INTERNATIONAL STANDARD

ISO 10418

Second edition
2003-10-01

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

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

Reference number
ISO 10418:2003(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

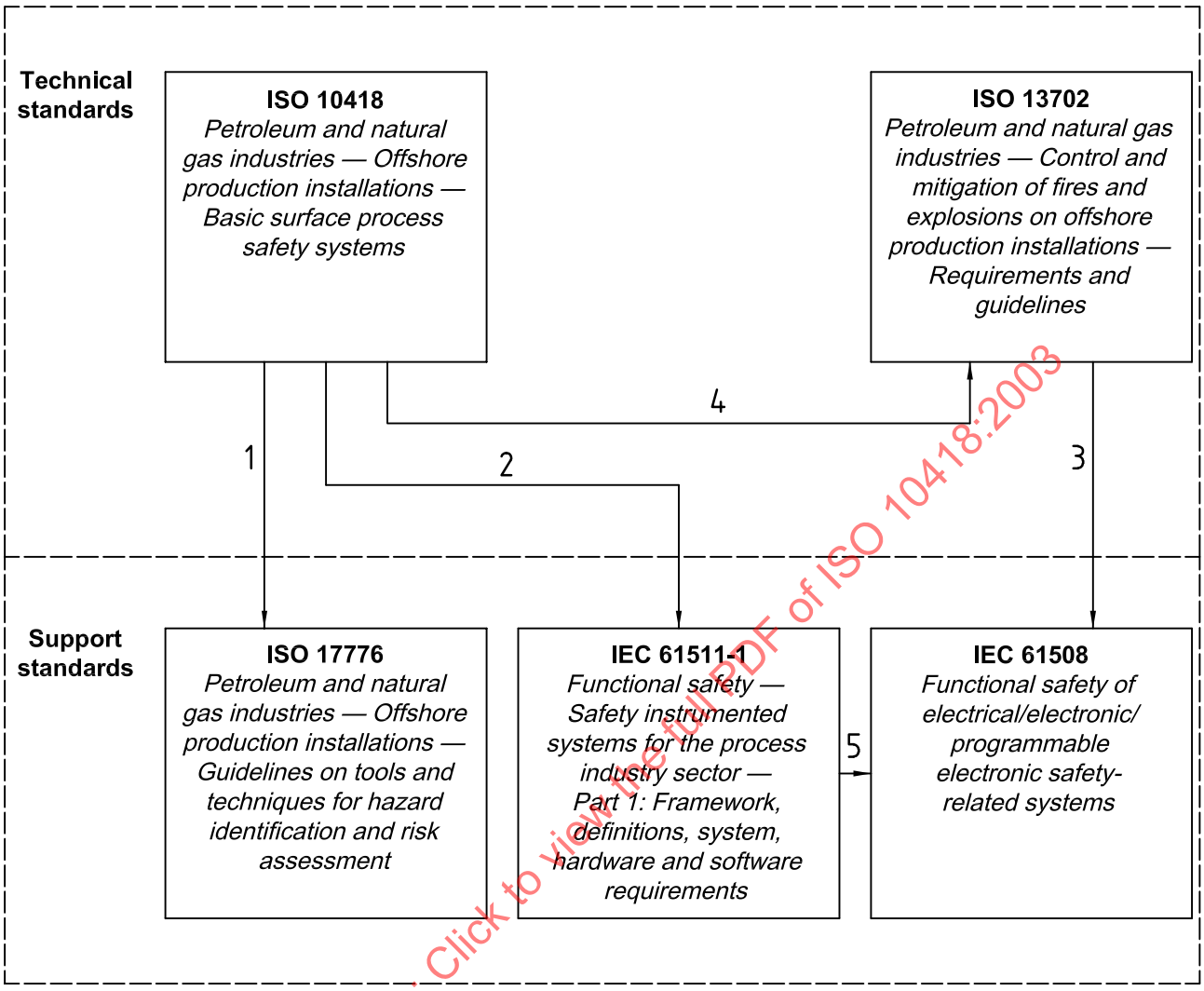
Particular requirements for the control and mitigation of fires and explosions on offshore installations are given in ISO 13702. General requirements for fire and gas and emergency shutdown (ESD) systems are also included in ISO 13702.

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

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

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

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



Key

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

Figure 1 — Relationship between offshore-relevant standards

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

1 Scope

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

This International Standard is applicable to

— fixed offshore structures;

— floating production, storage and off-take systems;

for the petroleum and natural gas industries.

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 13702:1999, *Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines*

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

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

3 Terms, definitions and abbreviated terms

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

3.1 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1.22
hazardous event
incident which occurs when a hazard is realised

EXAMPLES Release of gas, fire, gas blowby.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXAMPLES Separator, heater, pump, tank.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXAMPLES Overpressure, underpressure, liquid overflow.

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

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

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

3.2 Abbreviated terms

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

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)
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.

The unique identifier (tag) shall consist of alphanumeric identifiers (i.e. AAAA, NNN). Letters shall identify the function, while numbers shall uniquely identify multiple devices with the same function (e.g. PSHH 005 means number 5 of pressure safety high, high sensor).

A number of graphical symbols are available depending on the contractors and CAD systems used. The same standard shall be used at least within one development project and for operation within one offshore installation. Graphical symbols used in this International Standard are shown in Annex A.

Table 1 gives a list of preferred alpha-identifiers for safety devices.

Table 1 — Safety device identifiers

Variable	Sensing and self-acting devices		
	Safety device designation		Identifier
	Common name	Process safety function	
Backflow	Check valve	Flow safety valve	FSV
Burner flame	Burner flame detector	Burner safety low	BSL
Flow	High flow sensor	Flow safety high	FSH
	Low flow sensor	Flow safety low	FSL
Level	High level sensor	Level safety high	LSH
	Low level sensor	Level safety low	LSL
Pressure	High pressure sensor	Pressure safety high	PSH
	High/low pressure sensor	Pressure safety high low	PSHL
	Low pressure sensor	Pressure safety low	PSL
	Pressure relief/safety valve	Pressure safety valve	PSV
	Rupture disc/safety head	Pressure safety element	PSE
Pressure or vacuum	Pressure/vacuum relief valve	Pressure safety valve	PSV
	Pressure/vacuum relief manhole cover	Pressure safety valve	PSV
	Vent	None	
Vacuum	Vacuum relief valve	Pressure safety valve	PSV
	Rupture disc or safety head	Pressure safety element	PSE
Temperature	Temperature fire detector	Temperature safety element	TSE
	High temperature sensor	Temperature safety high	TSH
	Low temperature sensor	Temperature safety low	TSL
	High/low temperature sensor	Temperature safety high low	TSHL
	Fire relief valve	Temperature safety valve	TSV

Actuated valves	
Service	**Safety identifier**
Wellhead surface safety valve	SSV
Underwater safety valve	USV
Blowdown valve	BDV
All other shutdown valves	SDV

5 Safety analysis concepts

5.1 Objectives

The purpose of safety analysis concepts is

— 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 for a process composed of components and systems normally used offshore,

— to establish guidelines for analysing components or systems that are new or significantly different from those covered in this International Standard,

— 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 verify the protection arrangements provided to detect, prevent, mitigate or control undesirable events which may develop in a process component under worst-case conditions.

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 component,

— 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

— the approach using tables, checklists and functional evaluation charts as described in 5.3 or

— the approach involving the use of structured review techniques as described in 5.4.

In many instances there are benefits in using a combination of the above techniques. In particular the following should be considered:

a) If process components are used that are not included in the basic list in Annex B, or if process components are used in a novel way, then use of the structured techniques as described in 5.4 should be considered;

b) If analysis techniques as described in 5.3 have been used, then elimination of some primary or secondary protection devices may be considered if analysis using the techniques in 5.4 confirms adequate levels of safety.

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

— the analysis approach which has been traditionally used for facilities in that location;

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

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

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

5.3 Functional requirements for analysis using tables, checklists and functional evaluation charts

5.3.1 Analysis and design procedure

5.3.1.1 The analysis and design of a platform surface safety system shall include the following steps.

a) Describe the process by a detailed flow schematic and establish the operating parameters. The flow schematic and operating parameters shall be developed based on equipment design and process requirements.

b) The overall design should be divided into basic process components that can be analysed on a systematic basis as described in B.2. B.3 includes an analysis of a number of common basic process components. If a process component significantly different from those covered in B.3 is used in a process, a SAT and SAC table shall be developed for that component using the principles described in B.2 or as described in 5.3.1.3.

c) Using SATs, verify the need for basic safety devices to protect each process component viewed as an individual unit. SACs for individual components are then used to justify the elimination of any safety device when each process component is analysed in relation to other process components. The SAC lists specific conditions under which some safety devices may be eliminated when larger segments of the process are considered.

d) Using the SAFE chart, logically integrate all safety devices and self-protected equipment into a complete platform safety system. List on the SAFE chart all process components and their required safety devices. Enter the functions that the devices perform, and relate each device to its function by checking the appropriate box in the chart matrix.

e) If designing a new facility, show all devices to be installed on the process flow schematic.

f) If analysing an existing facility, compare the SAFE chart with the process flow schematic and add the devices required but not shown.

5.3.1.2 The analyses should define the monitoring devices (sensors) and self-actuating safety devices needed for a process facility. They should also establish the safety function required to return the process to a safe state (shutdown, diverting the input, pressure relief, etc.).

5.3.1.3 The use of proven systems analysis techniques, adapted to the production process, will determine the minimum protection requirements for a process component. If such analysis is applied to the component as an independent unit, assuming worst-case conditions of input and output, the analysis will be valid for that component in any process configuration. Appropriate analysis techniques are described in ISO 17776.

5.3.2 Safety analysis table (SAT)

5.3.2.1 SATs shall be completed for each process component which forms part of the design.

5.3.2.2 For each identified undesirable event, the SATs shall address

— the cause,

— the detectable abnormal condition.

5.3.2.3 The SATs are applicable to a component regardless of its position in the process flow. The boundaries of each process component include the inlet piping, control devices, and the outlet piping to another component. Every outlet pipe and pipe branch shall be included up to the point where safety devices on the next component provide protection.

NOTE SATs for the basic process components of a platform production facility are presented in Annex B.

5.3.2.4 The safety analysis of each process component highlights undesirable events (effects of equipment failures, process upsets, accidents, etc.) from which protection shall be provided, along with detectable abnormal conditions that can be monitored for safety surveillance. These detectable conditions are used to initiate action through manual or automatic controls to prevent or minimize the effect of undesirable events. The tables present the logical sequence of safety system development, including undesirable events that could be created in downstream process components because of failures in the equipment or safety devices of the component under consideration.

5.3.2.5 The generic causes of each undesirable event shall be listed. The primary causes are equipment failures, process upsets, operator error and accidents, but all primary causes in a category will create the same undesirable event. Thus, a blocked line could be due to plugging, freezing, or other failure of a control

valve, or the inadvertent closing of a manual valve. The undesirable events shall be determined from a detailed investigation of the failure modes of the component and its ancillary equipment. These failure modes are grouped under causes, according to the manner in which they can generate the undesirable event.

5.3.3 Safety analysis checklist (SAC)

5.3.3.1 SACs shall be completed for each process component which forms part of the process design.

NOTE SACs for basic process components are presented in Annex B.

5.3.3.2 The SAC lists the safety devices that would be required to protect each process component if it were viewed as an individual unit with the worst probable input and output conditions. Listed under each recommended device are certain conditions that eliminate the need for that particular device when the component is viewed in relation to other process components. This action is justified because safety devices on other components will provide the same protection, or because in a specific configuration, the abnormal condition that the device detects will not lead to a risk to safety.

5.3.4 Safety analysis function evaluation (SAFE) chart

5.3.4.1 A SAFE chart shall be completed relating all sensing devices, SDVs, shutdown devices, and emergency support systems to their functions. The SAFE chart shall list all process components and emergency support systems with their required safety devices, and shall list the functions to be performed by each device.

5.3.4.2 If the device is not needed, the reason shall be listed on the SAFE chart by referring to the appropriate SAC item number. If the reason for eliminating a device is that a device on another component provides equivalent protection, this alternative device should also be shown on the SAFE chart. The relation of each safety device with its required function can be documented by checking the appropriate box in the chart matrix. If a safety device on a process component is omitted for reasons not covered in the SAC, a notation describing the reason for omitting the safety device should be included on the SAFE chart. Completion of the SAFE chart provides a means of verifying the design logic of the basic safety system.

NOTE A typical SAFE chart is shown in Figure C.1. Examples of use are shown in Annex C.

5.4 Functional requirements for analysis using structured review techniques

5.4.1 A risk management process shall be applied for the identification of hazards and the assessment and control of risks. Guidance on risk management is contained in Clause 5 of ISO 17776:2000.

5.4.2 The structured review techniques used for hazard identification and risk assessment shall be selected to 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.

5.4.3 A strategy for managing process hazards for the particular process plant shall be developed. The following elements shall be included or referenced in the strategy:

— process control and shutdown philosophy;

— ESD plant segregation philosophy;

— ESD philosophy;

— relief and blowdown philosophy;

— flare and vent philosophy.

5.4.4 The strategy should be developed for the hazards identified by the techniques outlined in ISO 17776.

5.4.5 The emergency shutdown philosophy should include a description of the hierarchy of shutdown systems on the installation.

5.4.6 A systematic study should be made of all the HP/LP interfaces in the process plant. The study should assess the adequacy of the protection systems for overpressure, underpressure and liquid overfill for the plant downstream of each HP/LP interface, and should consider

— overpressure sources,

— relief capacity requirement and the design relief case,

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

— design information on the PSVs to demonstrate that they will work effectively in particular overpressure scenarios,

— adequacy of the relief capacity,

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

— the executive action of the instrumented protection devices to enable judgement on whether they will be effective in preventing overpressure in particular scenarios.

5.4.7 The operation of the process safety system should be checked for operability during normal plant start-up and normal plant shutdown conditions. The use of inherently safer designs as discussed in Clause 5 of ISO 17776:2000 will help to reduce the risks from plant and equipment.

5.4.8 The operation of the process safeguarding system should be confirmed by

— the SIL of each shutdown loop,

— the inhibits and bypasses required by the system,

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

NOTE 1 Inhibits and bypasses prevent an automatic action, on a temporary basis, to allow continued operation.

NOTE 2 Annex E provides guidelines on bypassing.

6 Process safety system design

6.1 Objectives

The goal of process safety system design is

— 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 if it occurs,

— to prevent ignition of released hydrocarbons,

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

— to prevent undesirable events that could cause the release of hydrocarbons from equipment other than that in which the event occurs.

6.2 Functional requirements

6.2.1 The design basis for the protection system provided 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 should be valid in the process configuration.

6.2.2 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.

6.2.3 Protection measures shall be provided to

— isolate if necessary a part of the process 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.

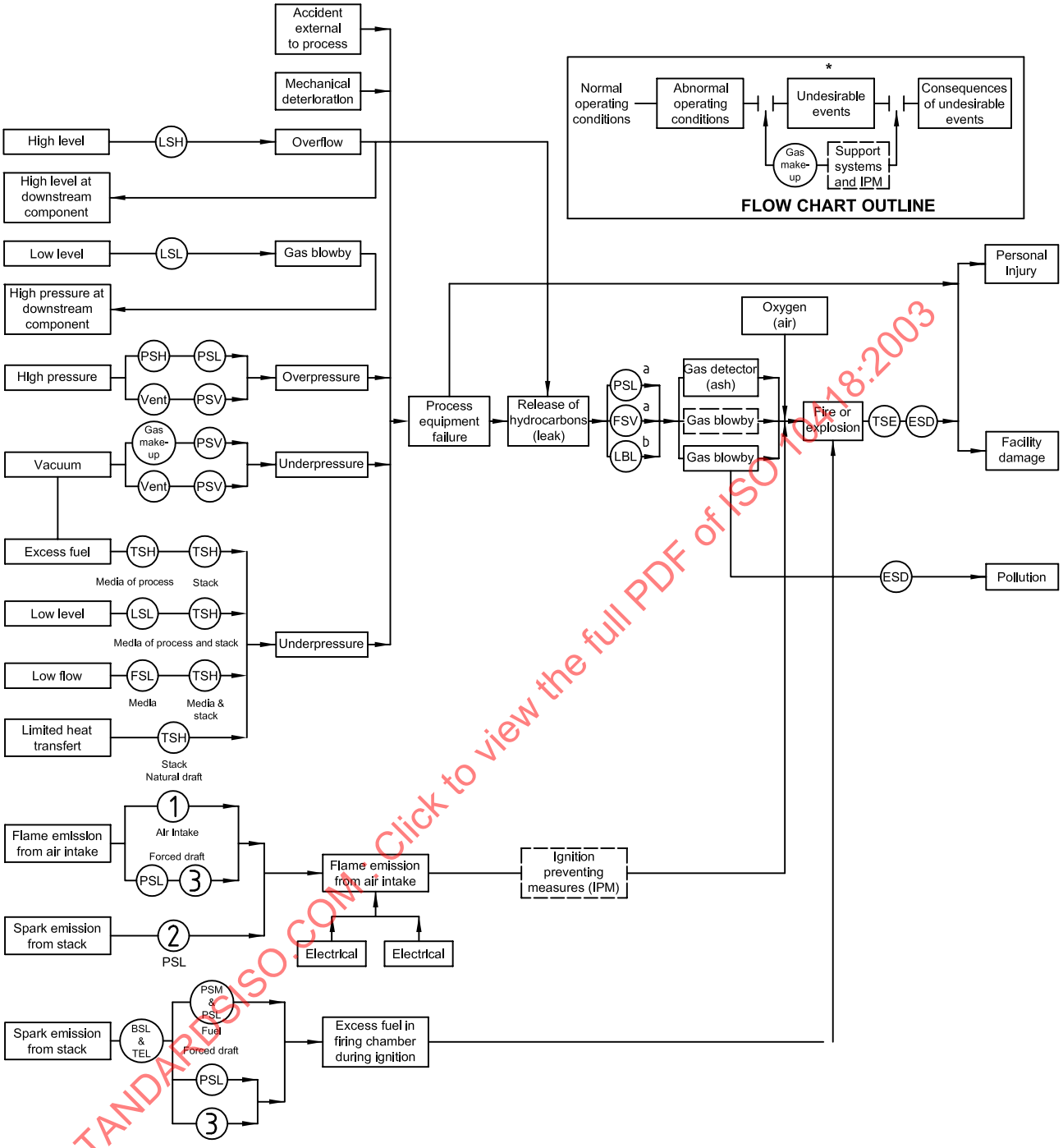
6.2.4 These analysis techniques shall be applied to all process components, from wellhead to the most downstream discharge point.

6.2.5 The safety system provided shall be independent, such that a 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 Abnormal operating conditions which may lead to an undesirable event shall be detected by the provision of sensors monitoring one or more process variable, or self-actuating devices.

6.2.7 Accidents that occur external to the process on a production platform are not self-propagating unless they affect the process or start a fire. If they affect the process, the safety system shall shut down the process or affected part of the process. If they result in fire, the safety system shall shut down all platform activity in the affected area except that which is necessary for fire fighting and other emergency operations.

NOTE Such accidents can be caused by natural phenomena, ship or helicopter collision, failure of tools and machinery, or mistakes by personnel. These types of accidents 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. Figure 2 indicates the manner in which external accidents can affect the process.



Key

1 air intake flame arrestor
2 stack spark arrestor
3 motor starter interlock

a For pressure components.
b For atmospheric components.

Figure 2 — Safety flow chart — Offshore production facility

6.2.8 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.

6.2.9 The safety system shall normally provide two levels of protection to prevent or minimize the consequences of an equipment failure within the process. The two levels of protection shall be independent of, and in addition to, the control devices used in normal process operation. In general, the two levels should be provided by functionally different types of device.

NOTE. Similar devices would have the same characteristics and might have the same mode of failure.

6.2.10 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 should be given to the following:

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

— the value should 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.

6.2.11 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.

6.2.12 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 to achieve the necessary safety integrity level in accordance with IEC 61511-1.

NOTE 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.

6.2.13 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 D.

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

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 logically integrated into a process safety system, the entire facility is protected.

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

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

It is not advisable to close the process inlet to a component if this could create an abnormal condition in the upstream component, causing its safety devices to shut it in. This would be repeated for each component back through the process until the primary source is shut in. Each component would therefore be subjected to abnormal conditions and must be protected by its safety devices every time a downstream component shuts in. This cascading effect depends on the operation of several additional safety devices, may place undue stress on the equipment and should be avoided if practicable.

There may be special cases where shut-in by cascading as described above is acceptable. Examples of where shut-in by cascading would be acceptable are as follows.

EXAMPLE 1 The source of input to a separator is frequently changed as wells are periodically switched into the separator. If the well(s) producing to the separator is to be directly shut in when an abnormal condition is detected, the safety system logic must be changed each time different wells are switched into the unit. This creates the possibility of oversight in changing the logic. In this case, it may be preferable to close the separator inlet, and let the resulting high flowline pressure cause the well(s) to shut in by action of the flowline PSH sensor. The header and the flowline should be rated for the maximum pressure that could be caused by this action.

EXAMPLE 2 A platform receives production through a flowline from a satellite well. Although the source of energy to the system is the satellite well, detection of an abnormal condition on the platform should cause activation of an SDV on the incoming flowline. If it is desired to shut in the satellite well following closure of the flowline SDV at the platform, this may be accomplished by use of a flowline PSH sensor installed at the satellite location.

EXAMPLE 3 A compressor installation is equipped with an automatic divert valve that permits production to be maintained from wells capable of producing against pipeline pressure when a compressor shutdown occurs. In this case, wells incapable of producing against pipeline pressure may be shut in by action of the individual flowline PSH sensors to minimize potential safety system logic problems.

6.2.17 It may be desirable to shut in the inlet to a process component for additional protection or to prevent upstream components from equalizing pressure or liquid levels after the primary source is shut in. If this is desirable, the primary source of energy should be shut in simultaneously with or prior to closing of the component inlet valve.

6.2.18 Ignition preventing measures shall be in accordance with ISO 13702:1999, Annex B.

6.2.19 Ventilation shall be in accordance with ISO 13702:1999, Annex B.

6.2.20 Protection from ignition by electrical sources shall be in accordance with ISO 13702:1999, Annex B.

6.2.21 Equipment shall be located in accordance with ISO 13702.

6.2.22 Hot-surface protection shall be in accordance with ISO 13702.

6.2.23 Hot-equipment shielding shall be in accordance with ISO 13702.

6.2.24 The ESS (see Annex D) shall minimize the effects of escaped hydrocarbons and high pressure 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;

NOTE Annex E provides guidelines on annunciation of alarms.

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

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

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

d) a fire loop system to sense the heat of a fire and initiate platform shutdown;

e) other fire detection devices (flame, thermal, and smoke) that are used to enhance fire detection capability;

f) an ESS to provide a method to manually initiate platform shutdown by personnel observing abnormal conditions or undesirable events;

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

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

6.2.25 The ESS should 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 D.

6.2.26 The integrity of a platform surface safety 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 should be equally well maintained. Those discussed or referenced in Annex D are the pneumatic and hydraulic supply systems 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.

NOTE 1 ISO 13702 is referenced for requirements for these systems.

NOTE 2 D.5 provides further guidance on discharging gas to atmosphere.

6.2.27 SSSVs should be installed below the mudline to prevent uncontrolled well flow in the event of an emergency situation. SSCSSVs should shut in if well rate exceeds a predetermined rate that might indicate a large leak. SCSSVs should 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].

6.2.28 The design shall include arrangements for controlling

— inhibits and bypasses on shutdown loops,

— resetting of tripped shutdown loops,

— testing of shutdown loops,

— control of change to shutdown loops and shutdown systems.

NOTE Annex G provides details of typical testing and reporting procedures.

6.3 Requirements when tables, checklists and function evaluation charts are used as the analysis method

6.3.1 In addition to the requirements of 6.2, the requirements of 6.3.2 to 6.3.4 shall apply.

6.3.2 The safety devices determined in the SAT, in conjunction with necessary SDVs or other final control devices, shall be installed to protect the process component in any process configuration.

It is important that the user understand the SAT logic and how the SATs are developed.

6.3.3 If design of the safety system is to be based solely on this International Standard, all safety devices listed in the SATs for each component should be considered and shall be installed unless conditions exist whereby the function normally performed by a safety device is not required or is performed adequately by another safety device(s).

NOTE 1 The SACs in Annex B list equivalent protection methods, thereby allowing the exclusion of some devices.

NOTE 2 There may be cases where alternative analysis techniques are used for some components which may result in a different approach to safety.

6.3.4 If a process component is used that is not covered in Annex B, a SAT for that component should be developed as discussed in Clause 5.

6.4 Requirements when tools and techniques for hazard identification and risk assessment have been selected from ISO 17776

6.4.1 Systems shall be installed to meet the functional and performance requirements as determined by the analysis techniques used.

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

— specifications and drawings;

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

— index of alarms and trips;

— index of PSVs.

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

Annex A
(informative)

Component identification and safety device symbols

A.1 General considerations

It is recommended that, in order to avoid misinterpretation during the design process and operation, that a clear indication of the “tagging” system to be used for all process and utility components, supported by a comprehensive table of symbols, should be declared.

