare radiation.

© ISO 2015 – All rights reserved

Annex B
(informative)

Toxic gases

B.1 General

This annex provides guidelines and methods of handling sour production (e.g. production containing hydrogen sulfide) on offshore platforms. This annex includes discussion of general criteria, toxic gas detectors, and atmospheric discharging systems. These are essential systems and procedures that provide a minimum acceptable level of protection to the facility and personnel by initiating shut-in functions or reacting to minimize the consequences of released toxic gases. In addition to the following recommendations, API RP 55[11] should be consulted.

Production of liquid and gaseous hydrocarbons containing hydrogen sulfide (H_2S) in significant amounts can be hazardous to personnel and can cause failure of equipment. The presence of H_2S also presents the possibility of exposure to sulfur dioxide (SO_2) that is produced from the combustion of H_2S. H_2S gas detectors or an alternative detection system should be installed on offshore facilities wherever the processing and handling of gases and/or liquids has the potential for creating atmospheres containing H_2S in concentrations exceeding 50×10^{-6}, particularly in enclosed or inadequately ventilated areas. The aim should be to detect releases that present a toxicity threat to personnel. SO_2 monitoring equipment should be utilized when flaring operations could result in personnel exposure to atmospheric concentrations of SO_2 of 2 ml/m^3 or greater. SO_2 monitoring equipment should indicate when concentrations reach a level of 2 ml/m^3. Hydrocarbon detectors can be used to indicate toxic gas levels when the set point for the gas detection system will respond before the exposure level for the toxic gas has been exceeded. If the toxic gas hazard requires action before the flammable gas level is reached, then dedicated toxic gas detection is required.

The occupational exposure limit for SO_2 is considerably lower than for H_2S, but the lethal concentration of H_2S is considerably lower than for SO_2, as indicated in the following table.

Table B.1 — Assessment criteria for sulfur dioxide and hydrogen sulfide exposure

Gas	Averaging period	Occupational exposure limit mg·m^{-3}	World Health Organization (1997) µg·m^{-3}	Fatal level $\times 10^{-6}$
SO_2	10 min		500	
	24 h		125	
	Threshold limit value (time-weighted average)	10		
	Threshold limit value (short-term exposure level)			
	LC_{50} [a]			4 673
H_2S	24 h		150	
	Threshold limit value (time-weighted average)	14		
	Threshold limit value (short-term exposure level 10 min)	21		
	LC_{50} [a]			1 817
	Industry practice [b]			700

[a] LC_{50} is the lethal concentration with 50 % fatalities after 5 min exposure.

[b] Industry practice is to recognize that the fatality from H_2S exposure can occur over a wide band but at a level of around 500 ml/m^3 to 1 000 ml/m^3 exposure for a short period, the fatal exposure levels would be significant.

Accumulations of toxic gases or vapours are more likely to occur in enclosed and poorly ventilated areas containing a source of H_2S. Methods for increasing safety and minimizing personnel exposure include improving ventilation and installing OSH systems. OSH systems should alert personnel by unique audible and

© ISO 2015 – All rights reserved

visual alarms, as appropriate for the area or zone where low-level concentrations of toxic gases have been detected. These systems may also initiate executive actions to increase ventilation and shut off the gas source. In exploration and production operations, toxic gases are normally encountered as constituents of hydrocarbon gases and vapours which are flammable. Therefore, combustible gas detectors (ASHs) should be installed to prevent concentrations from reaching the LFL of the gas present. Ignition sources should be eliminated and electrical installations should be made in accordance with API RP 14F[9].

Strict controls should be used when exposing materials to an environment containing hydrogen sulfide. Many materials may suddenly fail by a form of embrittlement known as sulfide stress-cracking (SSC) that increases as strength and tensile stress (residual or applied) increase. Material hardness is frequently used as an indirect measurement of strength and sometimes is referenced as a limiting parameter. The failure of certain producing and gas processing components used in the SSC regime could allow the uncontrolled release of H_2S to the atmosphere. Guidelines for equipment and materials selection on the basis of resistance to SSC sulfide stress cracking and corrosion is provided by ISO 15156-1[5], ISO 15156-2[6] and ISO 15156-3[7].

The safety integrity level for toxic gas detection systems should be determined following the approach described in A.2.4.

B.2 Installation, operation, and testing of fixed detection systems

Decisions on the installation of fixed hydrogen sulfide detectors and their placement involve consideration of many variables, including concentration of toxic gas in process streams, specific gravity of the gas mixture, process pressure, atmospheric conditions, ventilation, equipment location, type of decking (solid or grated), and direction of prevailing winds. A detailed design analysis that might include dispersion modelling should be performed to determine the need for and placement of detector systems.

