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 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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**

© ISO 2019 – 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.

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.

© ISO 2019 – All rights reserved

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.

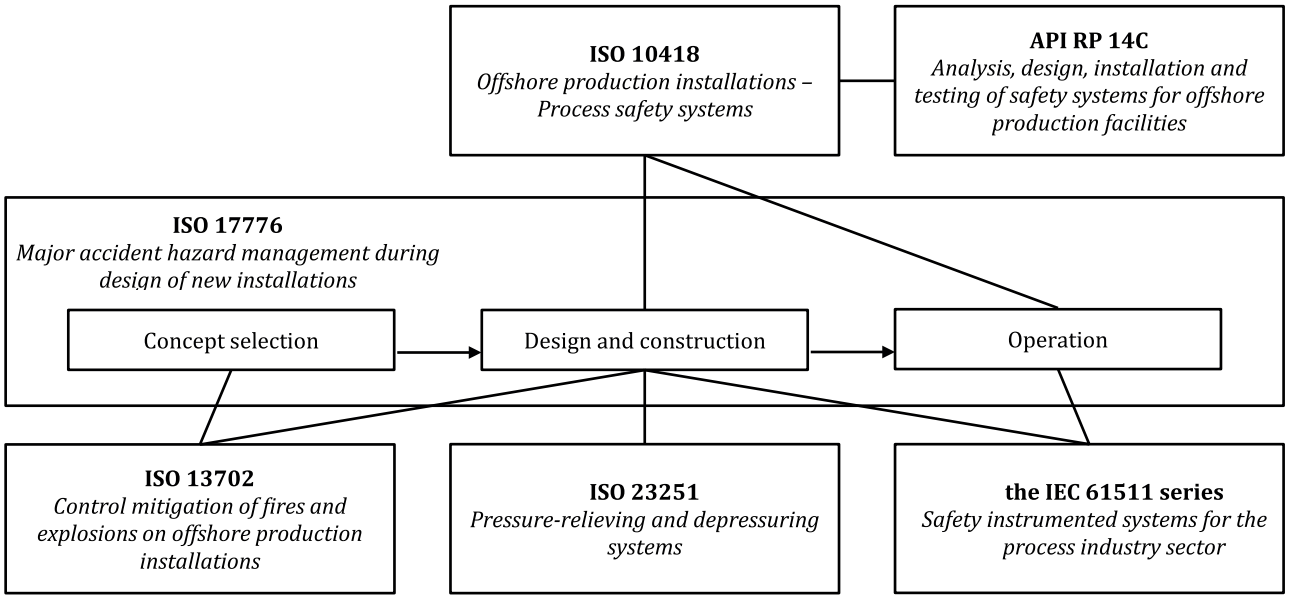
This document sets out three options for identifying appropriate process safety systems. The first option is to adopt the prescriptive approach specified in API RP 14C. The second approach is to use structured review techniques to identify hazards and evaluate risk, with process safety systems being 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.

© ISO 2019 – All rights reserved



NOTE The lines between the standards illustrate the main relationships.

Figure 1 — Relationship between offshore-relevant standards

© ISO 2019 – All rights reserved

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/

© ISO 2019 – All rights reserved

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]

© ISO 2019 – All rights reserved

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.

© ISO 2019 – All rights reserved

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

© ISO 2019 – All rights reserved

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.

© ISO 2019 – All rights reserved