Adoption of a consistent “tagging” system aids the development of the analysis and design of the basic process safety systems. The proposed method of illustrating process safety devices is based upon the ISA S 5.1[17].

The complete identification of a safety device comprises two parts as follows

— the functional device identification;

— a reference to the component it protects.

Details of the identification schemes for the two parts are given in A.2 to A.4.

A.2 Functional device identification

Each safety device should be identified by a system of letters and numbers which are used to classify the device in terms of the monitored process variable and its function within the safety system (e.g. PSV, LSH). If two or more devices of the same type are installed, the devices should be identified with unique numbers which form part of the device identification tag number (e.g. PSV-001, LSH-015). Table A.1 provides a non-exhaustive list of such safety device symbols.

Table A.1 — Safety device symbols

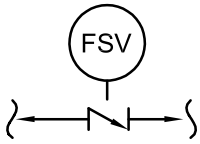
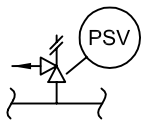
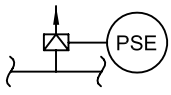
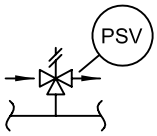
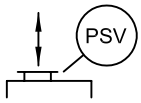
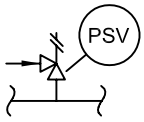
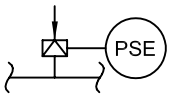
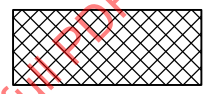
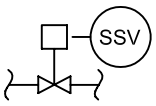
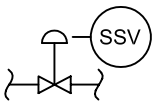
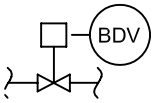
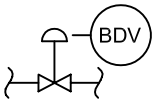
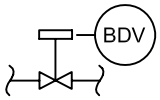
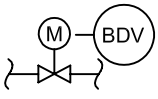
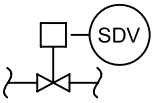
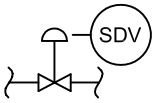
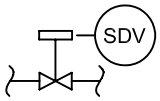
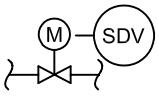
Variable	Sensing and self-actuating device			
	Safety device designation		Symbol	
	Common	Instrument Society of America (ISA)	Single device	Combination device
Backflow	Check valve	Flow safety valve		
Burner flame	Burner flame detector	Burner safety low		
Flow	High flow sensor	Flow safety high		
	Low flow sensor	Flow safety low		
Level	High level sensor	Level safety high		
	Low level sensor	Level safety low		
Pressure	High pressure sensor	Pressure safety high		
	Low pressure sensor	Pressure safety low		
	Pressure relief or safety valve	Pressure safety valve		
	Rupture disc or safety head	Pressure safety element		
Pressure or vacuum	Pressure/vacuum relief valve	Pressure safety valve		
	Pressure/vacuum relief manhole cover	Pressure safety valve		
	Vent	None		

Table A.1 (*continued*)

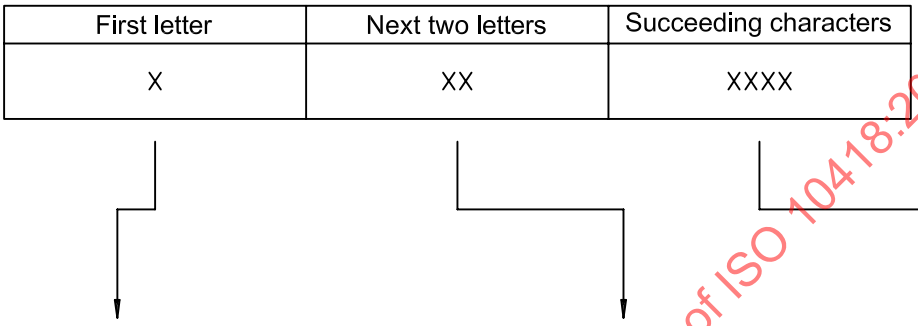
Variable	Sensing and self-actuating device			
	Safety device designation		Symbol	
	Common	Instrument Society of America (ISA)	Single device	Combination device
Vacuum	Vacuum relief valve	Pressure safety valve		
	Rupture disc or safety head	Pressure safety element		
Temperature	High temperature sensor	Temperature safety high		
	Low temperature sensor	Temperature safety low		
Flame	Flame or stack arrestor	None		
Fire	Flame detector (ultraviolet/infrared)			
	Heat detector (thermal)	Temperature safety high		
	Smoke detector (ionization)			
	Fusible material	Temperature safety element		
Combustible gas concentration	Combustible gas detector	Analyser safety high		
Toxic gas concentration	Toxic gas detector			

Actuated valves				
Service	**Common symbols**			
Wellhead surface safety valve or underwater safety valve			NOTE Show “USV” for underwater safety valves.	
Blowdown valve				
All other shutdown valves				

A.3 Component identification

The device functional identification is followed by a reference to the component it protects. The first letter of the component identification represents the component type. The first letter should be one of the letters in the code column in Table A.2. The letter is selected according to the component type listed in the second column in Table A.2. The succeeding two letters are used to further define or modify the first letter. The last four characters identify the specific component. These characters are user-assigned and should be unique to the component at the particular location.

Table A.2 — Component identification



Component type			Component modifier		Component identifier (User-assigned identification unique to equipment at location)
Code	**Component**	**Common modifiers**	**Code**	**Component**	
A	Atmospheric vessel (ambient temperature)	BH,BJ,BM	AA	Bidirectional	
B	Atmospheric vessel (heated)	AP,BC,BK,BM	AB	Blowcase	
C	Compressor	None	AC	Boiler	
D	Enclosure	AE,AN,AU,BB	AD	Coalescer	
E	Fired or exhaust-heated component	AL,AW,BN	AE	Compressor	
F	Flowline	A1 to A9	AF	Contactor	
G	Header	AR,AS,AT,AY,AZ	AG	Control unit	
H	Heat exchanger	BG	AH	Departing	
J	Injection line	AR,AS,AT	AJ	Filter	
K	Pipeline	AA,AH,AQ	AK	Filter-separator	
L	Platform	AG	AL	Forced draft	
M	Pressure vessel (ambient temperature)	AB,AD,AF,AJ,AK,AM, AV,BD,BF,BH,BJ,BL,BM	AM	Freewater knockout	
N	Pressure vessel (heated)	AC,AF,AM,AP,BC,BD, BG,BJ,BK	AN	Generator	
P	Pump	AX,BA,BE	AP	Heater	
Q	Wellhead	AR,AT,AY,AZ	AQ	Incoming	
Z	Other		AR	Injection, gas	
			AS	Injection, gas lift	
			AT	Injection, water	
			AU	Meter	
			AV	Metering vessel	
			AW	Natural draft	
			AX	Pipeline	
			AY	Production, hydrocarbon	
			AZ	Production, water	

Table A.2 (*continued*)

Component type			Component modifier		Component identifier (User-assigned identification unique to equipment at location)
Code	**Component**	**Common modifiers**	**Code**	**Component**	
			A1-A9	Flowline segment	
			BA	Process, other	
			BB	Pump	
			BC	Reboiler	
			BD	Separator	
			BE	Service	
			BF	Scrubber	
			BG	Shell and tube	
			BH	Sump	
			BJ	Tank	
			BK	Treater	
			BL	Volume bottle	
			BM	Water treating	
			BN	Exhaust-heated	
			ZZ	Other	

A.4 Example identification

Examples of the recommended identification methods are given in Figure A.1.

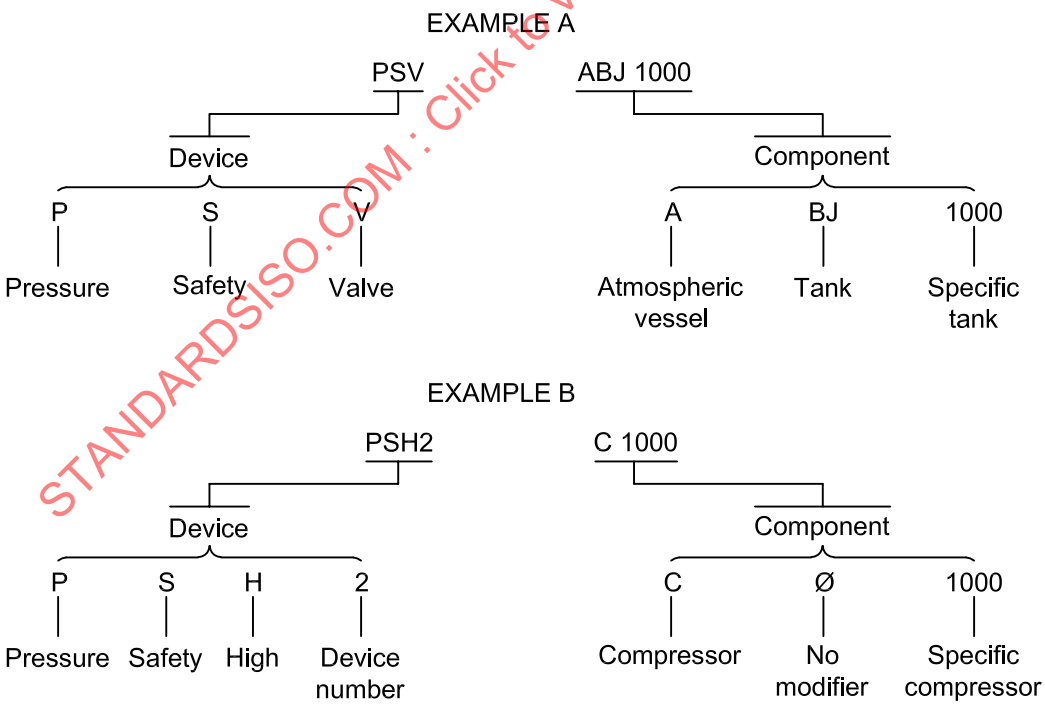


Figure A.1 — Examples of safety device identification

Annex B
(informative)

Analysis using tables, checklists and functional evaluation charts

B.1 General

This annex presents a complete safety analysis of each basic process component normally used in a platform production process system. This component analysis includes the following:

a) the undesirable events which should be considered when designing process facilities, together with likely causes, effects, primary and secondary methods of protection and the location of safety devices;

b) a description of each process component;

c) a typical drawing of each process component showing all recommended safety devices that should be considered based on individual component analysis. A discussion of each process component is included, outlining recommended safety device locations;

d) a SAT for each process component, analysing the undesirable events that could affect the component;

e) a SAC for each process component, listing all recommended safety devices and showing conditions under which particular safety devices may be excluded. A discussion of the rationale for including or excluding each safety device is presented;

f) a SAFE chart relating all sensing devices, SDVs, shutdown devices, and ESSs to their functions.

B.2 Undesirable events — Causes, effects and protection methods

B.2.1 General

An undesirable event is an adverse occurrence in a process component that poses a risk to safety. The undesirable events discussed in this clause are those that can develop in a process component under worst-case conditions of input and output. An undesirable event can be indicated by one or more process variables ranging out of operating limits. These abnormal operating conditions can be detected by sensors that initiate shutdown action to protect the process component. Each undesirable event that can affect a process component is discussed according to the following format:

— cause;

— effect and detectable abnormal condition;

— primary and secondary protection that should prevent or react to its occurrence. The general approach has been applied to a wide range of process components in common use, and the results are shown in B.3 through B.12. If a process component is to be used which is not included in B.3 through B.12, then the general approach can be used to derive the required SATs, SACs and device requirements.

It should be noted that a device or system can only be considered as a method of protection if it is sufficient on its own to prevent the undesirable occurrence, e.g. in the case of overpressure the PSH can only be considered as primary protection if it can safely shut off all inflow and heat sources and prevent a rupture or overpressure event.

B.2.2 Overpressure

B.2.2.1 Cause

Overpressure can be caused by an input source that develops pressure in excess of a process component's maximum allowable working pressure if inflow exceeds outflow. Inflow can exceed outflow if an upstream flowrate control device fails, if there are restrictions or blockage in the component's outlets, or if overflow or gas blowby from an upstream component occurs. Overpressure can also be caused by thermal expansion of fluids within a component if heat is added while the inlets and outlets are closed.

B.2.2.2 Effect and detectable abnormal condition

Overpressure can result in a sudden rupture and subsequent leak of hydrocarbons. “High pressure” is the detectable abnormal condition that indicates that overpressure can occur.

B.2.2.3 Primary protection

Primary protection from overpressure in a pressurized component should be provided by a PSH protection system to shut off inflow. If a vessel is heated, the PSH sensor should also shut off the fuel or source of heat. Primary protection for atmospheric pressure components should be provided by an adequate vent system.

B.2.2.4 Secondary protection

Secondary protection from overpressure in a pressurized component should be provided by a PSV. Secondary protection for atmospheric pressure components should be provided by a second vent. The second vent may be identical to the primary vent, a gauge hatch with a self-contained PSV or an independent PSV. Alternatively, an instrument-based system may be used for primary and secondary protection, provided it is implemented in accordance with IEC 61511-1. If a pilot relief valve is used, then the design should be such that in the case of pilot failure the valve will continue to function so that pressure is kept within the maximum allowable pressure.

If appropriate, bursting discs (PSEs) or buckling-pin valves may be used as an alternative to a PSV.

Low temperature can be caused by release of certain materials to atmosphere, and relief systems should be designed for the low temperature that can result from such operations.

B.2.2.5 Location of safety devices

In a process component with both liquid and gas sections, the PSH system, PSV or vent should be installed to sense or relieve pressure from the gas or vapour section. The sensing connections for the safety devices should be located at the highest practical location on the component, in order to minimize the chance of fouling by flow stream contaminants. The installation of PSVs and vents on atmospheric tanks should be in accordance with API Std 2000[14] or other applicable standards.

B.2.3 Leaks

B.2.3.1 Cause

A leak can be caused by deterioration from corrosion, erosion, mechanical failure or excess temperature; by rupture from overpressure; or by accidental damage from external forces.

B.2.3.2 Effect and detectable abnormal conditions

A leak can result in the release of hydrocarbons to the atmosphere. “Low pressure”, “backflow” and “low level” are the abnormal conditions that might be detectable to indicate that a leak has occurred. Alternatively, the ESS system should be able to detect such occurrences by detecting the ultrasound emitted by the leak or by detecting gas accumulation.

B.2.3.3 Primary protection

Primary protection from leaks of sufficient rate to create an abnormal operating condition within a pressure component should be provided by a PSL sensor to shut off inflow and an FSV to minimize backflow. Primary protection from leaks from the liquid section may also be provided by an LSL sensor to shut off inflow. On an atmospheric pressure component, primary protection from liquid leaks should be provided by an LSL sensor to shut off inflow. A containment system should provide primary protection from small liquid leaks that cannot be detected by the safety devices on a process component. Primary protection from small gas leaks that occur in an inadequately ventilated area and cannot be detected by component sensing devices should be provided by a combustible-gas detection system.

Pressure- and level-sensing devices are in many cases incapable of detecting even severe leaks, and need not be provided for leak detection purposes if it can be shown that the ESS is capable of detecting fire and gas occurrences such that the likelihood of escalation is minimized.

If pressure- and level-sensing devices are not provided for leak detection, then fire and gas detection should be provided as described in a) or b) below.

a) The number and location of detectors should be in accordance with the fire and explosion strategy as specified in ISO 13702.

b) As a minimum, four point detectors should be installed around the device, typically at a distance of 4 m to 5 m from the equipment, or two beam-type gas detectors should be installed on opposite sides of the equipment, with the beams typically at a distance of 4 m to 5 m from the equipment.

B.2.3.4 Secondary protection

Secondary protection from gas leaks should be provided by the ESS. Secondary protection from small liquid leaks should be provided by an LSH sensor installed on the sump tank to shut in all components that could leak into the sump.

B.2.3.5 Location of safety devices

In a process component with both liquid and gas sections, the PSL sensor should be connected to sense pressure from the gas or vapour section. The PSL sensor should be installed at the highest practical location on the component, in order to minimize the chances of fouling by flow stream contaminants. FSVs should be installed in each component operating outlet line subject to significant backflow. The LSL sensor should be located a sufficient distance below the lowest operating liquid level to avoid nuisance shutdowns, but with adequate volume between the LSL sensor and liquid outlet to prevent gas blowby before shutdown is accomplished.

B.2.4 Liquid overflow

B.2.4.1 Cause

Liquid overflow can be caused by liquid input in excess of liquid outlet capacity. This can be the result of failure of an upstream flowrate control device, failure of the liquid level control system, or blockage of a liquid outlet.

B.2.4.2 Effects and detection of abnormal condition

Liquid overflow can result in overpressure or excess liquids in a downstream component, or release of hydrocarbons to the atmosphere. "High level" is the detectable abnormal condition that indicates that overflow can occur.

B.2.4.3 Primary protection

Primary protection from liquid overflow should be provided by an LSH sensor to shut off flow into the component.

B.2.4.4 Secondary protection

Secondary protection from liquid overflow to the atmosphere should be provided by the ESSs. Secondary protection from liquid overflow to a downstream component should be provided by safety devices on the downstream component. Alternatively, an instrument-based system may be used for primary and secondary protection systems, providing it is implemented in accordance with IEC 61511-1.

B.2.4.5 Location of safety devices

The LSH sensor should be located a sufficient distance above the highest operating liquid level of a component to prevent nuisance shutdowns, but with adequate volume above the LSH sensor to prevent liquid overflow before shutdown is accomplished.

With high-flowrate deepwater wells in the event of a blocked liquid outlet, the volume required between LSH and the gas outlet is very large and greatly increases the required size of the vessel. If the liquid overflow is contained by downstream components, then the volume available in the downstream vessel can be taken into account provided this does not pose a hazard.

B.2.5 Gas blowby

B.2.5.1 Cause

Gas blowby can be caused by failure of a liquid level control system or inadvertent opening of a bypass valve around a level control valve.

B.2.5.2 Effect and detectable abnormal condition

Gas blowby can result in overpressure in a downstream component. “Low level” is the detectable abnormal condition that indicates gas blowby may occur.

B.2.5.3 Primary protection

Primary protection from gas blowby should be provided by an LSL sensor to shut off inflow or shut off the liquid outlet.

B.2.5.4 Secondary protection

Secondary protection from gas blowby to a downstream component should be provided by safety devices on the downstream component. Alternatively, an instrument-based system may be used for primary and secondary protection provided it is implemented in accordance with IEC 61511-1.

Flow restrictions may be installed on the liquid outlet to reduce gas blowby, in order to meet the relief capacity of downstream components.

B.2.5.5 Location of safety devices

The LSL sensor should be located a sufficient distance below the lowest operating liquid level to avoid nuisance shutdowns, but with an adequate volume between the LSL sensor and liquid outlet to prevent gas blowby before shutdown is accomplished.

B.2.6 Underpressure

B.2.6.1 Cause

Underpressure can be caused by fluid withdrawal in excess of inflow that may be the result of failure of an inlet or outlet control valve, blockage of an inlet line during withdrawal, shut-in of production during withdrawal, or thermal contraction of fluids when the inlets and outlets are closed.

B.2.6.2 Effect and detectable abnormal condition

Underpressure can result in collapse of the component and a leak. “Low pressure” is the detectable abnormal condition that indicates underpressure may occur.

B.2.6.3 Primary protection

Primary protection from underpressure in an atmospheric component should be provided by an adequate vent system. Primary protection for a pressure component subject to underpressure should be provided by a gas make-up system.

B.2.6.4 Secondary protection

Secondary protection for an atmospheric component should be provided by a second vent or by a PSV (vacuum breaker). Secondary protection for a pressure component subject to underpressure should be provided by a PSL sensor to shut off inflow and outflow or a gas make-up system.

NOTE If primary protection is provided by a gas make-up system and secondary protection is provided by a gas make-up system or an instrument-based protection system and a hazardous condition would occur on underpressure, then the systems should be implemented in accordance with IEC 61511-1.

B.2.6.5 Location of safety devices

The PSL sensor should be installed at the highest practical location on the component to minimize the chances of fouling by flow stream contaminants. Vents and PSVs should be installed in accordance with API Std 2000[14] or other applicable standards.

B.2.7 Excess temperature (fired and exhaust-heated components)

B.2.7.1 General

This undesirable event in fired and exhaust-heated components is categorized as excess medium or process fluid temperature and excess stack temperature. Excess temperature or low temperature in unfired components is discussed in individual component analyses in this annex.

B.2.7.2 Cause

Excess medium or process fluid temperature can be caused by excess fuel or heat input due to failure or inadvertent bypassing of the fuel or exhaust gas control equipment, extraneous fuel entering the firing chamber through the air intake, or a leak of combustible fluids into the fired or exhaust-heated chamber; insufficient volume of heat transfer fluid due to low flow in a closed heat transfer system (where the heated medium is circulated through tubes located in the firing or exhaust-heated chamber); or low liquid level in a fired component with an immersed fire or exhaust gas tube. Excess stack temperature in a fired component can be caused by any of the above or by insufficient transfer of heat because of accumulation of foreign material (sand, scale, etc.) in the heat transfer section. Excess stack temperature in an exhaust-heated component can result from ignition of a combustible-medium leak into the exhaust-heated chamber.

B.2.7.3 Effect and detectable abnormal condition

High medium or process fluid temperature can result in a reduction of the working pressure and subsequent leak or rupture of the affected component and/or overpressure of the circulating tubes in a closed heat transfer system, if the medium is isolated in the tubes. High stack temperature can result in a direct ignition source for combustibles coming in contact with the stack surface. “High temperature”, “low flow” and “low level” are the detectable abnormal conditions that indicate that excess temperature may occur.

B.2.7.4 Primary protection

Primary protection from excess medium or process fluid temperature resulting from excess or extraneous fuel, heat, or medium leaks into the fired or heated chamber should be provided by a TSH sensor. If caused by low liquid level, protection should be provided by an LSL sensor. The TSH and LSL sensors on fired components should shut off fuel supply and inflow of combustible fluids. The TSH and LSL sensors on exhaust-heated components should divert or shut off the fuel or heat source. If excess medium temperature is due to low flow in a closed heat transfer system containing combustible fluid, primary protection should be provided by an FSL sensor to shut off fuel supply to a fired component or to divert the exhaust flow from an exhaust-heated component. Primary protection from excess stack temperature should be provided by a TSH (stack) sensor to shut off the fuel or exhaust gas source and inflow of combustible fluids.

B.2.7.5 Secondary protection

Secondary protection from excess medium or process fluid temperature in a fired component, if caused by excess or extraneous fuel, should be provided by a TSH (stack) sensor, and, if caused by low flow, by a TSH (medium) sensor and TSH (stack) sensor. If caused by low level, secondary protection should be provided by a TSH (medium or process fluid) sensor and TSH (stack) sensor. Secondary protection from excess medium or process fluid temperature in an exhaust-heated component, if caused by low level or low flow, should be provided by a TSH (medium) sensor. These TSH sensors should perform the same function as the primary protection. Secondary protection for excess stack temperature should be provided by the ESS and an FSV, where applicable.

B.2.7.6 Location of safety devices

Temperature sensors, other than fusible or skin contact types, should be placed in a thermowell for ease of removing and testing. In a two-phase (gas/liquid) system, the TSH sensor should be located in the liquid section. In a tube-type heater, where the heated medium flows through tubes located in the firing or heating chamber, the TSH sensor should be located in the tube outlet as close as practical to the heater. An FSV should be installed on medium tube outlet piping.

B.2.8 Direct ignition source (fired components)

B.2.8.1 General

A direct ignition source is an exposed surface, flame or spark at sufficient temperature and heat capacity to ignite combustibles. Direct ignition sources discussed in this clause are limited to fired components. Electrical systems and other ignition sources are discussed in ISO 13702.

B.2.8.2 Cause

Direct ignition sources can be caused by flame emission from the air intake due to the use of improper fuel (e.g. liquid carryover in a gas burner), reverse draft from a natural-draft burner, or extraneous fuel entering the air intake; spark emission from the exhaust stack, or hot surfaces resulting from excess temperature.

B.2.8.3 Effect and detectable abnormal condition

A direct ignition source can result in a fire or explosion if contacted by a combustible material. “High temperature” and “low air flow” (forced-draft burners only) are the detectable abnormal conditions that indicate a direct ignition source may occur.

B.2.8.4 Primary protection

Primary protection from flame emission through the air intake of a natural-draft burner should be provided by a flame arrestor to contain the flame in the firing chamber. Primary protection from flame emission through the air intake of a forced-draft burner should be provided by a PSL (air intake) sensor to detect low air flow and shut off the fuel and air supply. A stack arrestor should provide primary protection from exhaust-stack spark emission. Primary protection from hot surfaces due to excess temperature should be provided by a TSH (medium or process fluid) sensor and TSH (stack) sensor. The TSH sensor should shut off fuel supply and inflow of combustible fluids.