Within a specific facility, the potential for H_2S to be present in the atmosphere varies from location to location. Areas within the facility may be categorized according to their H_2S risk as follows.

a) **Category 0**: Areas where H_2S in the atmosphere is encountered during normal operations and which cannot be made H_2S free, e.g. within legs and storage cells of gravity-base structures.

   Entry to and work in such areas requires the use of breathing apparatus at all times. Since toxic gas is always likely to be present, installation of a fixed detection/monitoring system is not required from a safety viewpoint.

b) **Category 1**: Areas in which H_2S may be encountered during normal operations but which can be made safe for working by applying specific laid down procedures, e.g. utility legs of some gravity-base structures.

   Entry to such areas should only be allowed with portable toxic gas monitoring equipment. Breathing apparatus should be worn on first entering the area until confirmation is obtained that the H_2S concentration in the atmosphere is below the OEL. Fixed detection systems are recommended for these areas to maintain a H_2S risk history but should not be used for making safety-related decisions.

c) **Category 2**: Areas which are free of H_2S in the atmosphere during normal operations but which may be contaminated by a leak, system malfunction or opening up pipework or equipment.

   These areas should have fixed detection linked to an alarm system providing alarm indications both in the facility control-room and at the affected workplace. The detection system sensors may be flammable-gas or H_2S detectors depending on the concentration of H_2S in the process streams,

If H_2S concentrations in the process stream are known to be less than 500×10^{-6} ml/m^3 (in the equilibrium gas phase after flashing to atmospheric pressure), fixed flammable-gas detection can be used to indicate a potential toxic gas hazard and initiate the appropriate response. Flammable-gas detectors are normally set to alarm at 20 % methane LFL (i.e. 1 % methane in air). If a hydrocarbon gas containing 500×10^{-6} ml/m^3 of H_2S is diluted to 1 % in air, the corresponding H_2S concentration in the atmosphere will be 5×10^{-6} ml/m^3. Therefore, the flammable-gas detector will signal alarm before the H_2S concentration in the atmosphere

© ISO 2015 – All rights reserved

reaches the OEL. However, the area coverage should be sufficient, including detectors sited at low level to cater for heavy vapours, if appropriate.

Detector selection should take into account the cross-sensitivity of detectors to different gas compositions and the risk of poisoning of some types of detector due to the presence of the H_2S.

For H_2S concentrations in the production streams exceeding 500×10^{-6} ml/m^3 (in the equilibrium gas phase after flashing to atmospheric pressure), fixed H_2S detectors should be installed.

Placement of fixed detectors should generally follow the same philosophy as for flammable gas detectors, i.e. located at points where gas could potentially accumulate or migrate. Detectors should therefore be placed along the logical access routes to the area concerned, and at other places within the area where gas might accumulate. Due account should be taken of prevailing wind directions when selecting locations for the detectors. If a design analysis has identified specific potential leak sources, consideration should be given to also locating detectors close to (within 0,8 m) these points for an even faster response to leaks.

Although H_2S itself is slightly heavier than air, for most exploration and production facilities the concentrations present in process streams will not dissociate from the hydrocarbon gases and form a separate gas phase. Fixed area-monitoring detectors should therefore be sited not lower than 1,2 m above deck level, where they more closely monitor concentrations in the breathing zone and are less susceptible to mechanical damage or being splashed by liquids. Placement at lower level should only be considered if there is the potential for leaks or accumulation of heavy vapours, such as from flashing NGLs. Due consideration should be given to adequate access for calibration and testing of the detectors.

It is recommended that H_2S detection instruments be approved by an NRTL and meet ISA S 92.0.02, *Part I* [15]. Furthermore, it is recommended that H_2S detection systems be installed, operated, and maintained in accordance with ISA RP 92.0.02, *Part II* [16].

Detection of 10×10^{-6} ml/m^3 of H_2S gas in the atmosphere should initiate audible and visual alarms in the area where the gas has been detected, any adjacent areas where personnel may need to take executive action on detection of H_2S and the facility's control room. A visual warning system should also be provided at locations at which such that personnel in approaching helicopters or boats can be effectively warned of the release of toxic gas. When concentrations in the atmosphere around the landing area exceed 10×10^{-6} ml/m^3, H_2S warning alarms should be readily distinguishable from other alarms at the location.

Detection of 15×10^{-6} ml/m^3 of H_2S gas in the atmosphere should initiate an audible general platform alarm and a visual alarm, as most appropriate for the area where in which the gas has been detected. Signs and flags should be displayed if the concentration of gas exceeds 15×10^{-6} ml/m^3 around the landing areas for boats and helicopters, or if personnel arriving by boat or helicopter would not have access to safe briefing areas. Normally, automatic executive shutdown actions should not be initiated by H_2S detection, since this will be taken care of by the flammable-gas protection system. However, in specific circumstances, there may be a case for taking direct executive actions, such as:

— valved isolation of the sour production handling equipment, applicable wells, and pipelines/flowlines;

— blowdown of certain process equipment;

— providing (or increasing) ventilation in enclosed modules;

— closure of ventilation intakes to accommodation/control modules, to prevent H_2S ingress.