B.2.8.5 Secondary protection

Secondary protection from flame emission through the air intake of a natural-draft burner should be provided by the ESS. Secondary protection from flame emission through the air intake of a forced-draft burner should be provided by a blower motor interlock to detect blower motor failure and to initiate a signal to shut off the fuel and air supply. Secondary protection from exhaust-stack spark emission and hot surfaces should be provided by the ESS and an FSV where applicable.

B.2.8.6 Location of safety devices

The location of air-intake flame arrestors and exhaust-stack spark arrestors is fixed. These items should be installed to facilitate inspecting and cleaning. TSH (stack, media, process fluids) sensors should be installed as discussed in B.2.6.7. A PSL (air intake) sensor should be installed downstream of the blower fan inside the air intake on a forced-draft burner. Forced-draft burners should have starter interlocks installed on the blower motor starter. An FSV should also be installed in medium tube outlet piping.

B.2.9 Excess combustible vapours in the firing chamber (fired component)

B.2.9.1 General

Excess combustible vapours in the firing chamber are combustible vapours in addition to those required for normal ignition of either the pilot or main burner.

B.2.9.2 Cause

Accumulation of excess combustible vapours in the firing chamber can be caused by a failure of the fuel or air supply control equipment or improper operating procedures.

B.2.9.3 Effect and detectable abnormal condition

Excess combustible vapours in the firing chamber, on ignition, can result in an explosion and possible rupture of the component. “Flame failure” and “high or low fuel supply pressure” are detectable abnormal conditions that can indicate excess combustible vapours in the firing chamber. Low air supply pressure and blower failure may also indicate this condition in forced-draft burners.

B.2.9.4 Primary protection

Primary protection from excess combustible vapours in the firing chamber caused by a mechanical failure of the fuel control equipment should be provided by a flame-failure sensor. The sensor should detect a flame insufficient to ignite the entering vapours and shut off the fuel. The sensor may be the light-detecting type (BSL), such as an ultraviolet detector, or the heat-sensing type (TSL).

B.2.9.5 Secondary protection

Secondary protection from excess combustible vapours in the firing chamber due to fuel control failure should be provided by a PSH (fuel) sensor to shut off the fuel. On a forced-draft burner, a PSL sensor should be installed on the fuel supply; also, a PSL (air) sensor and motor starter interlock should be installed to detect an inadequate air supply and initiate a signal to shut off the fuel and air. An FSL sensor may be installed in place of a PSL sensor in the air intake to sense low air flow. In addition to the above safety devices, safe operating procedures should also be followed to prevent firebox explosions during ignition of the pilot or main burner. Recommended safe operating procedures are shown in Table B.15.

B.2.9.6 Location of safety devices

A BSL or TSL sensor should be installed in the firing chamber to monitor the pilot and/or main burner flame. PSH and PSL sensors in the fuel supply should be installed downstream of all fuel pressure regulators. A PSL (air intake) sensor should be installed in the air intake downstream of the forced-draft blower.

B.2.10 Excess temperature (pipe embrittlement)

B.2.10.1 Causes

Excessive pressure drop of dry gases can produce a Joule-Thompson effect. This effect can create extremely low temperatures in the downstream piping after the pressure drop, and can cause the low temperature limit of the piping to be exceeded.

B.2.10.2 Effect and detectable abnormal conditions

Extremely low temperature in the downstream piping can result in brittle fracture and failure of the piping. “Low temperature” in the downstream section is the detectable condition.

B.2.10.3 Primary protection

Primary protection from low temperature embrittlement should be through the installation of a TSL located downstream of the pressure drop. If low temperatures only result from a high pressure drop, then a high differential pressure monitor may give a quicker response time and could be considered as an alternative. The monitoring devices should shut off the process flow.

B.2.10.4 Secondary protection

Secondary protection should be through the process design, such that the containment envelope is not vulnerable to low temperature embrittlement. If the system cannot be designed to avoid low temperature embrittlement or there are temperature-based operating constraints, e.g. the system must be allowed to warm up following a low temperature event before repressurization can occur, then a TSL designed to the requirements of IEC 61511-1 is required.

B.2.10.5 Location of safety devices

TSL sensors should be installed as insertion elements protected by thermowells in the downstream piping no more than 5 diameters from the source of pressure drop.

TSL sensors to monitor the ambient conditions should be installed in the vicinity of vulnerable plant in a location where the temperature is representative of that experienced by the plant.

High differential pressure sensors should be located so that there are no isolation valves between the sensing elements and the source of pressure drop.

B.3 Wellheads and flowlines

B.3.1 Description

Wellheads furnish surface control (manual and automatic) and containment of well fluids and provide downhole access for well servicing. Flowlines transport hydrocarbons from the wellhead to the first downstream process component.

For analysis purposes and assignment of safety devices, flowlines are divided into flowline segments. A flowline segment is any portion of a flowline that has an assigned operating pressure different from other portions of the same flowline. These flowline segments can be classified as either initial (beginning at wellhead), intermediate, or final (terminating at another process component) segments. Thus, a flowline that experiences a reduction in operating pressure due to some inline pressure-reducing device, such as a choke, and has two different assigned operating pressures, will have an initial and final segment. A flowline that experiences no reduction in operating pressure due to a pressure-reducing device will have only one segment. In this case, the initial and final flowline segments will be the same. Each flowline segment shall be analysed to determine appropriate safety devices. Recommended safety devices for typical wellheads and flowlines are shown in Figures B.1, B.2 and B.3.

Dimensions in metres

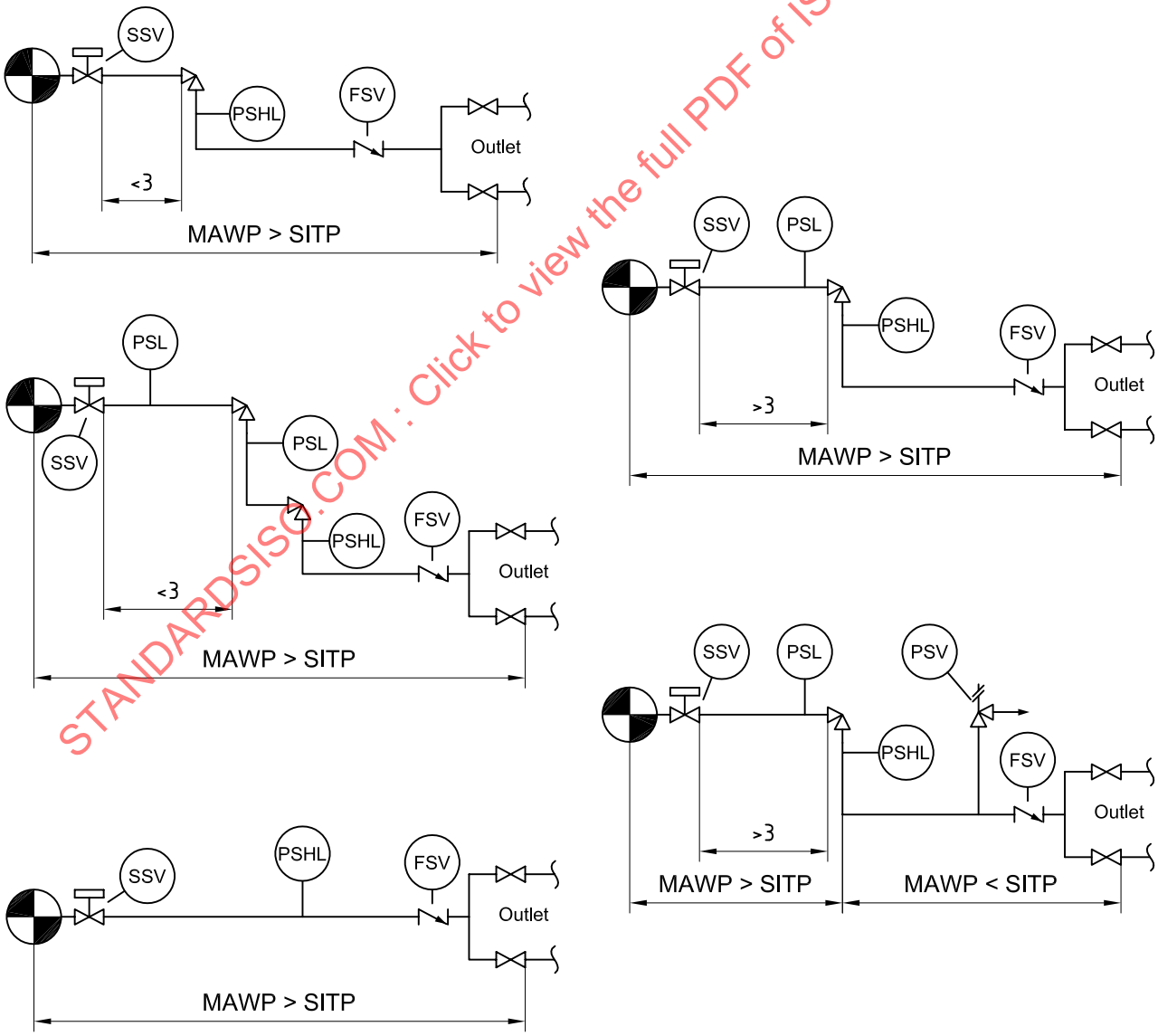
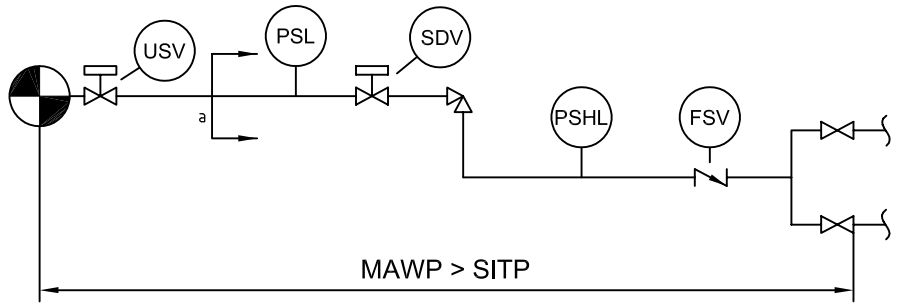


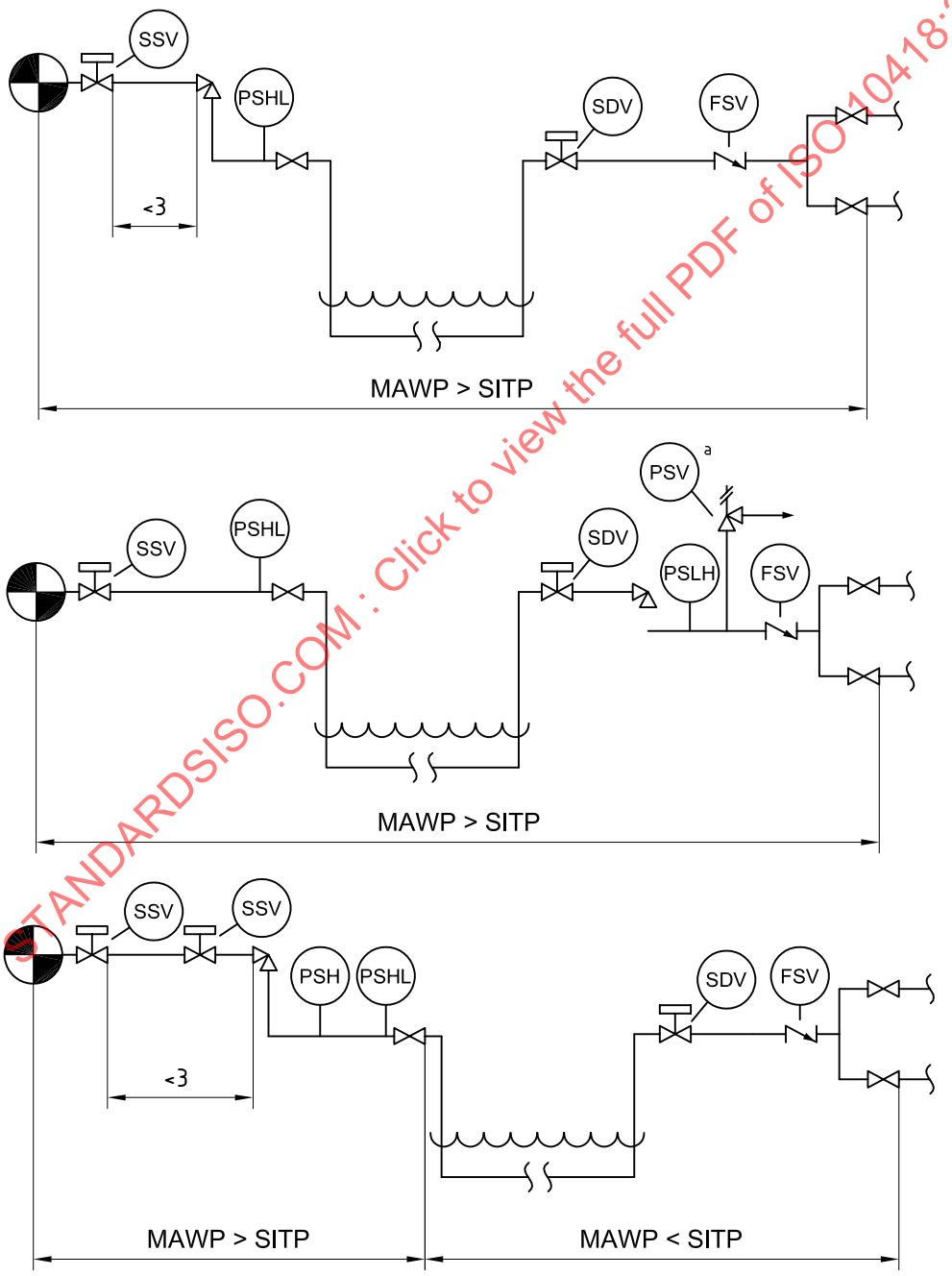
Figure B.1 — Recommended safety devices — Typical wellhead flowlines



a Denotes platform limits.

Figure B.2 — Recommended safety devices — Underwater wellhead flowlines

Dimensions in metres



a PSV location can be upstream or downstream of FSV.

Figure B.3 — Recommended safety devices — Satellite well

B.3.2 Safety analysis

B.3.2.1 Safety analysis table (SAT)

The SAT for a flowline segment is presented in Table B.1. The undesirable events that can affect a flowline segment are overpressure, leak and excess temperature.

Table B.1 — Safety analysis table (SAT) — Flowline segment

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted line Downstream choke plugged Hydrate plug Upstream flow control failure Changing well conditions Closed outlet valve	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure or fire or gas accumulation
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature

B.3.2.2 Safety analysis checklist (SAC) (see Table B.2)

Table B.2 — Safety analysis checklist (SAC) — Flowline segment

SAC Ref. No.	Device SAFE (see Table B.1)	Checklist
a)	PSH	1) PSH installed. 2) Flowline segment has a maximum allowable working pressure greater than maximum shut-in pressure and is protected by a PSH on a downstream flowline segment.
b)	PSL	1) PSL installed. 2) Flowline segment is between the well and the first choking device and is less than 3 m in length or, for an underwater installation, reasonably close to that distance. 3) ESS is capable of detecting fire and gas accumulation such that the likelihood of escalation is minimized.
c)	PSV	1) PSV installed. 2) Flowline segment has a maximum allowable working pressure greater than the maximum shut-in pressure. 3) A system is installed meeting the requirements of IEC 61511-1 where there is adequate flowline volume upstream of any block valves to allow sufficient time for the SDVs to close before exceeding the maximum allowable working pressure. 4) Flowline segment is protected by a PSV on upstream segment. 5) Flowline segment is protected by a PSV on downstream component that cannot be isolated from the flowline segment and there are no chokes or other restrictions between the flowline segment and the PSV.
d)	FSV	1) FSV installed. 2) Flowline segment is protected by FSV in final flowline segment.
e)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
f)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.

B.3.2.2.1 Pressure safety devices (PSH, PSL, and PSV)

Because wells are the primary source of pressure, a PSH sensor to shut in the well should always be provided on each flowline to detect abnormally high pressure. A PSH sensor to shut in the well should be installed on the final flowline segment and on any other segment that has a maximum allowable working pressure less than the maximum shut-in tubing pressure of the well. A PSL sensor to shut in the well should be provided on each flowline segment, except the initial segment if the first choking device is less than 3 m from the wellhead. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas accumulation such that escalation can be prevented.

A PSV is not required if the maximum allowable working pressure of a flowline segment is greater than the maximum shut-in tubing pressure of the well, or if the segment is protected by a PSV located on an upstream flowline segment. An SDV (in addition to the SSV) with an independent PSH sensor implemented in accordance with IEC 61511-1 is an acceptable alternate to a PSV, providing the flowline volume upstream of block valves is adequate to allow sufficient time for the SDVs to close before exceeding the maximum allowable working pressure. This alternative should be approached with caution, after thorough consideration of other alternatives.

B.3.2.2.2 Flow safety device (FSV)

A check valve (FSV) is only necessary in the final flowline segment to minimize backflow to the flowline.

B.3.2.2.3 Temperature safety devices (TSH and TSL)

A temperature safety device is only required if fluid temperatures during fault conditions can cause design limits of the piping to be exceeded. Low temperatures can be caused by gas pressure drops or active cooling. High temperatures can be caused by fluid conditions or active heating.

B.3.3 Safety device locations

B.3.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors should be located for protection from damage due to vibration, shock and accidents. The sensing point should be located on top of a horizontal run or in a vertical run. An independent sensing point should be provided for a second PSH used with an SDV as alternative protection for a PSV. The PSV should be located upstream of the first blocking device in the flowline segment and should not be set higher than the rated working pressure of the segment.

B.3.3.2 Flow safety device (FSV)

The check valve (FSV) should be located in the final flowline segment so that the entire flowline is protected from backflow.

B.3.3.3 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

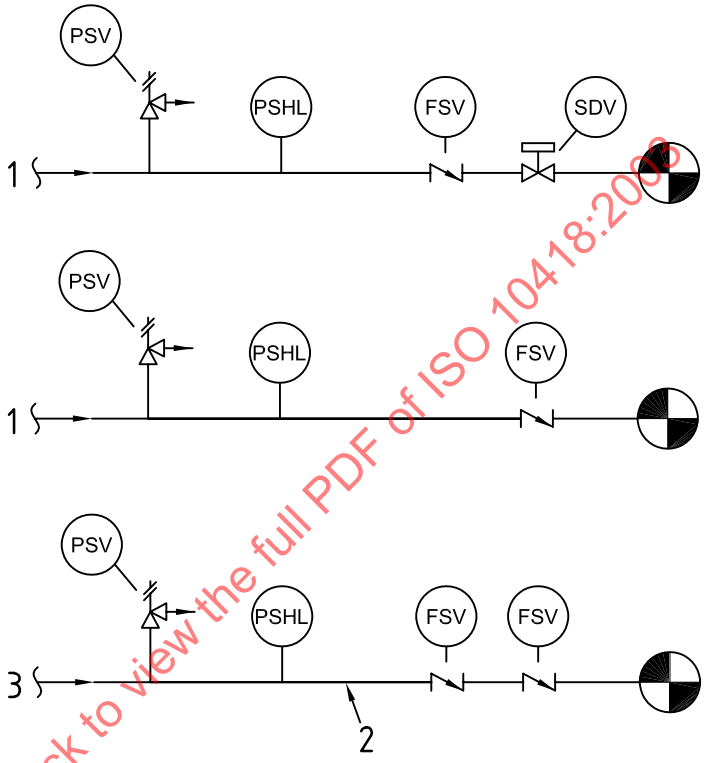
B.3.3.4 Shutdown devices (SSV or USV)

The SSV should be located on the wellhead as the second valve in the flow stream after the lower master block valve. The SSV should be actuated by the flowline pressure sensors, ESD system, fire loop system, and sensors on downstream process components. An SDV (in addition to the SSV) may be installed on the wellhead downstream of the SSV. If an SDV is installed, it may be actuated, in lieu of the SSV, by the flowline pressure sensors and sensors on downstream process components. The USV should be in a practical location in the wellhead flowstream, and within reasonable proximity of the wellbore. The USV should be actuated by the flowline pressure sensors located upstream of any SDV, by the ESD system, and by the fire loop system. The SDV is optional on subsea wells equipped with USVs.

B.4 Wellhead injection lines

B.4.1 Description

Injection lines transfer fluids to the wellbore for artificial lift or reservoir injection. Recommended safety devices for typical wellhead injection lines are shown in Figure B.4.



Key

1 from injection source
2 wellhead gas lift line
3 from gas lift source

Figure B.4 — Recommended safety devices — Typical wellhead injection lines

B.4.2 Safety analysis

B.4.2.1 Safety analysis table (SAT)

The SAT for wellhead injection lines is presented in Table B.3. The undesirable events that can affect an injection line are overpressure, leak and excess temperature.

Table B.3 — Safety analysis table (SAT) — Wellhead injection lines

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Hydrate plug Upstream flow control failure Plugged formation	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration	Low pressure or fire or gas accumulation
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature

B.4.2.2 Safety analysis checklist (SAC) (see Table B.4)

Table B.4 — Safety analysis checklist (SAC) — Wellhead injection lines

SAC Ref. No.	Device SAFE (see Table B.3)	Checklist
a)	PSH	1) PSH installed. 2) Line and equipment are protected by an upstream PSH.
b)	PSL	1) PSL installed. 2) Line and equipment are protected by an upstream PSL. 3) ESS is capable of detecting fire and gas accumulation such that the likelihood of escalation is minimized.
c)	PSV	1) PSV installed. 2) Line and equipment have a maximum allowable working pressure greater than the maximum pressure that can be imposed by the injection source. 3) Line and equipment are protected by an upstream PSV. 4) A system is installed meeting the requirements of IEC 61511-1 which is capable of shutting off sources of pressure which exceed maximum allowable working pressure.
d)	FSV	FSV installed.
e)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
f)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.

B.4.2.2.1 Pressure safety devices (PSH, PSL and PSV)

Pressure protection is usually provided by a PSH and a PSL sensor on the injection source, such as a compressor or pump, to shut off inflow. If the PSH and PSL sensors also protect the injection line, wellhead and other equipment, these devices are not required on the injection line. A PSV is not necessary if the injection line is designed to withstand the maximum pressure that can be imposed by the injection source. Usually, a PSV is provided on the injection source that will also protect the injection line, wellhead and other equipment. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented.

B.4.2.2.2 Flow safety device (FSV)

A check valve (FSV) should be provided on each injection line to minimize backflow.

B.4.2.2.3 Temperature safety devices (TSH and TSL)

A temperature safety device is only required if fluid temperatures during fault conditions can cause design limits of the piping to be exceeded. Low temperatures can be caused by gas pressure drops or active cooling. High temperatures can be caused by fluid conditions or active heating.

B.4.3 Safety device location

B.4.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors should be located upstream of the FSV, and the sensing point should be on top of a horizontal run or in a vertical run. The PSV should be located so that it cannot be isolated from any portion of the injection line subject to overpressure.

B.4.3.2 Flow safety device (FSV)

The check valve (FSV) should be located on each injection line as near the wellhead as is practical, so that the entire line is protected from backflow.

B.4.3.3 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

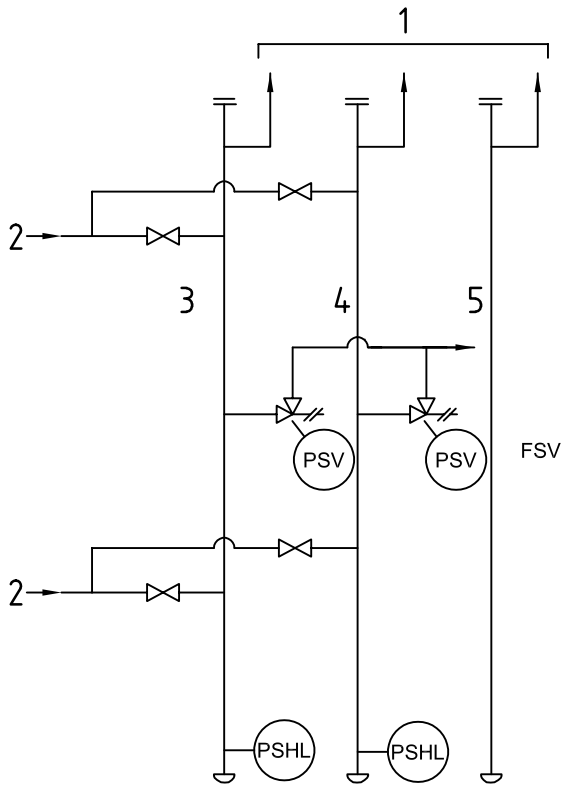
B.4.3.4 Shutdown devices (SDV)

Injection line SDVs should be located as near the wellhead as is practical to minimize the amount of line exposed (Figure B.4 top drawing). SDVs are not required on gas lift lines if they are protected at an upstream component and if they are not subject to backflow from the producing formation (Figure B.4 middle drawing). Also, an SDV is not required if the injection line is for the purpose of injecting water and the subsurface formation is incapable of backflowing hydrocarbons (Figure B.4 bottom drawing). If closing an SDV could cause rapid pressure buildup in the injection line, consideration should be given to shutdown of the injection source and/or use of a second FSV in lieu of an SDV.

B.5 Headers

B.5.1 Description

Headers receive production from two or more flow streams and distribute production to the required process systems, such as the low, intermediate, or high pressure production and test separation facilities. Recommended safety devices for typical headers are shown in Figure B.5.



Key

1 outlets
2 inlet
3 production
4 test
5 relief

Figure B.5 — Recommended safety devices — Headers

B.5.2 Safety analysis

B.5.2.1 Safety analysis table

The SAT for headers is presented in Table B.5. The undesirable events that can affect a header are overpressure, leak and excess temperature.

Table B.5 — Safety analysis table (SAT) — Headers

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Hydrate plug Upstream flow control failure Excess inflow	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration	Low pressure or Fire or Gas accumulation
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature

B.5.2.2 Safety analysis checklist (SAC) (see Table B.6)

Table B.6 — Safety analysis checklist (SAC) — Headers

SAC Ref. No.	Device SAFE (see Table B.5)	Checklist
a)	PSH	1) PSH installed. 2) Each input source is equipped with a PSH set less than the maximum allowable working pressure of the header. 3) Header is protected by downstream PSH that cannot be isolated from the header. 4) Header is for flare, relief, vent, or other atmospheric service and has no valving in the outlet piping.
b)	PSL	1) PSL installed. 2) Each input source is protected by a PSL and there are no pressure control devices or restrictions between the PSL and the header. 3) Header is for flare, relief, vent, or other atmospheric service. 4) ESS is capable of detecting fire and gas accumulation such that the likelihood of escalation is minimized.
c)	PSV	1) PSV installed. 2) Header has a maximum allowable working pressure greater than the maximum shut-in pressure of any connected well. 3) Pressure relief protection is provided on each input source having a maximum shut-in pressure greater than the maximum allowable working pressure of the header. 4) Header is protected by downstream PSV that cannot be isolated from the header. 5) Header is for flare, relief, vent, or other atmospheric service and has no valving in the outlet piping. 6) Input source is a well(s) having a pressure greater than the maximum allowable working pressure of the header and is equipped with a system meeting the requirements of IEC 61511-1. Other input sources having a pressure greater than the maximum allowable working pressure of the header are protected by PSVs.
d)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
e)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.

B.5.2.2.1 Pressure safety devices (PSH, PSL and PSV)

PSH and PSL sensors are not required on headers if each input source is equipped with a PSH and a PSL sensor and the PSH sensor is set less than the rated working pressure of the header. Also, a PSH sensor is not required if the header is protected by a PSH sensor on a downstream process component and the header cannot be isolated from the downstream component. A PSL is not required if the header is for flare, relief, vent or other atmospheric service. If the header requires a PSH and a PSL sensor, the signal from each should shut off all input sources to the header. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that the likelihood of escalation is minimized.

A PSV is not required on a header if

— the maximum allowable working pressure is greater than the maximum shut-in pressure of any connected input source,

— pressure-relief protection is provided on all connected input sources that have a maximum shut-in pressure greater than the maximum allowable working pressure of the header,

— the header is protected by a PSV on a downstream process component that cannot be isolated from the header,

— the header is for flare, relief, vent or other atmospheric service and has no valving in the outlet piping,

— the input source is a well(s) having a pressure greater than the maximum allowable working pressure of the header and is equipped with two SDVs (one of which may be the SSV) controlled by independent PSHs connected to separate relays and sensing points, and other input sources having a pressure greater than the maximum allowable working pressure of the header are protected by PSVs.

The use of two SDVs in lieu of a PSV should be approached with caution after thorough consideration of other alternatives. In some cases, installation of a PSV in addition to two SDVs might be desirable, even at locations having no containment system.

B.5.2.2.2 Temperature safety devices (TSH and TSL)

A temperature safety device is only required if fluid temperatures during fault conditions can cause design limits of the piping to be exceeded. Low temperatures can be caused by gas pressure drops or active cooling. High temperatures can be caused by fluid conditions or active heating.

B.5.3 Safety device location

B.5.3.1 Pressure safety devices (PSH, PSL and PSV)

PSH and PSL sensors or a PSV, if required, should be located to sense pressure throughout the header. If different pressure conditions exist in separate sections of the header, each section should have the required protection.

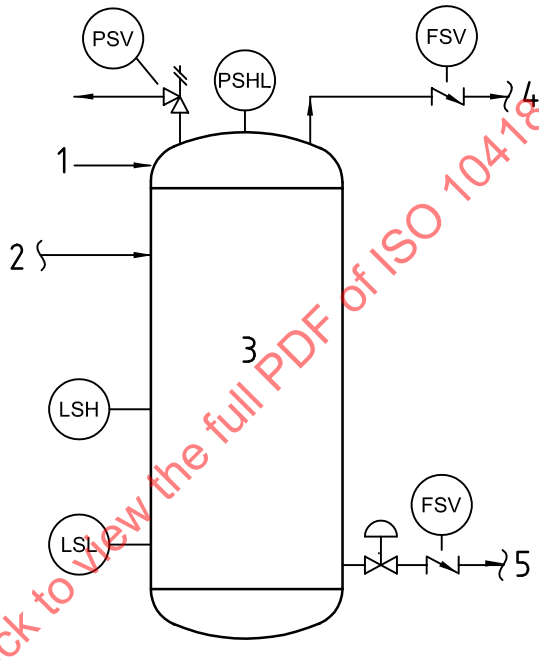
B.5.3.2 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

B.6 Pressure vessels

B.6.1 Description

Pressure vessels handle hydrocarbons under pressure for liquid-gas separation, dehydration, storage and surge. Some pressure vessel applications require heat input. This discussion covers only the effects of heat input to the process section of a heated vessel. Heating equipment is covered in B.8 and B.12. Pressure vessels associated with compressors, other than compressor cylinders, should be protected in accordance with this clause. Compressor cylinders and cases are covered in B.10. Recommended safety devices for typical pressure vessels are shown in Figure B.6.



Key

1 gas makeup system
2 inlet
3 pressure vessel
4 gas outlet
5 oil outlet

If the pressure vessel is heated, TSH should be installed.

Figure B.6 — Recommended safety devices — Pressure vessels

B.6.2 Safety analysis

B.6.2.1 Safety analysis table

The SAT for pressure vessels is presented in Table B.7. The undesirable events that can affect a pressure vessel are overpressure, underpressure, overflow, gas blowby, leak, and excess temperature if the vessel is heated.

Table B.7 — Safety analysis table (SAT) — Pressure vessels

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Inflow exceeds outflow Pressure control system failure Thermal expansion Excess heat input Gas blowby (upstream component)	High pressure
Underpressure	Withdrawals exceed inflow Thermal contraction Open outlet Pressure control system failure	Low pressure
Liquid overflow	Inflow exceeds outflow Liquid slug flow Blocked or restricted liquid outlet Level control system failure	High liquid level
Gas blowby	Liquid withdrawals exceed inflow Open liquid outlet Level control system failure	Low level
Leak	Deterioration Erosion Corrosion Impact damage Vibration	Low pressure, Low liquid level or fire or gas accumulation
Excess temperature	Temperature control system failure High inlet temperature	High temperature

B.6.2.2 Safety analysis checklist (SAC) (see Table B.8)

Table B.8 — Safety analysis checklist (SAC) — Pressure vessels

SAC Ref. No.	Device SAFE (see Table B.7)	Checklist
a)	PSH	1) PSH installed. 2) Input is from a pump or compressor that cannot develop pressure greater than the maximum allowable working pressure of the vessel. 3) Input source is not a wellhead flowline(s), production header, or pipeline and each input source is protected by a PSH that protects the vessel. 4) Adequately sized piping without block or regulating valves connects gas outlet to downstream equipment protected by a PSH that also protects the upstream vessel. 5) Vessel is final scrubber in a flare, relief, or vent system and is designed to withstand maximum built-up back pressure. 6) Vessel operates at atmospheric pressure and has an adequate vent system.
b)	PSL	1) PSL installed. 2) Minimum operating pressure is atmospheric pressure when in service. 3) Each input source is protected by a PSL and there are no pressure control devices or restrictions between the PSL(s) and the vessel. 4) Vessel is scrubber or small trap, is not a process component, and adequate protection is provided by downstream PSL or design function (e.g. vessel is gas scrubber for pneumatic safety system or final scrubber for flare, relief, or vent system). 5) Adequately sized piping without block or regulating valves connects gas outlet to downstream equipment protected by a PSL that also protects the upstream vessel. 6) ESS is capable of detecting gas accumulation and fire such that the likelihood of escalation is minimized and vessel is not subject to underpressure damage.

Table B.8 (*continued*)

SAC Ref. No.	Device SAFE (see Table B.7)	Checklist
c)	PSV	1) PSV installed. 2) Each input source is protected by a PSV set no higher than the maximum allowable working pressure of the vessel and a PSV is installed on the vessel for fire exposure and thermal expansion. 3) Each input source is protected by a PSV set no higher than the vessel's maximum allowable working pressure and at least one of these PSV's cannot be isolated from the vessel. 4) PSVs on downstream equipment can satisfy relief requirement of the vessel and cannot be isolated from the vessel. 5) Vessel is final scrubber in a flare, relief or, vent system, is designed to withstand maximum built-up back pressure, and has no internal or external obstructions, such as mist extractors, back pressure valves, or flame arrestors. 6) Vessel is final scrubber in a flare, relief or, vent system, is designed to withstand maximum built-up back pressure, and is equipped with a rupture disk or safety head (PSE) to bypass any internal or external obstructions, such as mist extractors, back pressure valves, or flame arrestors. 7) An input source has a pressure greater than the maximum allowable working pressure of the vessel and the vessel is equipped with a system meeting the requirements of IEC 61511-1. 8) Input source to the vessel cannot develop pressure greater than the maximum allowable working pressure of the vessel and a PSV is installed on the vessel for fire exposure and thermal relief.
d)	LSH	1) LSH installed. 2) Equipment downstream of gas outlet is not a flare or vent system and can safely handle maximum liquid carry-over. 3) Vessel function does not require handling separated fluid phases. 4) Vessel is a small trap from which liquids are manually drained.
e)	LSL	1) LSL installed to protect each liquid outlet. 2) Liquid level is not automatically maintained in the vessel, and the vessel does not have an immersed heating element subject to excess temperature. 3) Equipment downstream of liquid outlet(s) can safely handle maximum gas rates that can be discharged through the liquid outlet(s), and vessel does not have an immersed heating element subject to excess temperature. Restrictions in the discharge line(s) may be used to limit the gas flow rate.
f)	FSV	1) FSV installed on each outlet. 2) The maximum volume of hydrocarbons that could backflow from downstream equipment is insignificant. 3) A control device in the line will effectively minimize backflow.
g)	TSH [a]	1) TSH installed. 2) See Note. 3) Heat source is incapable of causing excess temperature.
h)	LSH (downstream overflow protection)	1) Gas lines subject to overflow are connected to process item capable of handling liquids. 2) Vessel is equipped with a second LSH designed in accordance with IEC 61511-1. 3) Vessel is scrubber for gas compressor and only receives process gas from other vessels equipped with LSH devices.
i)	LSL (downstream gas blowby protection)	1) Downstream PSV is sized to pass maximum gas blowby from this vessel. 2) Vessel is equipped with a second LSL designed in accordance with IEC 61511-1.
NOTE This option was deleted from the original checklist in API RP 14C [8] when the second edition was published. The number reference is retained here to allow easy comparison of SAFE charts.		
[a] High temperature sensors are applicable only to vessels having a heat source.		

B.6.2.2.1 Pressure safety devices (PSH, PSL and PSV)

a) A pressure vessel that receives fluids from a well or from other sources that can cause overpressure should be protected by a PSH sensor to shut off inflow to the vessel. The PSH sensor need not be provided on the vessel if a PSH sensor on other process components will sense vessel pressure and shut off inflow to the vessel, and the PSH sensor cannot be isolated from the vessel; or if the vessel is the final scrubber in a flare, relief, or vent system and is designed to withstand maximum built-up back pressure; or if the vessel operates at atmospheric pressure and has an adequate vent system. A vessel receiving fluids from a well should always be protected by a PSH sensor because the pressure potential of a well may increase due to changes in reservoir conditions, artificial lift, workover activities, etc.

b) A pressure vessel should be provided with a PSL sensor to shut off inflow to the vessel when leaks large enough to reduce pressure occur, unless PSL sensors on other components will provide necessary protection and the PSL sensor cannot be isolated from the vessel when in service. A PSL sensor should not be installed if the vessel normally operates at atmospheric pressure or frequently varies to atmospheric while in service. In this case, the complexity of lockout devices to keep the vessel from shutting in during these operating modes could more than offset the protection afforded by the PSL sensor. In many cases a PSL will be incapable of detecting even severe leaks and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented.

c) A pressure vessel should always be protected by one or more PSVs with sufficient capacity to discharge maximum vessel input rates. At least one PSV should be set no higher than the maximum allowable working pressure of the vessel. API RP 521 [13] may be used as a guide in determining set pressures of multiple relief valve installations. A PSV need not be provided on a vessel if the vessel is the final scrubber in a flare, relief, or vent system; and is 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 element; and has no internal or external obstructions, such as mist extractors, back pressure valves, or flame arrestors. If obstructions exist, a PSV, or, as an alternative, a PSE should be installed to bypass the restriction. A PSV need not be provided on a vessel if PSVs on other process components provide adequate relief capacity, relieve at or below vessel maximum allowable working pressure, and cannot be isolated from the vessel when in service. If such PSVs are located on downstream components, they must not be isolated from the vessel at any time. Moreover, if upstream PSVs provide necessary protection when the vessel is in service, but can be isolated when the vessel is shut in, a PSV should be installed on the vessel for pressure relief due to thermal expansion or fire exposure.

   NOTE Some national standards allow a maximum accumulation of 10 %.

d) If a pressure vessel is subject to underpressure that could cause it to collapse, the vessel should be provided with a gas make-up system that will maintain adequate pressure in the vessel and a PSL sensor is required.

B.6.2.2.2 Level safety devices (LSH and LSL)

A pressure vessel that discharges to flare should be protected from liquid overflow by an LSH sensor to shut off inflow to the vessel. Vessels that do not discharge to flare should also be protected by an LSH sensor unless downstream process components can safely handle maximum liquids that could overflow. A pressure vessel should be protected from gas blowby by an LSL sensor to shut off inflow to the vessel or close the liquid outlet. The LSL sensor is not required if a liquid level is not maintained in the vessel during normal operation, or downstream equipment can safely handle gas that could blowby. An LSL sensor to shut off the fuel supply should be provided in a heated vessel if the heating element is immersed.

A second LSH may be required on vessels where the relief system is not designed for liquids.

Level devices are not required on pressure vessels that are not designed for liquid-gas separation or on small traps from which liquids are manually drained. This includes such vessels as pressure-surge bottles, desanders, gas volume bottles, gas-meter drip traps, fuel gas filters, etc.

B.6.2.2.3 Temperature safety devices (TSH)

If a pressure vessel is heated and the heat source can cause excessive temperature, a TSH sensor should be provided to shut off the source of heat when process fluid temperature becomes excessive.

B.6.2.2.4 Flow safety devices (FSV)

A check valve (FSV) should be installed in each gas and liquid discharge line if significant fluid volumes could backflow from downstream components in the event of a leak. An FSV is not required if a control device in the line will effectively minimize backflow. Whether backflow is significant is a judgement decision. If a line discharges to a pressure vessel at a point above the liquid level range, the backflow of liquids should be insignificant. Whether or not the gas volume is insignificant should depend on the size and pressure of the gas section and the conditions where a leak might occur.

B.6.3 Safety device location

B.6.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors and the PSV should be located to sense or relieve pressure from the gas or vapour section of the vessel. This is usually on or near the top. However, such devices may be located on the gas outlet piping if the pressure drop from the vessel to the sensing point is negligible and if the devices cannot be isolated from the vessel. Such isolation could be caused externally (e.g. by blocked valves on gas outlet) or internally (e.g. by plugged mist extractors).

B.6.3.2 Level safety devices (LSH and LSL)

The LSH sensor should be located a sufficient distance above the highest operating liquid level to prevent nuisance shutdowns, but with adequate vessel volume above the LSH sensor to prevent overflow before shutdown can be effected. The LSL sensor should be located a sufficient distance below the lowest operating liquid level to prevent nuisance shutdowns, but with adequate liquid volume between the LSL sensor and liquid outlet to prevent gas blowby before shutdown can be effected. In fire-tube heated components, the LSL should be located above the fire tubes. The LSH and LSL sensors should preferably be installed in external columns that can be isolated from the vessel. This will permit testing the devices without interrupting the process. However, if solid deposits or foam cause fouling or false indication of devices in external columns, the level sensors may be installed directly in the vessel. In this case, a pump may be required to manipulate vessel liquid level for testing.

B.6.3.3 Flow safety device (FSV)

Check valves (FSVs) should be located in outlet piping.

B.6.3.4 Temperature safety devices (TSH)

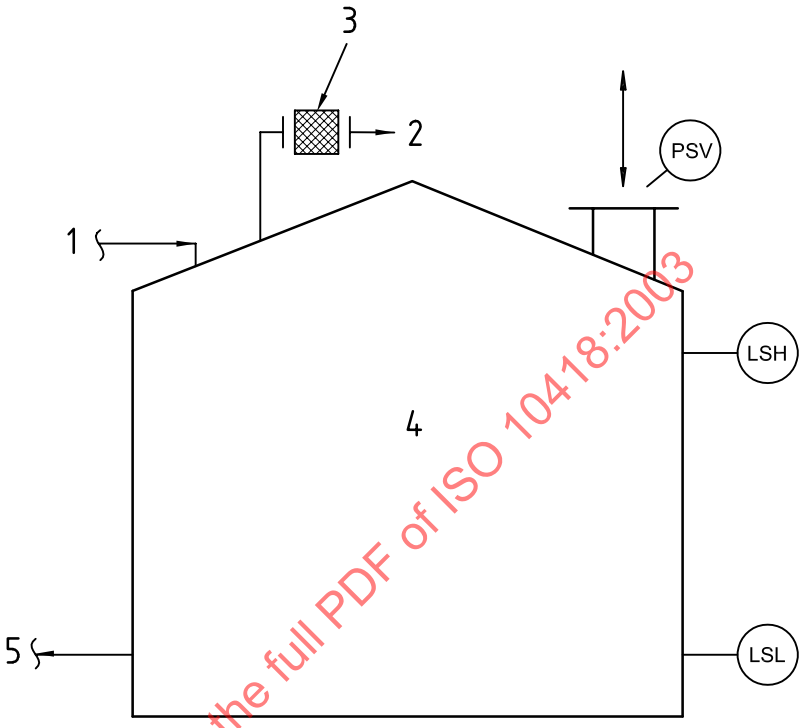
The TSH sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removing and testing. The thermowell should be located where it will be accessible and continuously immersed in the heated fluid.

B.7 Atmospheric pressure vessels

B.7.1 Description

Atmospheric pressure vessels are used for processing and temporary storage of liquid hydrocarbons. Some applications require heat input to the vessel. This discussion covers only the effects of heat input to the process section of an atmospheric pressure vessel. Heating equipment is covered in B.8 and B.12. If the atmospheric pressure vessel is heated, TSH should be installed. Recommended safety devices for typical atmospheric pressure vessels used in a production process system are shown in Figure B.7.

Vessels such as those used for diesel fuel and chemical storage that are ancillary to the production process system are not covered by this International Standard. However, some of the recommendations contained in D.2 concerning ESSs might be applicable when installing such equipment.



Key

1 inlet
2 vent
3 flame arrestor
4 atmospheric pressure vessel
5 outlet

NOTE 1 A vent line can contain a pressure and/or vacuum relief device.

NOTE 2 A second vent may be installed in lieu of the pressure and/or vacuum relief device.

Figure B.7 — Recommended safety devices — Atmospheric pressure vessels

B.7.2 Safety analysis

B.7.2.1 Safety analysis table

The SAT for atmospheric pressure vessels is presented in Table B.9. The undesirable events that can affect an atmospheric vessel are overpressure, underpressure, overflow, gas blowby, leak, and excess temperature if the vessel is heated.

Table B.9 — Safety analysis table (SAT) — Atmospheric pressure vessels

Undesirable event	Cause	Detectable condition at component
Overpressure	Inflow exceeds outflow Blocked outlet or vent Pressure control system failure Thermal expansion Gas blowby (upstream component)	High pressure
Underpressure	Withdrawals exceed inflow Thermal contraction	Low pressure
Liquid overflow	Liquid overflow Inflow exceeds outflow Blocked or restricted liquid outlet Level control system failure	High level
Gas blowby	Liquid withdrawals exceed inflow Open liquid outlet Level control system failure	Low level
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure and backflow or fire or gas accumulation
Excess temperature	Temperature control system failure High inlet temperature	High temperature

B.7.2.2 Safety analysis checklist (SAC) (see Table B.10)

B.7.2.2.1 Pressure safety devices (vent and PSV)

An atmospheric pressure vessel should be protected from overpressure and underpressure by an adequately sized vent system. API Std 2000[14] may be used as a guide for sizing vent systems. A flame arrestor should be included in the vent system to prevent flame migration back to the vessel. A pressure/vacuum relief device (PSV) or a second vent should be installed to protect the vessel in case the primary vent control device(s) fouls or otherwise obstructs flow. The PSV or second vent is not required when

a) a pressure vessel not subject to collapse is used in atmospheric service, or

b) an atmospheric vessel has no pressure sources (except blanket gas) piped to it.

A blanket gas system may be desirable to exclude air from an atmospheric vessel.

B.7.2.2.2 Level safety devices (LSH and LSL)

Protection from liquid overflow from an atmospheric pressure vessel should be provided by an LSH sensor to shut off inflow unless fill operations are continuously attended or overflow is diverted to other process components.

An LSL sensor should be provided to shut off the heat source if the vessel has an immersed heating element subject to excess temperature. If liquid level is not automatically maintained in the vessel, an LSL sensor should be provided to protect against leaks by shutting of inflow. A containment system to collect leakage is preferable to a low level sensor when normal inflow of liquids would preclude the sensor's detection of a leak.

B.7.2.2.3 Temperature safety devices (TSH)

If an atmospheric pressure vessel is heated, a TSH sensor should be provided to shut off the source of heat when process fluid temperature becomes excessive.

Table B.10 — Safety analysis checklist (SAC) — Atmospheric pressure vessels

SAC Ref. No.	Device SAFE (see Table B.9)	Checklist
a)	Vent [a]	Vent installed.
b)	PSV	1) PSV installed. 2) Vessel has second vent capable of handling maximum gas volume. 3) Component is a pressure vessel, not subject to collapse, that operates in atmospheric service and is equipped with an adequately sized vent. 4) Vessel has no pressure sources (except blanket gas and/or manual drains) and is equipped with an adequately sized vent.
c)	LSH	1) LSH installed. 2) Fill operations are continuously attended. 3) Overflow is diverted or contained by other process components.
d)	LSL	1) LSL installed. 2) Adequate containment system is provided. 3) Liquid level is not automatically maintained in the vessel, and vessel does not have an immersed heating element subject to excess temperature. 4) Component is final vessel in a containment system designed to collect and direct hydrocarbon liquids to a safe location.
e)	TSH [b]	1) TSH installed. 2) See Note. 3) Heat source is incapable of causing excess temperature.
NOTE This option was deleted from the original checklist in API RP 14C[8] when the second edition was published. The number reference is retained here to allow easy comparison of SAFE charts.		
[a] A vent is a pipe or fitting on a vessel that opens to atmosphere. A vent line might contain a pressure and/or vacuum relief device. [b] High temperature sensors are applicable only to vessels having a heat source.		

B.7.3 Safety device location

B.7.3.1 Pressure safety devices (vent and PSV)

The vent and PSV should be located on the top (highest practical elevation in the vapour section) of atmospheric vessels.

B.7.3.2 Level safety devices (LSH and LSL)

The LSH sensor should be located at a sufficient distance above the highest operating liquid level to prevent nuisance shutdowns, but with adequate vessel volume above the LSH sensor to contain liquid inflow during shut-in. The LSL should be located at a sufficient distance below the lowest operating liquid level to avoid nuisance shutdowns. In firetube heated components, the LSL should be located above the fire tubes. The LSH and LSL sensors should preferably be located in external columns for ease of testing without interrupting the process. However, internally mounted sensors are also acceptable, as discussed in B.6.3.2.