Careful consideration should be given to the form of automatic corrective action taken to ensure that the situation is not made more hazardous.

Any shutdown devices controlled by H_2S gas detection systems should be installed “normally energized” (commonly referred to as “failsafe”). See API RP 14F[9], Section 9, “Special Systems”.

© ISO 2015 – All rights reserved

In addition to being toxic, H_2S gas is combustible. The range of concentration for combustibility is approximately 4,3 % to 45,5 % (volume fraction). Areas subject to combustible levels of H_2S should be classified as Group C and electrical equipment should be suitable for atmospheres of Groups C and D. For mixtures of H_2S and natural gas, the mixture should be considered Group D if the H_2S constitutes less than 25 % (volume fraction) of the mixture and Groups C and D if greater than 25 %. If machinery or equipment shutdown can create an ignition source, consideration should be given to actuation of a fire-inerting system prior to shutdown.

If sour gas is sweetened to reduce the hazard of personnel exposure or for equipment protection, the sweetened gas should be continuously monitored for H_2S prior to the gas leaving the facility, and preferably before being utilized for fuel or control gas at the facility. Devices specifically designed for analysing an instream sample for H_2S content on a continuous basis should be utilized.

To better ensure proper application of H_2S -detection instruments, it is recommended that an environment and application checklist (similar to the example shown in Annex A, ISA RP 92.0.02, *Part II* [16]) be provided to prospective suppliers by the user.

B.3 Systems for discharging H_2S and SO_2 to atmosphere

Discharge of pressure-relief and normally venting devices should be located away from work areas and designed to provide adequate dispersion and to limit personnel exposure to H_2S and SO_2 concentrations not exceeding those discussed in API RP 55[11], Annexes A and B. If dispersion modelling determines that ignition of vented gas is required, the flare outlets should be equipped with an automatic ignition system and contain a pilot(s) or other means to ensure combustion. On platforms where flaring is required, failure of the automatic ignition system and loss of flare should shut in the input source.

© ISO 2015 – All rights reserved

Bibliography

[1] ISO 3511 (all parts), *Process measurement control functions and instrumentation — Symbolic representation*

[2] ISO 9001, *Quality management systems — Requirements*

[3] ISO 10417, *Petroleum and natural gas industries — Subsurface safety valve systems — Design, installation, operation and redress*

[4] ISO 14001, *Environmental management systems — Specification with guidance for use*

[5] ISO 15156-1, *Petroleum and natural gas industries — Materials for use in H_2S-containing environments in oil and gas production — Part 1: General principles for selection of cracking-resistant materials*

[6] ISO 15156-2:, *Petroleum and natural gas industries — Materials for use in H_2S-containing environments in oil and gas production — Part 2: Cracking-resistant carbon and low alloy steels and cast irons*

[7] ISO 15156-3, *Petroleum and natural gas industries — Materials for use in H_2S-containing environments in oil and gas production — Part 3: Cracking-resistant CRAs (corrosion-resistant alloys) and other alloys*

[8] API RP 14C, *Analysis, design, installation and testing of basic surface safety systems on offshore production platforms*

[9] API RP 14F, *Design and installation of electrical systems for fixed and floating offshore petroleum facilities for unclassified and class I, division 1, and division 2 locations*

[10] API RP 14H, *Installation, maintenance and repair of surface safety valves and underwater safety valves offshore*

[11] API RP 55, *Conducting oil and gas producing and gas processing plant operation involving hydrogen sulfide*

[12] API RP 520, Part II, *Sizing, selection, and installation of pressure-relieving devices in refineries, Part II — Installation*

[13] API RP 521, *Guide for pressure-relieving and depressuring systems*

[14] API Std 2000, *Venting atmospheric and low-pressure storage tanks: Nonrefrigerated and refrigerated*

[15] ISA S 92.0.02, *Part I, Performance requirements for toxic gas-detection instruments: Hydrogen sulfide*

[16] ISA RP 92.0.02, *Part II, Installation, operation, and maintenance of toxic gas detection instruments: Hydrogen sulfide*

[17] ISA S.5.1, *Instrumentation symbols and identification*

[18] ASME, *Boiler and pressure vessel code, section VIII*

[19] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

© ISO 2015 – All rights reserved

[20] ISA-TR 84.07-2010, *Guidance on the evaluation of fire and combustible gas and toxic gas system effectiveness*

© ISO 2015 – All rights reserved