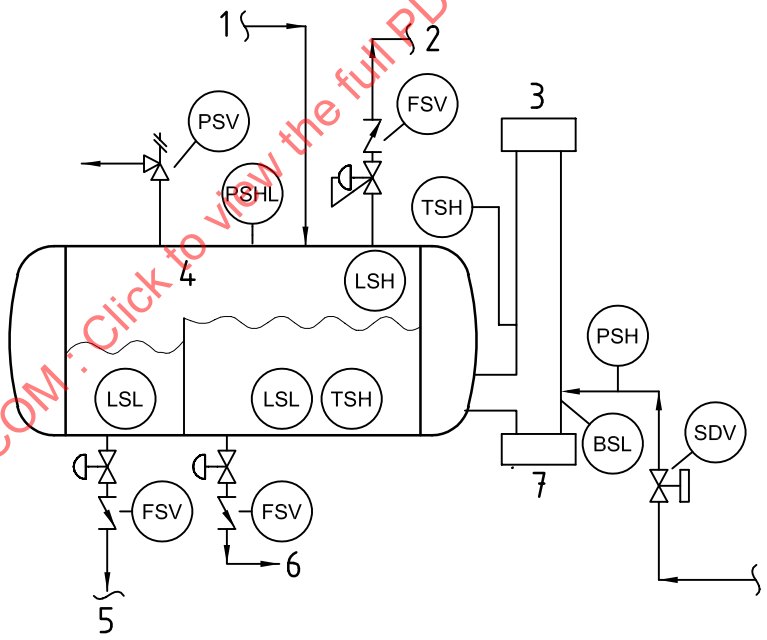
B.7.3.3 Temperature safety devices (TSH)

TSH sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

B.8 Fired and exhaust-heated components

B.8.1 Description

Fired and exhaust-heated components are used for processing and heating hydrocarbons. Included are both direct and indirect fired atmospheric and pressure vessels and tube-type heaters equipped with either automatically controlled natural or forced-draft burners. Also included are exhaust-heated components that use exhaust gases from other equipment such as turbines and engines as a heat source, and that may or may not be supplementary fired. This clause discusses the required protection for firing equipment of a fired component and for the heating section of exhaust-heated components. Protection for the process portion of a fired or exhaust-heated component is discussed under the appropriate component. Recommended safety devices for a typical fired vessel equipped with a natural-draft burner or a forced-draft burner are shown in Figures B.8 and B.9, respectively. Recommended safety devices for a typical exhaust-heated component are shown in Figure B.10.

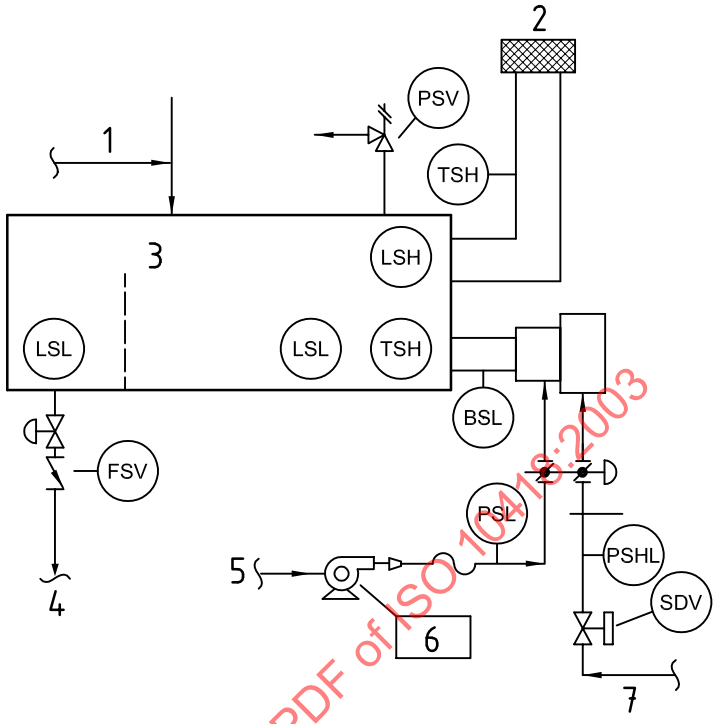


Key

1 inlet
2 gas outlet
3 stack arrestor
4 heater-treater
5 oil outlet
6 water outlet
7 flame arrestor

The vessel portion should be analysed in accordance with B.6 or B.7.

Figure B.8 — Recommended safety devices — Typical fired vessel (natural draft)



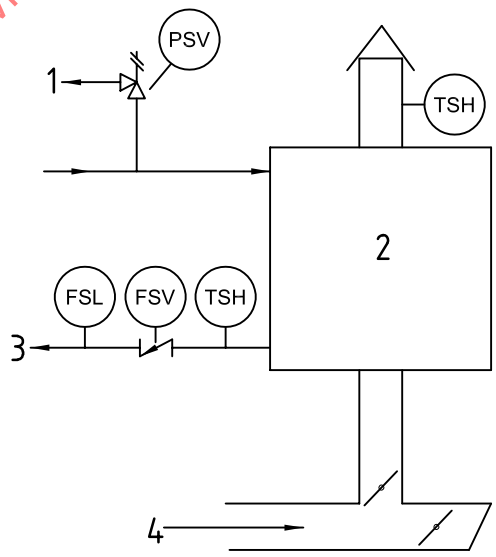
Key

1 glycol inlet
2 stack arrestor
3 glycol reboiler
4 glycol outlet
5 air inlet
6 motor interlock
7 fuel gas

The vessel portion should be analysed in accordance with B.6 or B.7.

NOTE The stack arrestor could be eliminated — see Table B.14, stack arrestor.

Figure B.9 — Recommended safety devices — Typical fired vessel (forced draft)



Key

1 medium inlet
2 exhaust-heated component
3 medium outlet
4 heat source (turbine exhaust, etc.)

Figure B.10 — Recommended safety devices — Exhaust-heated component

B.8.2 Safety analysis

B.8.2.1 Safety analysis table

The SAT for fired components with natural-draft burners is presented in Table B.11, for those with forced-draft burners in Table B.12, and for exhaust-heated components in Table B.13. The undesirable events that can affect a fired component or supplementary fired exhaust-heated component are excess temperature, direct ignition source, excess fuel in the firing chambers, and overpressure. The undesirable events that can affect an exhaust-heated component are excess temperature and overpressure.

Table B.11 — Safety analysis table (SAT) — Fired components (natural draft)

Undesirable event	Cause	Detectable condition at component
Excess temperature	Temperature control system fails Inadequate flow Limited heat transfer Ignition of medium leak into firing chamber Exposed heat transfer surface	High temperature (process) High temperature (stack) Low flow rate Low liquid level
Direct ignition source	Flame emission from air intake Spark emission from exhaust stack Excess stack temperature Exposed hot surface	Fire High temperature
Excess combustible vapours in firing chamber	Fuel control system failure	Flame failure High fuel pressure
Overpressure (flow tubes in firing chamber)	Blocked outlet Vaporization Thermal expansion	High pressure

Table B.12 — Safety analysis table (SAT) — Fired components (forced draft)

Undesirable event	Cause	Detectable condition at component
Excess temperature	Temperature control system fails Inadequate flow Limited heat transfer Ignition of medium leak into firing chamber Exposed heat transfer surface	High temperature Low flow High temperature High temperature High temperature
Direct ignition source	Flame emission from air intake Spark emission from exhaust stack Excess stack temperature Exposed hot surface	Fire High temperature stack
Excess combustible vapours in firing chamber	Fuel control system failure Air supply control system failure Blocked air inlet Blower failure	Low air pressure Flame failure High fuel pressure Low fuel pressure Low air velocity
Overpressure (flow tubes in firing chamber)	Blocked outlet Vaporization Thermal expansion	High pressure

Table B.13 — Safety analysis table (SAT) — Exhaust-heated components

Undesirable event	Cause	Detectable condition at component
Excess temperature	Temperature control system fails Inadequate flow Limited heat transfer Ignition of medium leak into firing chamber Exposed heat transfer surface	High temperature (medium) High temperature (stack) Low flow rate Low liquid level High temperature (process stack) Low liquid level
Overpressure (flow tubes in firing chamber)	Blocked outlet Vaporization Thermal expansion	High pressure
NOTE When supplemental firing is used, the component should also be analysed in accordance with Table B.11 or Table B.12, as applicable.		

B.8.2.2 Safety analysis checklist (SAC) (see Table B.14)

Table B.14 — Safety analysis checklist (SAC) — Fired and exhaust-heated components

SAC Ref. No.	Device SAFE (see Tables B.11, B.12, B.13)	Checklist
a)	TSH (medium or process fluid)	1) TSH installed. 2) Component is a steam generator protected by a PSH and, if fired, by an LSL. 3) Component is an indirect water-bath heater in atmospheric service and is protected by an LSL.
b)	TSH (stack)	1) TSH installed. 2) Component is isolated and does not handle combustible medium or process fluids other than fuel. 3) Component is exhaust-heated without supplemental firing and medium is not combustible.
c)	See Note.	—
d)	PSL (air supply)	1) PSL installed. 2) Component is equipped with a natural-draft burner. 3) Forced-draft burner is equipped with another type of low air supply sensor. 4) Component is exhaust-heated without supplemental firing.
e)	PSH (fuel supply)	1) PSH installed. 2) Component is exhaust-heated without supplemental firing.
f)	PSL (fuel supply)	1) PSL installed. 2) Component is equipped with a natural-draft burner. 3) Component is exhaust-heated without supplemental firing.
g)	BSL	1) BSL installed. 2) Component is exhaust-heated without supplemental firing.
h)	FSL (heated medium)	1) FSL installed. 2) Component is not a closed heat-transfer type in which a combustible medium flows through tubes located in the firing or exhaust-heated chamber.
i)	Motor interlock (forced-draft fan motor)	1) Motor interlock installed. 2) Component is equipped with a natural-draft burner. 3) Component is exhaust-heated without supplemental firing.
j)	Flame arrestor (air intake)	1) Flame arrestor installed. 2) Component is equipped with a forced-draft burner. 3) Component is located in an isolated area and not handling combustible medium or process fluids other than fuel. 4) Component is exhaust-heated without supplemental firing.
k)	Stack arrestor	1) Stack arrestor installed. 2) Component is equipped with a forced-draft burner and (1) the fluid being heated is non-flammable, or (2) the burner draft pressure at the exit of the transfer section is higher than the fluid pressure (head). 3) Component is isolated so process fluids will not contact stack emissions. 4) Component is exhaust-heated without supplemental firing.
l)	PSV (medium circulating tube)	1) PSV installed. 2) Component is not a tube-type heater. 3) PSV installed on another component will provide necessary protection and the PSV cannot be isolated from the tube section.
m)	FSV (medium circulating tube)	1) FSV installed on each outlet. 2) The maximum volume of combustible medium that could backflow from downstream equipment is insignificant, or medium is not combustible. 3) Component is not a tube-type heater.

NOTE This option was deleted from the original checklist in API RP 14C[8] when the second edition was published. The number reference is retained here to allow easy comparison of SAFE charts.

B.8.2.2.1 Temperature safety devices (TSH)

The medium or process fluid temperature in a fired component should be monitored by a TSH sensor to shut off the fuel supply and the inflow of combustible fluids. If a component is exhaust-heated, the exhaust should be diverted or the source of exhaust shut down. A TSH sensor is not necessary on a steam generator protected by a PSH sensor to detect high pressure caused by high temperature and by an LSL sensor to detect a low level condition that could cause high temperature. A TSH to sense medium or process fluid temperature is generally not necessary for an indirect water bath heater in atmospheric service, since the maximum temperature is limited by the boiling point of the water bath.

The flow of combustible medium in a closed heat-transfer system, where the medium is circulated through tubes located in the firing or exhaust-heated chamber, should not be shut off until the chamber has cooled. An ESD system and fire loop should immediately shut off medium flow if an uncontrolled fire has occurred in the area or the medium is escaping from a closed system.

Temperature in the burner exhaust stack should be monitored by a TSH sensor to shut off the fuel supply and the inflow of combustible fluids. Temperature in the exhaust-heated component stack should be monitored by a TSH sensor to shut off the inflow of combustible medium and to shut down the exhaust source. A TSH sensor is not required on a fired component located in an isolated area not handling combustibles other than fuel. A smoke detector (YSH) should be provided in the stack of glycol reboilers to detect any leakage of glycol into the fire tubes.

B.8.2.2.2 Flow safety devices (FSL and FSV)

If a combustible medium is circulated through tubes located in the firing or exhaust-heated chamber, the medium flow rate should be monitored by an FSL sensor to shut off the fuel supply to a fired component or to divert the exhaust flow from an exhaust-heated component. In this type of component, high temperature of the medium could occur before being detected by a TSH (medium) sensor located outside the heater. An FSL sensor is not required in other types of heater because the TSH (medium) sensor is located in the medium section and should immediately detect the high temperature condition. A check valve (FSV) should be located in tube outlet piping to prevent backflow into the fired or heated chamber in the event of tube rupture.

B.8.2.2.3 Pressure safety devices (PSH, PSL and PSV)

The pressure in the fuel supply line should be monitored by a PSH sensor to shut off the fuel supply to the burner. On a forced-draft burner, a PSL sensor should be installed on the fuel supply; in addition, the air intake pressure of a forced-draft burner should be monitored by a PSL sensor to shut off the fuel and air supply. A low air supply sensor may be used to monitor air supply in lieu of a PSL sensor. The PSL sensor is not required on a natural-draft burner because of the low air-intake pressure. Flow tubes located in the firing or exhaust-heated chamber of a tube type heater should be protected by a PSV from overpressure caused by expansion of the medium or process fluid.

B.8.2.2.4 Ignition safety devices

The air intake of a natural-draft burner should be equipped with a flame arrestor to prevent flame migration back through the air intake. A flame arrestor is not required on a forced-draft burner because the air velocity through the air intake prevents flame migration, or the PSL sensor in the air intake and fan motor starter interlock shut off the air intake.

The stack on a natural-draft burner should be equipped with a stack arrestor to prevent spark emission. If the fired component is not handling combustibles other than fuel and is located in an isolated area, the arrestor is not necessary. A stack arrestor may not be necessary on a forced-draft burner due to the higher combustion efficiency that prevents carbon build-up. A stack arrestor is required if the fluid being heated is flammable or the burner draft pressure at the exit of the transfer section is lower than the fluid pressure (head).

The motor on a forced-draft fan should be equipped with a motor starter interlock to sense motor failure and shut off the fuel and air supply.

The flame in the firing chamber should be monitored by a BSL or TSL sensor that will detect a flame insufficient to immediately ignite combustibles entering the firing chamber and will prevent fuel valves opening or shut off fuel supply.

Facilities should be installed to ensure fuel and air valves are opened and closed in the correct sequence.

B.8.3 Safety device location

B.8.3.1 Temperature safety devices (TSH)

Temperature sensors, other than fusible or skin contact types, should be installed in a thermowell for ease of removal and testing. If the fire tube is immersed, the TSH sensor should be located in the heated liquid medium or process fluid. If the liquid medium or process fluid flows through tubes within the firing or exhaust-heated chambers, the TSH sensor should be located in the discharge line as close as practical to the heater, and upstream of all isolating devices. A TSH sensor in the stack should be located near the base of the exhaust stack.

B.8.3.2 Flow safety devices (FSL and FSV)

In a closed heat-transfer system with a combustible medium, an FSL sensor should be located in the medium circulating tube piping. The sensor should be located in the medium outlet line as close to the heater as practical, and should monitor total flow through the heater. A check valve (FSV) should be installed in the tube outlet piping.

B.8.3.3 Pressure safety devices (PSH, PSL and PSV)

A PSL sensor in the air intake of a forced-draft burner should be located downstream of the blower. The PSH and PSL sensor in the fuel supply line should be located between the last pressure regulator and the fuel control valve. A PSV on the tubes of a tube-type heater should be located where it cannot be isolated from the heated section of the tubes.

B.8.3.4 Ignition safety devices

The flame and stack arrestors on fired components should be located to prevent flame emission from the air intake and spark emission from the exhaust stack. The BSL sensor should be located in the firing chamber.

B.8.4 Safe operating procedures

In addition to the safety devices indicated in Table B.14, the procedures shown in Table B.15 are required to safely operate a fired or exhaust-heated component.

Table B.15 — Safe operating procedures for fired or exhaust-heated components

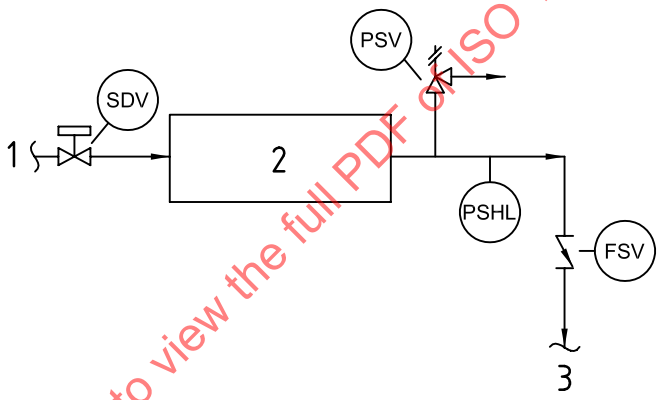
Step	Action
1	Assure complete fuel shut off.
2	Void firing chamber of excess combustibles prior to pilot ignition.
3	Limit time on trial for ignition of pilot and main burner to prevent excess fuel accumulation in fire chamber. After the time limit is exceeded, the fuel should be shut off and a manual reset start-up required.
4	Prove pilot and assure fuel-air proportioning dampers and burner controls are in low fire position prior to opening fuel supply to main burner.
5	Manually reset start-up controls following a flame failure of either the pilot or main burner.
6	Assure fuel is clean from all residue and foreign materials by providing adequate fuel-cleaning equipment.
7	Assure that exhaust is diverted around exhaust-heated component prior to starting up heat source, if applicable.

B.9 Pumps

B.9.1 Description

Pumps transfer liquids within the production process and into pipelines leaving the platform, or from the containment system to the process system (booster/charge pumps, sump pumps, chemical injection pumps, heating pumps). Pipeline pumps transfer produced hydrocarbons from the process system to a pipeline. Pumps that occasionally transfer small volumes of hydrocarbons from ancillary equipment (swab tanks, sumps, etc.) to a pipeline that receives the bulk of its volume from another source are not considered pipeline pumps. Glycol-powered glycol pumps circulate glycol within a closed system. Other pumps transfer produced liquids, heat-transfer liquids, or chemicals within the production process system, or from the containment system to the process system (booster/charge pumps, sump pumps, chemical injection pumps, heating-medium circulating pumps, glycol pumps, etc.). Recommended safety devices for typical pump installations are shown in Figures B.11, B.12 and B.13.

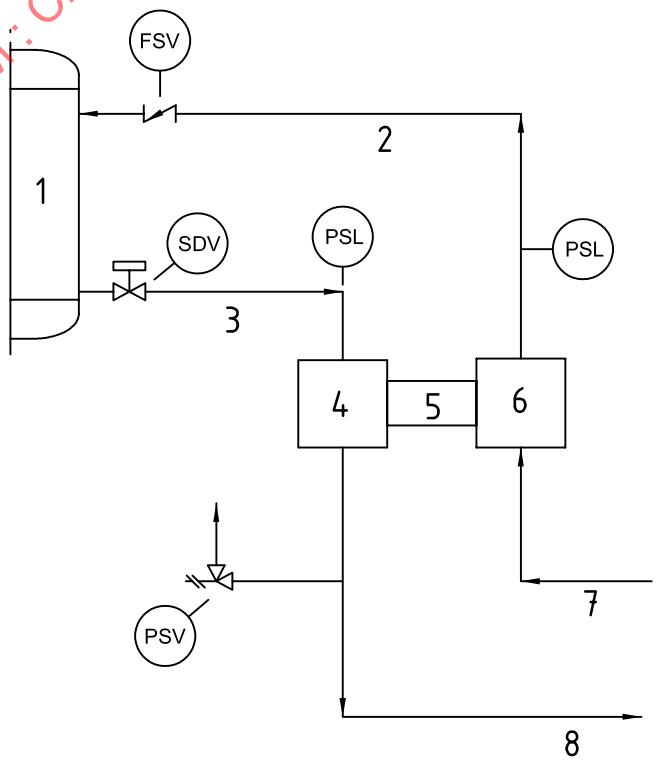
The recommendations of this clause do not apply to firewater pumps; in these cases the requirements of ISO 13702 apply.



Key

1 from storage component
2 pump
3 discharge

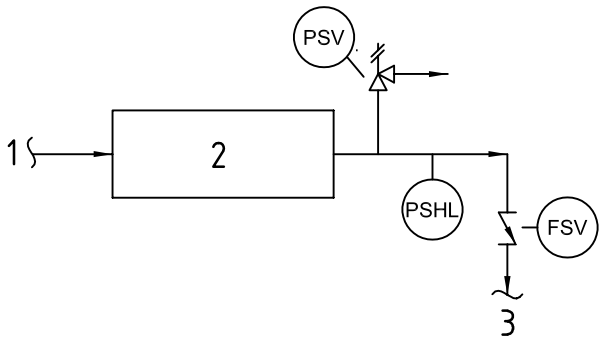
Figure B.11 — Recommended safety devices — Pipeline pumps



Key

1 glycol contactor
2 dry glycol to contactor
3 wet glycol from contactor
4 power end
5 pump
6 pump end
7 dry glycol from reboiler
8 wet glycol to reboiler

Figure B.12 — Recommended safety devices — Glycol-powered glycol pumps



Key

1 suction
2 pump
3 discharge

Figure B.13 — Recommended safety devices — Other pumps

B.9.2 Safety analysis

B.9.2.1 Safety analysis table

The SAT for pumps is presented in Table B.16. The undesirable events that can affect a pump are overpressure, leak, excess temperature and low flow.

Table B.16 — Safety analysis table (SAT) — Pumps

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Excess back pressure High inlet pressure (centrifugal) Overspeed Fluid density increase Reverse flow	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature
Low flow	Blocked or restricted outlet or inlet	Low flow

B.9.2.2 Safety analysis checklist (SAC) (see Table B.17)

Table B.17 — Safety analysis checklist (SAC) — Pumps

SAC Ref. No.	Device SAFE (see Table B.16)	Checklist
a)	PSH — Pipeline pumps	PSH installed.
b)	PSH — Other pumps	1) PSH installed. 2) Maximum pump discharge pressure does not exceed 70 % of the maximum allowable working pressure of the discharge piping. 3) Pump is manually operated and continuously attended. 4) Small, low volume pumps, e.g. chemical injection. 5) Pump discharges to an atmospheric pressure vessel. 6) Pump is a glycol-powered glycol pump.
c)	PSL — Pipeline pumps	1) PSL installed. 2) Pump does not handle hydrocarbons. 3) ESS is capable of detecting fire and gas accumulation such that the likelihood of escalation is minimized.
d)	PSL — Other pumps	1) PSL installed. 2) Pump is manually operated and continuously attended. 3) Adequate containment is provided. 4) Small, low volume pumps, e.g. chemical injection pumps. 5) Pump discharges to an atmospheric vessel. 6) ESS is capable of detecting fire and gas accumulation such that the likelihood of escalation is minimized.
e)	PSV — Pipeline pumps	1) PSV installed. 2) Pump is kinetic energy type and incapable of generating a head greater than the maximum allowable working pressure of the discharge piping.
f)	PSV — Other pumps	1) PSV installed. 2) Maximum pump discharge pressure is less than the maximum allowable working pressure of discharge piping. 3) Pump has internal pressure relief capability. 4) Pump is a glycol-powered glycol pump, and the wet glycol low-pressure discharge piping is rated higher than the maximum discharge pressure. 5) Pump is a glycol-powered glycol pump, and the wet glycol low-pressure discharge piping is protected by a PSV on a downstream component that cannot be isolated from the pump.
g)	FSV — All pumps	Check valve installed.
h)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
i)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.
j)	FSL	1) FSL installed. 2) Pump curve is such that the PSH installed is capable of detecting blocked outlet and PSL installed is capable of detecting blocked inlet 3) Pump is not damaged by low flow.

B.9.2.2.1 Pressure safety devices (PSH, PSL and PSV)

PSH and PSL sensors should be provided on all hydrocarbon pipeline pump discharge lines to shut off inflow and shut down the pump. A PSH sensor to shut down the pump should be provided on the discharge line of other pumps, unless the maximum pump discharge pressure does not exceed 70 % of the maximum allowable working pressure of the discharge line, or the pump is manually operated and continuously attended. A PSH sensor is not required on glycol-powered glycol pumps. Other hydrocarbon pumps should also be provided with a PSL sensor to shut down the pump, unless the pump is manually operated and continuously attended or adequate containment is provided. PSL sensors should be provided on glycol-powered glycol pumps to shut off wet glycol flow to the pump. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented.

A PSV should be provided on all pipeline pump discharge lines, unless the pump is a kinetic energy type, such as a centrifugal pump, and is incapable of generating a head greater than the maximum allowable working pressure of the discharge piping. A PSV should be provided in the discharge line of all other pumps unless the maximum pump discharge pressure is less than the maximum allowable working pressure of the line, or the pump has an internal pressure relief capability. A PSV should be provided in the wet glycol low pressure discharge line of glycol-powered glycol pumps unless the line is rated higher than the maximum pump discharge pressure or is protected by a PSV on a downstream component that cannot be isolated from the pump.

B.9.2.2.2 Flow safety devices (FSV)

A check valve (FSV) should be provided in the pump discharge line to minimize backflow.

B.9.2.3 Temperature safety devices (TSH and TSL)

A temperature safety device is only required if fluid temperatures during fault conditions can cause design limits of the piping to be exceeded. Low temperatures can be caused by gas pressure drops or active cooling. High temperatures can be caused by fluid conditions or active heating.

B.9.2.4 Flow safety low (FSL)

A low-flow safety device (flow safety low) is only required if damage can result from low flow and the pump characteristic is such that the pressure safety devices (pressure safety low and pressure safety high) will not detect abnormal condition.

B.9.3 Safety device recommended locations

B.9.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors should be located on the pump discharge line upstream of the FSV or any block valve. In a glycol-powered glycol pump, the PSL on the wet glycol high pressure line should be located between the pump and the SDV. On pipeline pumps and other pumps where it is required, the PSV should be located on the discharge line upstream of any block valve.

B.9.3.2 Flow safety devices (FSV)

The check valve (FSV) should be located on the pump discharge line to minimize backflow.

B.9.3.3 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

B.9.3.4 Flow safety low (FSL)

The FSL should be located in the pump discharge line upstream of any FSV or any block valve.

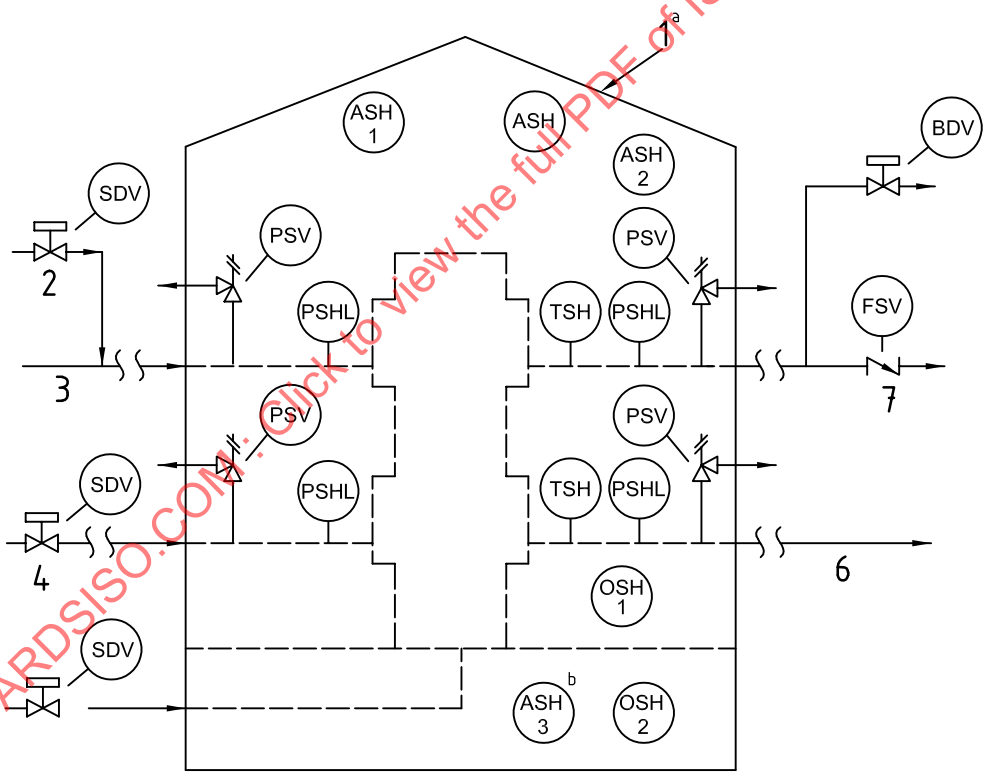
B.9.3.5 Shutdown devices (SDV)

An SDV should be located near the outlet of a storage component (tank, separator, etc.) that delivers product to a pipeline pump, to prevent the flow of hydrocarbons through the pipeline pump and into the pipeline in the event of a pipeline leak. If glycol-powered pumps are used, an SDV should be located near the high pressure wet glycol outlet of the glycol contactor to shut off flow from the contactor and to shut down the pumps.

B.10 Compressor units

B.10.1 Description

Compressor units transfer hydrocarbon gases within the production process and into pipelines leaving the platform. Recommended safety devices for a typical compressor unit are shown in Figure B.14.



Key

1 enclosure (optional)
2 external process inflow
3 intermediate suction
4 1st stage suction
5 fuel
6 intermediate discharge to next stage
7 final discharge

NOTE 1 Suction scrubbers are not shown; they should be analysed according to B.6. Shell-tube type discharge coolers are not shown; they should be analysed according to B.12.

NOTE 2 OSH should be considered based on the conditions stated in F.1 and F.2.

[a] ASH 1, 2 and OSH 1, 2 are not required if compressor is not installed in an enclosed building.

[b] ASH 3 is not required if compressor does not have piping or other potential source of gas leak below a solid subfloor.

Figure B.14 — Recommended safety devices — Compressor unit

B.10.2 Safety analysis

B.10.2.1 Safety analysis table

The SAT for compressor units is presented in Table B.18. The SAT analyses the compressor cylinder or case and the suction, discharge and fuel gas piping of a compressor unit. Hydrocarbon-handling equipment associated with compressors, other than compressor cylinders or cases, should be protected in accordance with appropriate clauses of this International Standard. The compressor and prime mover are normally furnished with devices to prevent mechanical damage. The undesirable events that can affect a compressor unit are overpressure, leak, excess temperature and surge.

Table B.18 — Safety analysis table (SAT) — Compressors

Undesirable event	Cause	Detectable condition at component
Overpressure (suction)	Excess inflow Failure of suction pressure control system Compressor or driver malfunction Reverse flow	High pressure
Overpressure (discharge)	Blocked or restricted discharge line Excess back pressure High inlet pressure Overspeed Fluid density increase	High pressure High gas concentration
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure and backflow or gas or fire
Excess temperature	Compressor valve failure Cooler failure Excess compression ratio Insufficient flow Excess recycle of gas at high pressure drop resulting in pipe embrittlement	High temperature Low temperature
Surge	Blocked or restricted discharge line Cooler failure Insufficient flow Compressor or driver malfunction Fluid density change	Variable computed from measurements approaches surge line

B.10.2.2 Safety analysis checklist (SAC) (see Table B.19)

Table B.19 — Safety analysis checklist (SAC) — Compressors

SAC Ref. No.	Device SAFE (see Table B.18)	Checklist
a)	PSH (suction)	1) PSH installed. 2) Each input source is protected by a PSH that will also protect the compressor.
b)	PSH (discharge)	1) PSH installed. 2) Compressor is protected by a downstream PSH, located upstream of any cooler, that cannot be isolated from the compressor.
c)	PSL (suction)	1) PSL installed. 2) Each input source is protected by a PSL that will also protect the compressor. 3) ESS is capable of detecting fire and gas occurrences such that the likelihood of escalation is minimized.
d)	PSL (discharge)	1) PSL installed. 2) Compressor is protected by a downstream PSL that cannot be isolated from the compressor. 3) ESS is capable of detecting fire and gas occurrence such that the likelihood of escalation is minimized.
e)	PSV (suction)	1) PSV installed. 2) Each input source is protected by a PSV that will also protect the compressor.
f)	PSV (discharge)	1) PSV installed. 2) Compressor is protected by a downstream PSV, located upstream of any cooler, that cannot be isolated from the compressor. 3) Compressor is kinetic energy type and incapable of generating a pressure greater than the maximum allowable working pressure of the compressor or discharge piping.
g)	FSV (final discharge)	FSV installed.
h)	TSH	TSH installed.
i)	YSH (surge protection)	1) Surge protection scheme installed. 2) Compressor will not surge under failure conditions.
j)	TSL	1) TSL installed. 2) Excess recycle of gas will not cause pipe embrittlement.

B.10.2.2.1 Pressure safety devices (PSH, PSL and PSV)

PSH and PSL sensors should be provided on each suction line of a compressor unit unless each input source is protected by PSH and PSL sensors that will also protect the compressor. Also, PSH and PSL sensors should be provided on each compressor discharge line. The PSH and PSL sensors should shut off all process inflow and fuel gas to the compressor. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented. A PSV should be provided on each compressor suction line, unless each input source is protected by a PSV that will protect the compressor. A PSV should be provided on each compressor discharge line. A PSV is not necessary on the discharge of a kinetic energy type compressor if the compressor is incapable of developing a pressure greater than the maximum allowable working pressure of the compressor or discharge piping.

B.10.2.2.2 Flow safety devices (FSV)

A check valve (FSV) should be provided in each final discharge line to minimize backflow.

B.10.2.2.3 Gas-detecting devices (ASH/OSH)

If a compressor unit is installed in an inadequately ventilated building or enclosure, gas detectors (ASHs and/or OSHs) should be provided to shut off all process inflow and fuel gas to the compressor and blowdown the compressor.

B.10.2.2.4 Temperature safety devices (TSH and TSL)

A TSH sensor should be provided to protect each compressor cylinder or case. The TSH sensor should shut off all process inflow and fuel gas to the compressor. A TSL sensor should be provided, unless excess recycle of gas will not cause pipe embrittlement.

B.10.2.2.5 Surge-prevention devices (YSH)

Measurement, computing and actuation devices should be provided to protect the compressor against surge conditions.

B.10.3 Safety device location

B.10.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors should be located on each suction line as close to the compressor as practical, recognizing the detrimental effects of vibration and pulsation on equipment function and lifetime, and on each discharge line upstream of the FSV and any block valve. The PSVs should be located on each suction line as close to the compressor as practical, recognizing the detrimental effects of vibration and pulsation on equipment function and lifetime, and on each discharge line so that the PSV cannot be isolated from the compressor. If a PSV is located inside a building, its discharge outlet should be piped to a safe location outside the building.

B.10.3.2 Flow safety devices (FSV)

A check valve (FSV) should be located on the final discharge line of each compressor unit to minimize backflow. If the compressor unit is inside a building, the FSV should be located outside the building.

B.10.3.3 Gas-detecting devices (ASH/OSH)

Should the compressor unit be installed in an inadequately ventilated building or enclosure, gas detectors (ASHs and/or OSHs) should be located in areas where combustible and/or toxic gases can accumulate.

B.10.3.4 Temperature safety devices (TSH and TSL)

A TSH sensor should be located in the discharge piping of each compressor cylinder or case, as close as practical to the cylinder or case. A TSL should be provided on the recycle line.

B.10.3.5 Surge detection devices

Sensors to measure flow, temperature, density and pressure should be located to enable the onset of surge to be predicted and prevented.

B.10.3.6 Shutdown devices (SDV)

An SDV should be located on each process inflow line and fuel gas line, so that the compressor can be isolated from all input sources. If the compressor unit is installed in a building, SDVs should be located outside the building. All SDVs should be actuated by a signal from the ESD system and fire loop, and by any abnormal pressure condition sensed in the suction and discharge lines. A blowdown valve should be located on the final discharge line(s) of the compressor unit. The blowdown valve(s) may be actuated by a signal from the compressor's fire loop, gas detectors and compressor ESD system.

B.11 Pipelines

B.11.1 Description

Offshore pipelines direct liquids and gases between platforms or between a platform and a shore facility. Pipelines are classified as (a) incoming, (b) departing, or (c) bidirectional, depending on the direction of flow at the platform. An incoming pipeline directs fluids onto the platform, and a departing pipeline transports fluids from the platform. A bidirectional pipeline can transport fluids in either direction.

Pipelines can be further classified according to the delivery or receiving point as follows:

a) incoming pipelines:

   1) deliver to platform facilities;

   2) deliver to departing pipeline.

b) departing pipelines:

   1) receive from platform facilities;

   2) receive from incoming pipeline(s);

   3) receive from both platform facilities and incoming pipeline(s).

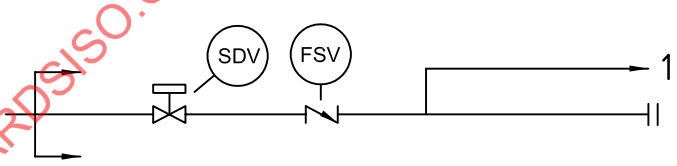
c) bidirectional pipelines:

   1) deliver to and receive from platform facilities;

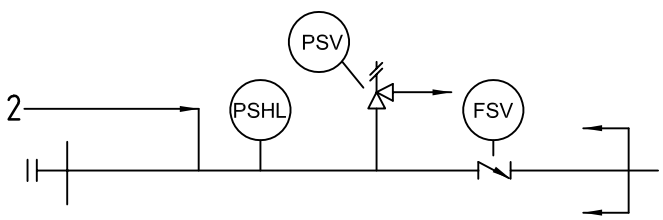
   2) deliver to and receive from another bidirectional pipeline;

   3) deliver to and receive from other bidirectional pipelines and receives from platform facilities.

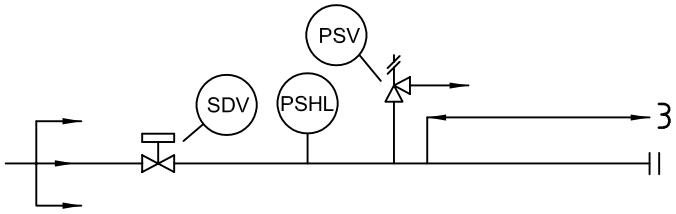
Recommended safety devices for typical pipelines are shown in Figure B.15.



a) Incoming pipeline



b) Departing pipeline



c) Bidirectional pipeline

Key

1 to process station or departing pipeline
2 from process station or incoming pipeline
3 to and from process station or bidirectional pipeline

Denotes platform limits

Figure B.15 — Recommended safety devices — Pipelines

B.11.2 Safety analysis

B.11.2.1 Safety analysis table

The SAT for pipelines is presented in Table B.20. The undesirable events that can affect a pipeline are overpressure, leak and excess temperature.

Table B.20 — Safety analysis table (SAT) — Pipelines

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Thermal expansion Inflow exceeds outflow	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure and backflow or gas or fire
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature

B.11.2.2 Safety analysis checklist (SAC) (see Table B.21)

Table B.21 — Safety analysis checklist (SAC) — Pipelines

SAC Ref. No.	Device SAFE (see Table B.20)	Checklist
a)	PSH	1) PSH installed. 2) Delivering pipeline protected by PSH located on upstream component. 3) Each input source is protected by a PSH that also protects a departing or bidirectional pipeline. 4) The pipeline is protected by a PSH located on a parallel component.
b)	PSL	1) PSL installed. 2) Delivering pipeline protected by PSL located on upstream component. 3) Each input source is protected by a PSL that also protects a departing or bidirectional pipeline. 4) The pipeline is protected by a PSL located on a parallel component. 5) ESS is capable of detecting fire and gas occurrences such that the likelihood of escalation is minimized.
c)	PSV	1) PSV installed. 2) Pipeline has a maximum allowable operating pressure greater than the maximum pressure of any input source. 3) Each input source having a pressure greater than the maximum allowable operating pressure of the pipeline is protected by a PSV set no higher than the maximum allowable operating pressure of the pipeline. 4) The pipeline does not receive input from the platform process. 5) Input source(s) having a pressure greater than the maximum allowable operating pressure of the pipeline are equipped with two SDVs (one of which may be the SSV/USV if sources are wells) controlled by independent PSHs designed in accordance with IEC 61511-1.
d)	FSV	1) FSV installed. 2) Departing pipeline is equipped with an SDV controlled by a PSL designed in accordance with IEC 61511-1. 3) Each input source is protected by an FSV located so that no significant length of pipeline is unprotected from backflow. 4) Pipeline is used for bidirectional flow.
e)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
f)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.

B.11.2.2.1 Pressure safety devices (PSH, PSL and PSV)

PSH and PSL sensors are required on departing pipelines to shut off all input sources. PSH and PSL sensors are not provided on an incoming pipeline that is protected by sensors provided at the upstream platform. Bidirectional pipelines should be provided with PSH and PSL sensors. Protection may be provided by PSH and PSL sensors located at each input source or on a parallel component (looped pipeline) if the sensors cannot be isolated from the pipeline. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented. Alternative systems to detect leakage in pipelines include systems which measure and compare inlet and outlet flows.

Each pipeline input source is normally protected by a PSV set also to protect the pipeline. A PSV is not required if

— the pipeline has a maximum allowable operating pressure greater than the maximum pressure of any input source;

— each input source having a pressure greater than the pipeline's maximum allowable operating pressure is protected by a PSV set no higher than the pipeline's maximum allowable operating pressure; or

— input source is a well(s) having a pressure greater than the pipeline's maximum allowable operating pressure and is equipped with two SDVs (one of which may be the SSV) controlled by independent PSHs connected to separate relays and sensing points. The use of two SDVs in lieu of a PSV should be approached with caution after thorough consideration of other alternatives. In some cases, installation of a PSV in addition to two SDVs might be desirable even at locations having no containment system.

B.11.2.2.2 Flow safety devices (FSV)

An FSV is provided on an incoming pipeline to minimize backflow to a leak or rupture in the pipeline, and on a departing pipeline to minimize backflow to a leak or rupture in a component on the platform. If an incoming pipeline connects only to a departing pipeline, the FSV on the departing pipeline also protects the incoming pipeline. An FSV may be eliminated on a departing pipeline if all input sources are equipped with FSVs located so that no significant length of piping is unprotected from backflow from the pipeline. An FSV cannot be installed on a bidirectional pipeline.

B.11.2.2.3 Temperature safety devices (TSH and TSL)

A temperature safety device is required only if fluid temperatures during fault conditions can cause design limits of the piping to be exceeded. Low temperatures can be caused by gas pressure drops or active cooling. High temperatures can be caused by fluid conditions or active heating.

B.11.3 Safety device location

B.11.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors should be located downstream of any platform input source and upstream of a departing pipeline FSV. If a PSV is required, it should be located downstream of all input sources and installed so that it cannot be isolated from inlet sources.

B.11.3.2 Flow safety devices (FSV)

Incoming pipelines delivering to a platform process station should have an FSV located immediately upstream from the process station. The FSV on a departing pipeline should be located as far downstream as practical, but upstream of a block valve.

B.11.3.3 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

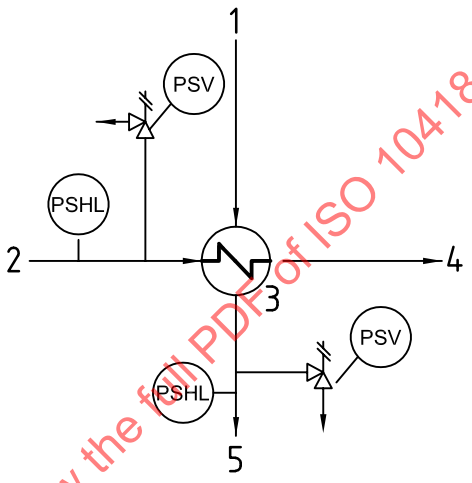
B.11.3.4 Shutdown devices (SDV)

Pipeline SDVs should be located to minimize the portion of pipeline exposed on the platform. All SDVs should be actuated by the platform ESD system, fire loop, and sensors on any downstream component through which the pipeline fluids flow. The SDV on a pipeline delivering to a departing pipeline should be actuated by the departing pipeline's PSH and PSL sensors, the ESD system, and the fire loop. Bidirectional pipelines should be equipped with SDVs on each platform terminus.

B.12 Heat exchangers

B.12.1 Description

Heat exchangers transfer thermal energy from one flow stream to another while maintaining isolation of the two flow streams. Recommended safety devices for a typical heat exchanger are shown in Figure B.16. This clause does not apply to exchangers used with primary heat sources such as turbine exhaust exchangers that should be analysed under B.8. This clause may be used to analyse heating or cooling coils inserted into vessels, but the vessels themselves should be analysed under B.6 or B.7, as appropriate. This clause may also be used to analyse heat exchangers using air to cool or heat hydrocarbons, in which case only the hydrocarbon section need be considered.



Key

1 heat medium in
2 process fluid in
3 heat exchanger
4 process fluid out
5 heat medium out

Figure B.16 — Recommended safety devices — Heat exchangers (shell-tube)

B.12.2 Safety analysis

B.12.2.1 Safety analysis table

The SAT for heat exchangers is presented in Table B.22. The undesirable events that can affect a heat exchanger are overpressure, underpressure, leak and excess temperature.

Table B.22 — Safety analysis table (SAT) — Heat exchangers

Undesirable event	Cause	Detectable condition at component
Overpressure	Blocked or restricted outlet Tube leak Vaporisation Thermal expansion Inflow exceeds outflow	High pressure
Leak	Deterioration Erosion Corrosion Impact damage Vibration Vacuum collapse	Low pressure and backflow or gas or fire
Underpressure	Withdrawals exceed inflow Thermal contraction Open outlet Pressure control system failure	Low pressure
Excess temperature	High fluid temperature Gas pressure drop	High temperature Low temperature

B.12.2.2 Safety analysis checklist (SAC) (see Table B.23)

Table B.23 — Safety analysis checklist (SAC) — Heat exchangers

SAC Ref. No.	Device SAFE (see Table B.22)	Checklist
a)	PSH	1) PSH installed. 2) Input source to heat-exchanger section cannot develop pressure greater than the maximum allowable working pressure of the heat-exchanger section. 3) Each input source is protected by a PSH that also protects the heat-exchanger section. 4) A PSH is installed on a downstream component and cannot be isolated from the heat-exchanger section by block or regulating valves.
b)	PSL	1) PSL installed. 2) Minimum operating pressure is atmospheric pressure when in service. 3) PSL installed on another component will provide necessary protection and the PSL cannot be isolated from the heat-exchanger section when the heat exchanger is in service. 4) ESS is capable of detecting fire and gas occurrences such that the likelihood of escalation is minimized.
c)	PSV	1) PSV installed [a]. 2) Each input source is protected by a PSV that is set no higher than the maximum allowable working pressure of the heat-exchanger section and a PSV is installed on the heat-exchanger section for fire exposure and thermal relief. 3) Each input source is protected by a PSV that is set no higher than the maximum allowable working pressure of the heat-exchanger section and that cannot be isolated from the heat-exchanger section. 4) PSVs on downstream equipment can satisfy the relief requirement of the heat-exchanger section and cannot be isolated from the heat-exchanger section. 5) See Note. 6) Input sources to the heat exchanger section cannot develop pressure greater that the maximum allowable working pressure of the heat-exchanger section, and the heat-exchanger section cannot be overpressured due to temperature or pressure in the other section. 7) Input sources to the heat-exchanger section cannot develop pressure greater than the maximum allowable working pressure of the heat-exchanger section and a PSV is installed on the heat-exchanger section for fire exposure and thermal relief.
d)	TSH	1) TSH installed. 2) Fluid temperature does not cause design limits of piping to be exceeded.
e)	TSL	1) TSL installed. 2) Gas pressure drop does not cause design limits of piping to be exceeded.
NOTE This option was deleted from the original checklist in API RP 14C[8] when the second edition was published. The number reference is retained here to allow easy comparison of SAFE charts.		
[a] For some heat exchangers, overpressure protection requires fast-acting bursting discs rather than relief valves. To be effective, such devices need to be located adjacent to the unit.		

B.12.2.2.1 Pressure safety devices (PSH, PSL and PSV)

In analysing heat exchangers for pressure safety devices, both sections (the heat-receiving section and the heat-input section) should be analysed separately, since each section may have different design and operating pressure requirements. A section of a heat exchanger that receives fluids from a source that can cause overpressure should be protected by a PSH sensor to shut off inflow of the source to that section of the heat exchanger. Also, a section of the heat exchanger that could be overpressurized because of a rupture or leak of another section of the heat exchanger should be protected by a PSH sensor to shut off inflow of the source of overpressure to that section. The PSH sensor need not be provided for a section of a heat

exchanger if an upstream PSH sensor on other process components will sense the pressure in the heat-exchanger section and shut off inflow to the heat exchanger, or if a downstream PSH sensor will sense pressure in the heat-exchanger section and cannot be isolated. Also, the PSH sensor need not be provided on a section of a heat exchanger, if the maximum allowable working pressure of that section is greater than the potential pressure of any input source to that section.

A heat-exchanger section containing hydrocarbons should be provided with a PSL sensor to shut off inflow to the heat exchanger when leaks large enough to reduce pressure occur, unless PSL sensors on other components will provide necessary protection and the PSL sensor cannot be isolated from the heat-exchanger section when in service. A PSL sensor should not be installed if the heat-exchanger section normally operates at atmospheric pressure or frequently varies to atmospheric pressure while in service. In this case, the complexity of lockout devices to keep the heat exchanger from shutting in during these operating modes could more than offset the protection afforded by the PSL sensor. In many cases a PSL will be incapable of detecting even severe leaks, and need not be provided if it can be shown that the ESS is capable of detecting fire and gas occurrences such that escalation can be prevented.

A heat-exchanger section should be provided with a PSV with sufficient capacity to discharge maximum input rates. A PSV need not be provided on a heat-exchanger section if PSVs on other process components provide adequate relief capacity, relieve at or below heat-exchanger section working pressure, and cannot be isolated from the section when in service. If such PSVs are located on downstream components, they should not be isolated from the heat-exchanger section at any time. Also, the PSV need not be provided on a section of a heat exchanger, if the maximum allowable working pressure of that section is greater than the potential pressure of any input source to that section. Moreover, if PSVs on other components provide necessary protection when the heat-exchanger section is in service, but can be isolated when the heat-exchanger section is shut in, a PSV should be installed on the heat-exchanger section for pressure relief due to thermal expansion or fire exposure.

B.12.2.2.2 Temperature safety devices (TSH)

A TSH is not generally required in an exchanger because both sections are normally rated for the maximum temperature of the heat medium.

B.12.3 Safety device location

B.12.3.1 Pressure safety devices (PSH, PSL and PSV)

The PSH and PSL sensors and the PSV should be located to sense pressure in or relieve it from each section of the heat exchanger. Such devices may be located in the inlet or outlet piping if the pressure drop from the heat-exchanger section to the sensing point is negligible and if the devices cannot be isolated from the heat-exchanger section. It should be noted that if a PSV is located a distance from the low pressure side of the exchanger then if, the shell is liquid filled (non-compressible fluid) a high pressure can be generated in the low pressure shell before the remote PSV will operate. The time delay in response due to remote location of the overpressure protection devices should be considered and assessed as part of the safety analysis.

B.12.3.2 Temperature safety devices (TSH and TSL)

The TSH and TSL sensors, other than fusible or skin contact types, should be installed in thermowells for ease of removal and testing. The thermowell should be located for accessibility and should be continuously immersed in the process fluid.

Annex C
(informative)

Examples of safety analysis flow diagram and safety analysis function evaluation (SAFE) chart

C.1 General

Figure C.1 shows the format of a safety analysis function evaluation. Figure C.2 shows an example of a flow diagram of a platform production process, for illustrative purposes only. Figure C.3 presents completed SAFE charts for the process components in the flow diagram shown in Figure C.2. Each process component is listed on the SAFE chart with its recommended safety devices determined from the individual components analysis (see Annex B). Each shutdown and safety function is also listed. For each safety device, a specific shutdown and/or safety function(s), or a SAC reference (see Annex B) should be documented on the SAFE chart. Provisions are also made for documenting alternative or substitute safety devices used in lieu of recommended safety devices.

C.2 Natural-draft burner on a heater treater pressure vessel

C.2.1 General

To analyse this combination, it is necessary to refer to B.6 for the pressure vessel and B.8 for the fired component.

Draw a simplified diagram with all required safety devices in accordance with B.6 and B.8 (see Figure C.4).

It is suggested that the component identifications (see Table A.1) for both the vessel and the fired component have the same component identifier (e.g. XXX-2000, YYY-2000).

Using B.6 and B.8 as guidelines, analyse Figure C.4.

C.2.2 Explanation

The following points should assist in understanding the analysis made of the example and the associated SAFE chart.

— The PSL sensor in the fuel supply line is not required on a natural-draft burner because of the low air intake pressure.

— The LSL cannot be eliminated because of fire tube exposure.

— Due to the internal design of the vessel, an additional LSL (LSL 2) is required. The blowby of the level control valve was calculated and it exceeded the process capacity of the downstream component. LSL 2 and an SDV were added to protect the downstream component from blowby.

— FSV 3 is not required because the regulator effectively minimizes backflow.

— It is not necessary to install two media TSHs in the vessel, i.e. one for the vessel and the other for the fired component. One TSH provides adequate protection, and it is mounted in the liquid portion of the vessel.

— Figure C.5 represents the heater after analysis. The safety devices that have been eliminated are indicated by dashed circles. Figure C.6 is the corresponding SAFE chart for Figure C.5.

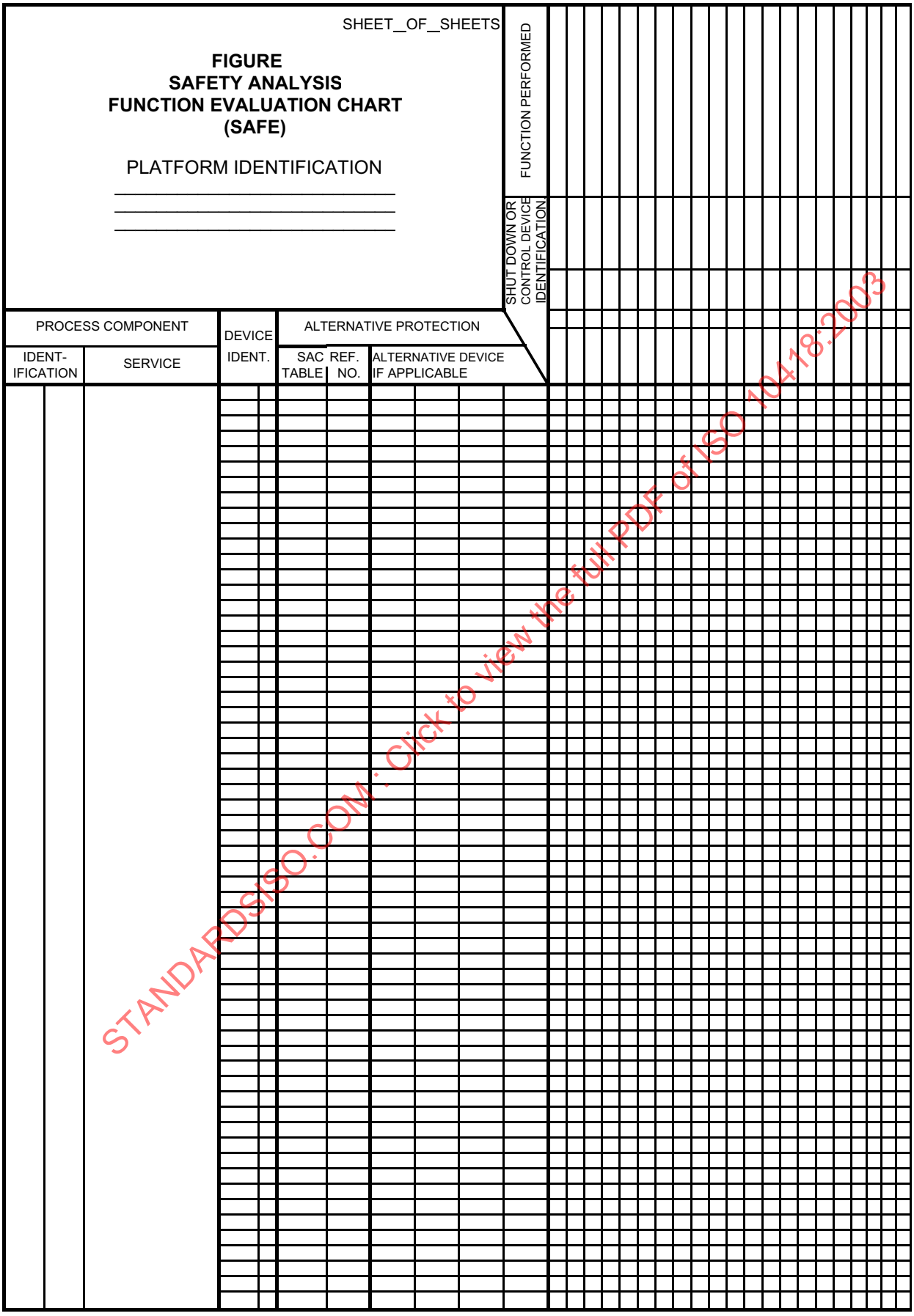


Figure C.1 — Safety analysis function evaluation chart (SAFE)

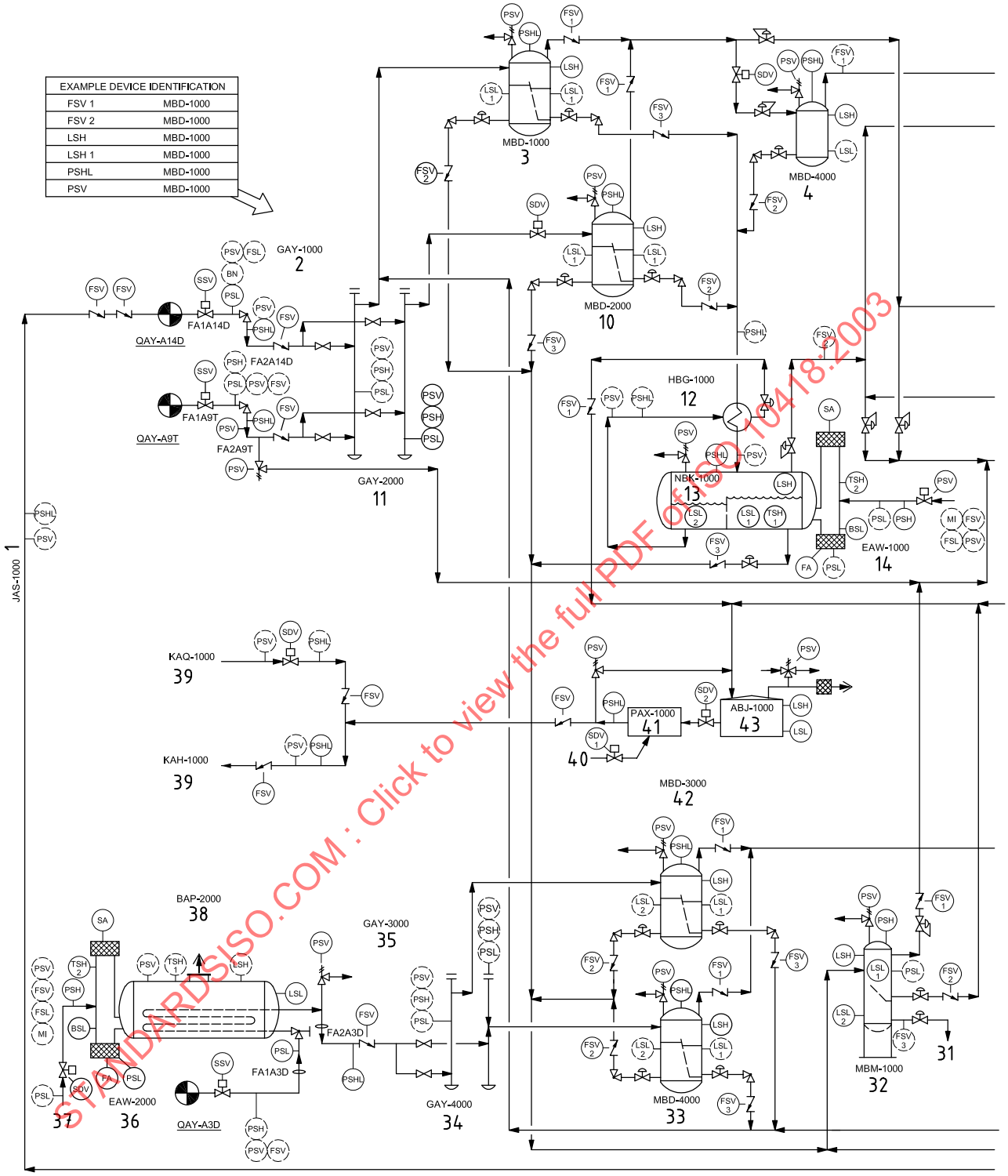


Figure C.2 — Example flow diagram of platform production process

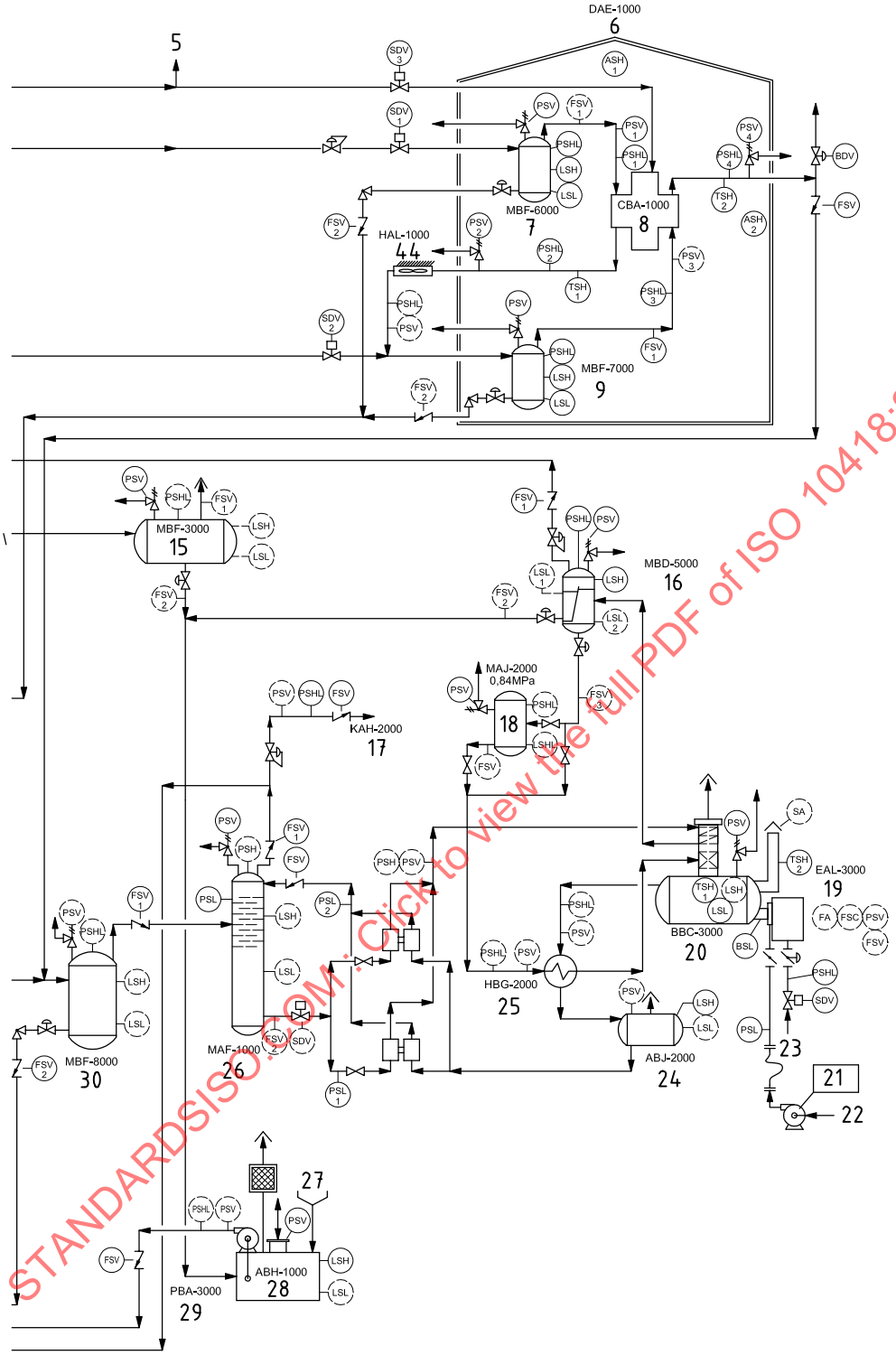


Figure C.2 (*continued*)

Key

1 gas lift line
2 L.P. prod. header, MWP — 9,6 MPa
3 L.P. prod. separator, MWP — 3,34 MPa
4 fuel and instrument gas scrubber, MWP — 0,84 MPa
5 to instrument and fuel systems
6 compressor building
7 suction scrubber, MWP — 0,84 MPa
8 compressor
9 interstage scrubber, MWP — 3,34 MPa
10 L.P. test separator, MWP — 3,34 MPa
11 L.P. test header, MWP — 9,6 MPa
12 heat exchanger, MWP — 3,34 MPa
13 heater-treater, MWP — 0,5 MPa
14 fired component
15 flare scrubber, MWP — 0,5 MPa
16 flash separator, MWP — 0,84 MPa
17 departing gas sales line, MOP — 9,6 MPa
18 filter
19 fire component forced draft
20 reboiler, MWP — 0,1 MPa
21 motor interlock
22 atmosphere
23 fuel gas
24 glycol surge tank, MWP — 0,1 MPa
25 heat exchanger, MWP — 0,1 MPa
26 contact, MWP — 9,6 MPa
27 drip pans
28 sump
29 sump pump
30 H.P. scrubber, MWP — 9,6 MPa
31 overboard
32 skimmer tank, MWP — 0,17 MPa
33 H.P. test separator, MWP — 9,6 MPa
34 H.P. test header, MWP — 33,4 MPa
35 H.P. prod. header, MWP — 33,4 MPa
36 fired component (natural draft)
37 fuel in
38 line header (indirect)
39 oil pipeline
40 fuel gas
41 pump
42 H.P. prod. separator, MWP — 9,6 MPa
43 atmospheric tank
44 gas cooler

NOTE 1 Manual block valves are not shown except on header. Valving on this drawing is limited to that necessary for control and shut down.

NOTE 2 Dashed symbols represent devices shown on the SAT, but have been eliminated in accordance with 5.3.3.2. For clarity, dashed symbols are not shown on the flowlines or header.

NOTE 3 Fusible plugs (TSE) installed in accordance with guidelines in Table D.1.

NOTE 4 Operational control devices are not shown unless relevant to the safety analysis.

Figure C.2 (*continued*)

SHEET 1 OF 6

SAFETY ANALYSIS
FUNCTION EVALUATION CHART
(SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

APP'D	MARK	DESCRIPTION	BY	DATE

PROCESS COMPONENTS: IDENTIFICATION		PROCESS COMPONENTS: SERVICE	DEVICE IDENT.	SAC REF. TABLE	SAC REF. NO.	ALTERNATIVE PROTECTION: ALTERNATIVE DEVICE IF APPLICABLE			SSV QAY A14D SHUT IN WELL	SSV QAY A9T SHUT IN WELL	SSV QAY A3D SHUT IN WELL	SDV MBD 2000 SHUT OFF INFLOW	SDV EAW 1000 SHUT OFF FUEL	SDV 1 CBA 1000 SHUT OFF INFLOW	SDV 2 CBA 1000 SHUT OFF INFLOW	SDV 3 CBA 1000 SHUT OFF FUEL	BDV CBA 1000 BLOWDOWN COMPRESSOR	SDV 1 PAX 1000 SHUT OFF FUEL	SDV 2 PAX 1000 SHUT OFF INFLOW	SDV KAQ 1000 SHUT OFF INFLOW	SDV EAW 2000 SHUT OFF FUEL	SDV PBA 1000&2000 SHUT OFF INFLOW	SDV EAL 3000 SHUT OFF FUEL	SDV MBF 4000 SHUT OFF INFLOW	PBA 3000 SHUT DOWN PUMP				ALARM	FA PREVENT FLAME EMISSION	SA PREVENT SPARK EMISSION	PSV PRESSURE RELIEF	PSV VACUUM RELIEF	FSV MINIMIZE BACKFLOW
FA1	A14D	UPSTREAM FLOWLINE SEGMENT	PSH	B.2	a.2	PSH	FA2	A14D																									
			PSL						•																			•					
			PSV	B.2	c.2																												
			FSV	B.2	d.2	FSV	FA2	A14D																									
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
FA2	A14D	DOWNSTREAM FLOWLINE SEGMENT	PSH						•																			•					
			PSL						•																			•					
			PSV	B.2	c.2																												
			FSV																														•
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
FA1	A9T	UPSTREAM FLOWLINE SEGMENT	PSH	B.2	a.2	PSH	FA2	A9T																									
			PSL	B.2	b.2																												
			PSV	B.2	c.2																												
			FSV	B.2	d.2	FSV	FA2	A9T																									
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
FA2	A9T	DOWNSTREAM FLOWLINE SEGMENT	PSH							•																		•					
			PSL							•																		•					
			PSV																												•		
			FSV																														•
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
FA1	A3D	UPSTREAM FLOWLINE SEGMENT	PSH	B.2	a.2	PSH	FA2	A3D																									
			PSL								•																	•					
			PSV	B.2	c.2																												
			FSV	B.2	d.2	FSV	FA2	A3D																									
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
FA2	A3D	DOWNSTREAM FLOWLINE SEGMENT	PSH								•																	•					
			PSL								•																	•					
			PSV																												•		
			FSV																														•
			TSH	B.2	e.2																												
			TSL	B.2	f.2																												
JAS	1000	GAS LIFT LINE	PSH	B.4	a.2	PSH	MBD	3000																									
						PSH	MBD	4000																									
			PSL	B.4	b.2	PSL	MAF	1000																									
			PSV	B.4	c.2																												
				B.4	c.3	PSV	MAF	1000																									
			FSV																														•
			TSH	B.4	e.2																												
			TSL	B.4	f.2																												
GAY	1000	LOW PRESSURE PRODUCTION HEADER	PSH	B.6	a.2	PSH	FA2	A14D																									
						PSH	FA2	A9T																									
			PSL	B.6	b.2	PSL	FA2	A14D																									
						PSL	FA2	A9T																									
			PSV	B.6	c.4																												
			TSH	B.6	d.2																												
			TSL	B.6	e.2																												
GAY	2000	LOW PRESSURE TEST HEADER	PSH	B.6	a.2	PSH	FA2	A14D																									
						PSH	FA2	A9T																									
			PSL	B.6	b.2	PSL	FA2	A14D																									
						PSL	FA2	A9T																									
			PSV	B.6	c.4																												
			TSH	B.6	d.2																												
			TSL	B.6	e.2																												

Figure C.3 — Safety analysis function evaluation chart (SAFE) example

SHEET 2 OF 6

SAFETY ANALYSIS FUNCTION EVALUATION CHART (SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

APP'D	MARK	DESCRIPTION	BY	DATE

PROCESS COMPONENTS: IDENTIFICATION		PROCESS COMPONENTS: SERVICE	DEVICE IDENT.		SAC REF. TABLE	SAC REF. NO.	ALTERNATIVE PROTECTION: ALTERNATIVE DEVICE IF APPLICABLE				SHUT IN WELL QAY A14D SSV	SHUT IN WELL QAY A9T SSV	SHUT IN WELL QAY A3D SSV	SHUT OFF INFLOW MBD 2000 SDV	SHUT OFF FUEL EAW 1000 SDV	SHUT OFF INFLOW CBA 1000 1 SDV	SHUT OFF INFLOW CBA 1000 2 SDV	SHUT OFF FUEL CBA 1000 3 SDV	BLOWDOWN COMPRESSOR CBA 1000 BDV	SHUT OFF FUEL PAX 1000 1 SDV	SHUT OFF INFLOW PAX 1000 2 SDV	SHUT OFF INFLOW KAQ 1000 SDV	SHUT OFF FUEL EAW 2000 SDV	SHUT OFF INFLOW PBA 1000&2000 SDV	SHUT OFF FUEL EAL 3000 SDV	SHUT OFF INFLOW MBF 4000 SDV	SHUT DOWN PUMP PBA 3000				ALARM	PREVENT FLAME EMISSION FA	PREVENT SPARK EMISSION SA	PRESSURE RELIEF PSV	VACUUM RELIEF PSV	MINIMIZE BACKFLOW FSV
GAY	3000	HIGH PRESSURE PRODUCTION HEADER	PSH		B.6	a.2	PSH		FA2	A3D																										
			PSL		B.6	b.2	PSL		FA2	A3D																										
			PSV		B.6	c.4																														
			TSH		B.6	d.2																														
			TSL		B.6	e.2																														
GAY	4000	HIGH PRESSURE TEST HEADER	PSH		B.6	a.2	PSH		FA2	A3D																										
			PSL		B.6	b.2	PSL		FA2	A3D																										
			PSV		B.6	c.4																														
			TSH		B.6	d.2																														
			TSL		B.6	e.2																														
MBD	1000	LOW PRESSURE PRODUCTION SEPARATOR	PSH								●	●	●			●	●	●	●												●					
			PSL								●	●	●			●	●	●	●												●					
			PSV																															●		
			LSH								●	●	●			●	●	●	●												●					
		OIL	LSL	1	B.8	e.3																														
		WATER	LSL	2	B.8	e.3																														
		GAS	FSV	1																																●
		WATER	FSV	2																																●
		OIL	FSV	3																																●
			LSH		B.8	h.1																														
			LSL		B.8	i.1																														
MBD	2000	LOW PRESSURE TEST SEPARATOR	PSH											●																	●					
			PSL											●																	●					
			PSV																															●		
			LSH											●																	●					
		OIL	LSL	1	B.8	e.3																														
		WATER	LSL	2	B.8	e.3																														
		GAS	FSV	1																																●
		WATER	FSV	2																																●
		OIL	FSV	3																																●
			LSH		B.8	h.1																														
			LSL		B.8	i.1																														
MBD	3000	HIGH PRESSURE PRODUCTION SEPARATOR	PSH										●																		●					
			PSL										●																		●					
			PSV																															●		
			LSH										●																		●					
		OIL	LSL	1	B.8	e.3																														
		WATER	LSL	2	B.8	e.3																														
		GAS	FSV	1																																●
		WATER	FSV	2																																●
		OIL	FSV	3																																●
			LSH		B.8	h.1																														
			LSL		B.8	i.1																														
MBD	4000	HIGH PRESSURE TEST SEPARATOR	PSH										●																		●					
			PSL										●																		●					
			PSV																															●		
			LSH										●																		●					
		OIL	LSL	1	B.8	e.3																														
		WATER	LSL	2	B.8	e.3																														
		GAS	FSV	1																																●
		WATER	FSV	2																																●
		OIL	FSV	3																																●
			LSH		B.8	h.1																														
			LSL		B.8	i.1																														
MBD	5000	GLYCOL FLASH SEPARATOR	PSH																					●							●					
			PSL																					●							●					
			PSV																															●		
			LSH																					●							●					
		OIL	LSL	1	B.8	e.3																														
		GLYCOL	LSL	2	B.8	e.3																														
		GAS	FSV	1																																●
		OIL/COND	FSV	2	B.8	f.3																														
		GLYCOL	FSV	3	B.8	f.3																														
			LSH		B.8	h.1																														
			LSL		B.8	i.1																														

Figure C.3 (*continued*)

SHEET 3 OF 6

SAFETY ANALYSIS FUNCTION EVALUATION CHART (SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

APP'D	MARK	DESCRIPTION	BY	DATE

PROCESS COMPONENTS IDENTIFICATION		SERVICE		DEVICE IDENT.		SAC REF. TABLE	SAC REF. NO.	ALTERNATIVE PROTECTION: ALTERNATIVE DEVICE IF APPLICABLE				SSV / QAY A14D / SHUT IN WELL	SSV / QAY A9T / SHUT IN WELL	SSV / QAY A3D / SHUT IN WELL	SDV / MBD 2000 / SHUT OFF INFLOW	SDV / EAW 1000 / SHUT OFF FUEL	SDV / CBA 1000 1 / SHUT OFF INFLOW	SDV / CBA 1000 2 / SHUT OFF INFLOW	SDV / CBA 1000 3 / SHUT OFF FUEL	BDV / CBA 1000 / BLOWDOWN COMPRESSOR	SDV / PAX 1000 1 / SHUT OFF FUEL	SDV / PAX 1000 2 / SHUT OFF INFLOW	SDV / KAQ 1000 / SHUT OFF INFLOW	SDV / EAW 2000 / SHUT OFF FUEL	SDV / PBA 1000&2000 / SHUT OFF INFLOW	SDV / EAL 3000 / SHUT OFF FUEL	SDV / MBF 4000 / SHUT OFF INFLOW	PBA 3000 / SHUT DOWN PUMP				ALARM	FA / PREVENT FLAME EMISSION	SA / PREVENT SPARK EMISSION	PSV / PRESSURE RELIEF	PSV / VACUUM RELIEF	FSV / MINIMIZE BACKFLOW
MBF	3000	FLARE SCRUBBER		PSH		B.8	a.6																														
				PSL		B.8	b.2																														
				PSV																														•		
				LSH								•	•	•																		•					
				LSL		B.8	e.3																														
			GAS	FSV	1	B.8	f.2																														
			LIQUID	FSV	2	B.8	f.2																														
				LSH		B.8	h.3																														
				LSL		B.8	i.1																														
MBF	4000	FUEL AND INSTRUMENT SCRUBBER		PSH																								•				•					
				PSL																								•				•					
				PSV																														•		
				LSH																								•				•					
				LSL		B.8	e.3																														
			GAS	FSV	1	B.8	f.2																														
			LIQUID	FSV	2																																•
				LSH		B.8	h.3																														
				LSL		B.8	i.1																														
MBM	1000	SKIMMER TANK		PSH								•	•	•		•	•	•	•										•			•					
				PSL		B.8	b.6																														
				PSV																														•		
				LSH								•	•	•		•	•	•	•										•			•					
			OIL	LSL	1							•	•	•		•	•	•	•										•			•					
			WATER	LSL	2							•	•	•		•	•	•	•										•			•					
			GAS	FSV	1																																•
			OIL	FSV	2																																•
			WATER	FSV	3	B.8	f.2																														
				LSH		B.8	h.1																														
				LSL		B.8	i.1																														
MAJ	2000	GLYCOL FILTER		PSH		B.8	a.3	PSH		MBD	3000																										
				PSL		B.8	b.2																														
				PSV		B.8	c.2																												•		
				LSH		B.8	d.3																														
				LSL		B.8	e.2																														
				FSV		B.8	f.2																														
				LSH		B.8	h.1																														
				LSL		B.8	i.1																														
MBF	6000	COMPRESSOR SUCTION SCRUBBER		PSH													•	•	•	•												•					
				PSL													•	•	•	•												•					
				PSV																														•		
				LSH													•	•	•	•												•					
				LSL													•	•	•	•												•					
			GAS	FSV	1	B.8	f.2																														
			WATER	FSV	2																																•
				LSH		B.8	h.3																														
				LSL		B.8	i.1																														
MBF	7000	COMPRESSOR INTERSTAGE SCRUBBER		PSH													•	•	•	•												•					
				PSL													•	•	•	•												•					
				PSV																														•		
				LSH													•	•	•	•												•					
				LSL													•	•	•	•												•					
			GAS	FSV	1	B.8	f.2																														
			WATER	FSV	2																																•
				LSH		B.8	h.3																														
				LSL		B.8	i.1																														
ABJ	1000	ATMOSPHERIC TANK		VENT																														•	•	
				PSV																														•		
				LSH								•	•	•			•	•	•	•												•					
				LSL								•	•	•			•	•	•	•												•					
ABJ	2000	GLYCOL SURGE TANK		VENT																														•	•	
				PSV		B.10	b.3																														
				LSH																					•							•					
				LSL		B.10	d.3																														

Figure C.3 (*continued*)

SHEET 4 OF 6

SAFETY ANALYSIS FUNCTION EVALUATION CHART (SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

APP'D	MARK	DESCRIPTION	BY	DATE

PROCESS COMPONENTS				DEVICE IDENT.		ALTERNATIVE PROTECTION					FUNCTION PERFORMED	SHUT IN WELL	SHUT IN WELL	SHUT IN WELL	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF INFLOW	SHUT OFF FUEL	BLOWDOWN COMPRESSOR	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT DOWN PUMP				ALARM	PREVENT FLAME EMISSION	PREVENT SPARK EMISSION	PRESSURE RELIEF	VACUUM RELIEF	MINIMIZE BACKFLOW
											SHUTDOWN OR CONTROL DEVICE IDENTIFICATION	QAY A14D	QAY A9T	QAY A3D	MBD 2000	EAW 1000	CBA 1000 1	CBA 1000 2	CBA 1000 3	CBA 1000	PAX 1000 1	PAX 1000 2	KAQ 1000	EAW 2000	PBA 1000&2000	EAL 3000	MBF 4000	PBA 3000									
IDENTIFICATION		SERVICE				SAC REF. TABLE	NO.	ALTERNATIVE DEVICE IF APPLICABLE				SSV	SSV	SSV	SDV	SDV	SDV	SDV	SDV	BDV	SDV	SDV	SDV	SDV	SDV	SDV	SDV						FA	SA	PSV	PSV	FSV
MBF	8000	COMPRESSOR		PSH		B.8	a.3	PSH		MBD	3000																									
		HIGH PRESSURE						PSH		MBD	4000																									
		SCRUBBER						PSH	4	CBA	1000																									
				PSL		B.8	b.3	PSL		MBD	3000																									
								PSL		MBD	4000																									
								PSL	4	CBA	1000																									
				PSV																												●		
				LSH		B.8	d.2																												
				LSL		B.8	e.3																												
			GAS	FSV	1																															●
			LIQUID	FSV	2																															●
				LSH		B.8	h.1																												
				LSL		B.8	i.1																												
MAF	1000	GLYCOL		PSH		B.8	a.3	PSH		MBD	3000																									
		CONTACTOR						PSH		MBD	4000																									
								PSH	4	CBA	1000																									
				PSL										●			●	●	●	●													●					
				PSV																												●		
				LSH		B.8	d.2																												
				LSL		B.8	e.2																												
			GAS	FSV	1																															●
			LIQUID	FSV	2	B.8	f.3																												
				LSH		B.8	h.1																												
				LSL		B.8	i.1																												
ABH	1000	SUMP		VENT																												●	●	
				PSV																												●		
				LSH								●	●	●																		●					
				LSL		B.10	d.4																												
NBK	1000	HEATER		PSH								●	●	●		●	●	●	●	●												●					
		TREATER		PSL								●	●	●		●	●	●	●	●												●					
				PSV																												●		
				LSH								●	●	●		●	●	●	●	●												●					
			WATER	LSL	1							●	●	●		●	●	●	●	●												●					
			OIL	LSL	2							●	●	●		●	●	●	●	●												●					
			OIL	FSV	1																															●
			GAS	FSV	2	B.8	f.3																												
			WATER	FSV	3																															●
				TSH								●	●	●		●	●	●	●	●												●					
				LSH		B.8	h.1																												
				LSL		B.8	i.1																												
BAP	2000	LINE HEATER		VENT																												●	●	
		(INDIRECT)		PSV		B.10	b.4																												
				LSH		B.10	c.2																												
				LSL																			●								●					
				TSH	1	B.10	e.3																												
BBC	3000	REBOILER		VENT																												●	●	
		(GLYCOL)		PSV																												●		
				LSH		B.10	c.3																												
				LSL																					●						●					
				TSH	1																					●						●					
EAW	1000	FIRED	FLUID	TSH	1	B.14	a.1	TSH	1	NBK	1000																									
		COMPONENT		TSH	2							●	●	●		●															●					
		(NATURAL	AIR	PSL		B.14	d.2																												
		DRAFT FOR	FUEL	PSH												●															●					
		HEATER	FUEL	PSL		B.14	f.2																												
		TREATER)		BSL												●															●					
				FSL		B.14	h.2																												
				MI		B.14	i.2																												
				FA																													●				
				SA																														●			
				PSV		B.14	l.2																												
				FSV		B.14	m.1	FSV	1,2,3	NBK	1000																									

Figure C.3 (*continued*)

SHEET 5 OF 6

SAFETY ANALYSIS
FUNCTION EVALUATION CHART
(SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

APP'D	MARK	DESCRIPTION	BY	DATE

PROCESS COMPONENTS / DEVICE IDENT. / ALTERNATIVE PROTECTION / SHUTDOWN OR CONTROL DEVICE IDENTIFICATION / FUNCTION PERFORMED

IDENTIFICATION		SERVICE	DEVICE IDENT.		SAC REF. TABLE	SAC REF. NO.	ALTERNATIVE DEVICE IF APPLICABLE				SSV QAY A14D SHUT IN WELL	SSV QAY A9T SHUT IN WELL	SSV QAY A3D SHUT IN WELL	SDV MBD 2000 SHUT OFF INFLOW	SDV EAW 1000 SHUT OFF FUEL	SDV CBA 1000 1 SHUT OFF INFLOW	SDV CBA 1000 2 SHUT OFF INFLOW	SDV CBA 1000 3 SHUT OFF FUEL	BDV CBA 1000 BLOWDOWN COMPRESSOR	SDV PAX 1000 1 SHUT OFF FUEL	SDV PAX 1000 2 SHUT OFF INFLOW	SDV KAQ 1000 SHUT OFF INFLOW	SDV EAW 2000 SHUT OFF FUEL	SDV PBA 1000&2000 SHUT OFF INFLOW	SDV EAL 3000 SHUT OFF FUEL	SDV MBF 4000 SHUT OFF INFLOW	PBA 3000 SHUT DOWN PUMP	ALARM	FA PREVENT FLAME EMISSION	SA PREVENT SPARK EMISSION	PSV PRESSURE RELIEF	PSV VACUUM RELIEF	FSV MINIMIZE BACKFLOW
EAW	2000	FIRED FLUID	TSH	1	B.14	a.1	TSH	1	NBK	1000																							
		COMPONENT	TSH	2																			•					•					
		(NATURAL AIR	PSL		B.14	d.2																											
		DRAFT FOR FUEL	PSH																				•					•					
		LINE HEATER) FUEL	PSL		B.14	f.2																											
			BSL																				•					•					
			FSL		B.14	h.2																											
			MI		B.14	i.2																											
			FA																										•				
			SA																											•			
			PSV		B.14	l.2																											
			FSV		B.14	m.3																											
EAL	3000	FIRED FLUID	TSH	1	B.14	a.1	TSH	1	BBC	3000																							
		COMPONENT	TSH	2																				•	•			•					
		(FORCED AIR	PSL																						•			•					
		DRAFT FOR FUEL	PSH																						•			•					
		REBOILER) FUEL	PSL																						•			•					
			BSL																						•			•					
			FSL		B.14	h.2																											
			MI																						•			•					
			FA		B.14	j.2																											
			SA		B.14	k.2																											
			PSV		B.14	l.1	PSV		BBC	3000																							
			FSV		B.14	m.3																											
PAX	1000	PIPELINE PUMP	PSH																	•	•							•					
			PSL																	•	•							•					
			PSV																												•		
			FSV																														•
			TSH		B.17	h.2																											
			TSL		B.17	i.2																											
			FSL		B.17	j.2																											
PBA	1000	GLYCOL PUMP	PSH		B.17	b.6																											
	2000	(TYPICAL OF WET GLYCOL	PSL	1																				•				•					
		TWO) DRY GLYCOL	PSL	2																				•				•					
			PSV		B.17	f.2																											
			FSV																														•
			TSH		B.17	h.2																											
			TSL		B.17	i.2																											
			FSL		B.17	j.3																											
PBA	3000	SUMP PUMP	PSH		B.17	b.2																											
			PSL		B.17	d.5																											
			PSV		B.17	f.2																											
			FSV																														•
			TSH		B.17	h.2																											
			TSL		B.17	i.2																											
			FSL		B.17	j.2																											
KAH	1000	DEPARTING OIL SALES LINE	PSH										•			•	•	•	•									•					
			PSL										•			•	•	•	•									•					
			PSV		B.21	c.2																											
			FSV																														•
			TSH		B.21	e.2																											
			TSL		B.21	f.2																											
KAQ	1000	INCOMING OIL SALES LINE	PSH		B.21	a.2																											
			PSL		B.21	b.2																											
			PSV		B.21	c.2																											
			FSV																														•
			TSH		B.21	e.2																											
			TSL		B.21	f.2																											
KAH	2000	DEPARTING GAS SALES LINE	PSH																	•	•	•						•					
			PSL																	•	•	•						•					
			PSV		B.21	c.2																											
			FSV																														•
			TSH		B.21	e.2																											
			TSL		B.21	f.2																											

Figure C.3 (*continued*)

SHEET 6 OF 6

SAFETY ANALYSIS FUNCTION EVALUATION CHART (SAFE)

PLATFORM IDENTIFICATION:

NOTES: (1) * INDICATES DEVICE INSTALLED BUT NOT REQUIRED.

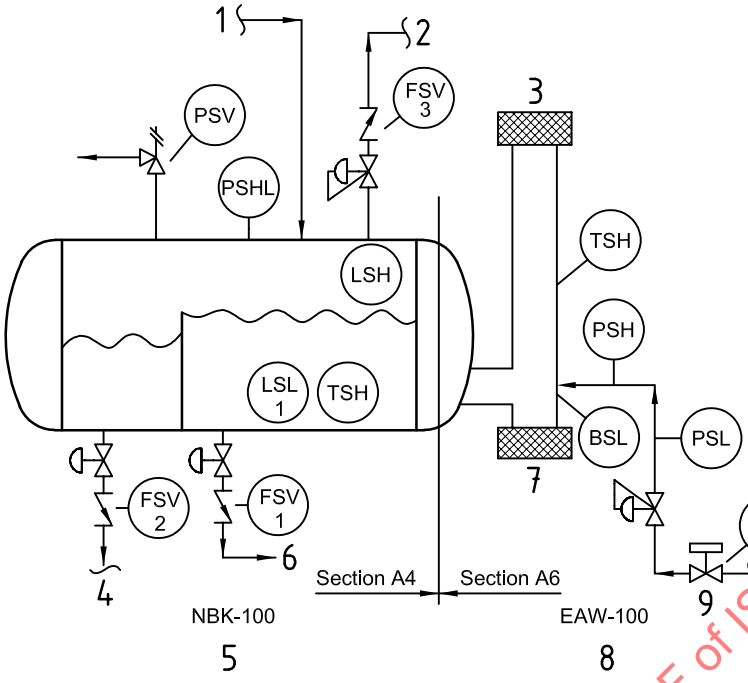
APP'D	MARK	DESCRIPTION	BY	DATE

FUNCTION PERFORMED

SHUTDOWN OR CONTROL DEVICE IDENTIFICATION

PROCESS COMPONENTS IDENTIFICATION		PROCESS COMPONENTS SERVICE	DEVICE IDENT.		ALTERNATIVE PROTECTION SAC REF. TABLE	SAC REF. NO.	ALTERNATIVE DEVICE IF APPLICABLE				SHUT IN WELL	SHUT IN WELL	SHUT IN WELL	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF INFLOW	SHUT OFF FUEL	BLOWDOWN COMPRESSOR	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT OFF FUEL	SHUT OFF INFLOW	SHUT DOWN PUMP				ALARM	PREVENT FLAME EMISSION	PREVENT SPARK EMISSION	PRESSURE RELIEF	VACUUM RELIEF	MINIMIZE BACKFLOW
											A14D	A9T	A3D	2000	1000	1000	1000	1000	1000	1000	1000	1000	2000	1000&2000	3000	4000	3000									
											QAY	QAY	QAY	MBD	EAW	CBA	CBA	CBA	CBA	PAX	PAX	KAQ	EAW	PBA	EAL	MBF	PBA									
																1	2	3		1	2															
											SSV	SSV	SSV	SDV	SDV	SDV	SDV	SDV	BDV	SDV	SDV	SDV	SDV	SDV	SDV	SDV						FA	SA	PSV	PSV	FSV
CBA	1000	COMPRESSOR	PSH	1	B.19	a.2	PSH		MBF	6000																										
			PSH	2												•	•	•	•												•					
			PSH	3	B.19	a.2	PSH		MBF	7000																										
			PSH	4												•	•	•	•												•					
			PSL	1	B.19	c.2	PSL		MBF	6000																										
			PSL	2												•	•	•	•												•					
			PSL	3	B.19	c.2	PSL		MBF	7000																										
			PSL	4												•	•	•	•												•					
			PSV	1	B.19	e.2	PSV		MBF	6000																										
			PSV	2																														•		
			PSV	3	B.19	e.2	PSV		MBF	7000																										
			PSV	4																														•		
			FSV																																	•
			TSH	1												•	•	•	•												•					
			TSH	2												•	•	•	•												•					
			YSH		B.19	i.2																														
			TSL		B.19	j.2																														
HAL	1000	GAS COOLER (SHELL IS ATMOSPHERIC) TUBE	PSH		B.23	a.3	PSH	4	CBA	1000																										
			PSL		B.23	b.3	PSL	4	CBA	1000																										
			PSV		B.23	c.3	PSV	4	CBA	1000																										
			TSH		B.23	d.2																														
			TSL		B.23	e.2																														
HBG	1000	HEAT EXCHANGER (HEATER TREATER)	TSL		B.23	a.3	PSH		NBK	1000																										
			PSL		B.23	b.3	PSL		NBK	1000																										
			PSV		B.23	c.3	PSV		NBK	1000																										
			TSH		B.23	d.2																														
			TSL		B.23	e.2																														
		TUBE	PSH		B.23	a.4	PSH		NBK	1000																										
			PSL		B.23	b.3	PSL		NBK	1000																										
			PSV		B.23	c.4	PSV		NBK	1000																										
			TSH		B.23	d.2																														
			TSL		B.23	e.2																														
HBG	2000	HEAT EXCHANGER (REBOILER) SHELL	PSH		B.23	a.2																														
			PSL		B.23	b.2																														
			PSV		B.23	c.3	PSV		BBC	1000																										
			TSH		B.23	d.2																														
			TSL		B.23	e.2																														
		TUBE	PSH		B.23	a.4	PSH		MBD	5000																										
			PSL		B.23	b.2																														
			PSV		B.23	c.4	PSV		BBC	1000																										
			TSH		B.23	d.2																														
			TSL		B.23	e.2																														
		EMERGENCY SUPPORT SYSTEMS																																		
DAE	1000	COMPRESSOR BUILDING	ASH	1												•	•	•	•												•					
			ASH	2												•	•	•	•												•					
LAG	A001	ESD STATIONS MANUAL VALVES	ESD								•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•				•					
LAG	A002	FUSIBLE LOOPS	TSE								•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•				•					

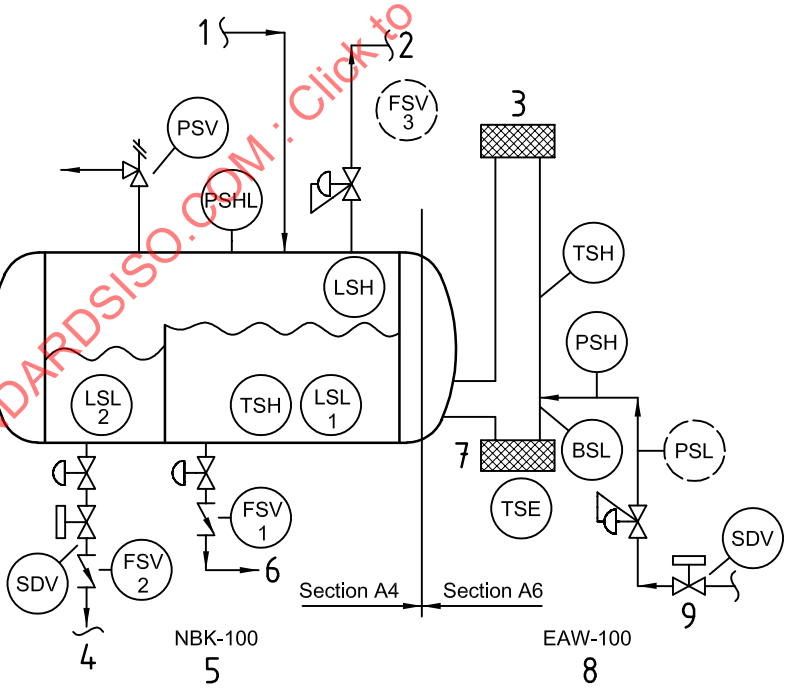
Figure C.3 (*continued*)



Key

1 inlet
2 gas outlet
3 stack arrestor
4 oil outlet
5 heater-treater MAWP = 100 kPa at 93 °C
6 water outlet
7 flame arrestor
8 fired component (natural draft)
9 fuel gas

Figure C.4 — Simplified diagram showing required safety devices



Key

1 inlet
2 gas outlet
3 stack arrestor
4 oil outlet
5 heater-treater MAWP = 100 kPa at 93 °C
6 water outlet
7 flame arrestor
8 fired component (natural draft)
9 fuel gas

Figure C.5 — Heater safety devices (see Figure C.4) after analysis

FIGURE
SAFETY ANALYSIS
FUNCTION EVALUATION CHART
(SAFE)

O.C.S NO.
FIELD: EXAMPLE - FOR FIGURE C.5
BLOCK NO. _____ **PLATFORM.**
PREV.: _____ **DATE:** _____ **BY:**
PREV. NO. 0 **DATE:** _____ **BY:**
DWG. # _____ **SHEET** 1 **OF** 1 **SHEETS**

FUNCTION PERFORMED

	SHUT DOWN OR CONTROL DEVICE IDENTIFICATION	SHUT IN PROCESS	SHUT IN COMPONENT		SHUT OFF OIL OUTLET	RELIEVE PRESSURE	MINIMIZE BACKFLOW	PREVENT FLAME EMISSION	PREVENT SPARK EMISSION
		100	100		100				
		EAW	EAW		NBK				
		SDV	SDV		SDV				

PROCESS COMPONENT IDENT-IFICATION		PROCESS COMPONENT SERVICE	DEVICE IDENT.		ALTERNATIVE PROTECTION SAC TABLE	ALTERNATIVE PROTECTION REF. NO.	ALTERNATIVE DEVICE IF APPLICABLE
NBK	100	HEATER TREATER	PSH				
			PSL				
			PSV				
			LSH				
			LSL	1			
			LSL	2			
			FSV	1			
			FSV	2			
			FSV	3	B.8	f.3	
			TSH				
EAW	100	FIRED COMPONENT (NATURAL DRAFT) HEATER TREATER	TSH				
			PSL		B.14	d.2	
			PSH				
			PSL		B.14	f.2	
			BSL				
			FSL		B.14	h.2	
			FA				
			SA				

Figure C.6 — Safety analysis function evaluation chart (SAFE) for Figure C.5

Annex D
(informative)

Support systems

D.1 General

ESSs and other support systems provide a method of performing specific safety functions common to the entire platform. The ESS includes ESD, fire detection, gas detection, EDP, ventilation, containment systems and sumps, and SSSV systems. These are essential systems that provide a level of protection to the facility by initiating shut-in functions or reacting to minimize the consequences of released hydrocarbons. To ensure shut-in of the installation and safe disposal of inventory during emergency conditions, the ESS should take action independent of the process safety system to actuate final-end elements. For example, the ESS should dump air supply to SDVs, trip control voltage for motor starters and where necessary blow down the inventory to a safe location.

The other support systems include the pneumatic supply systems, hydraulic supply systems, systems for discharging gas to the atmosphere, systems for containing leaks or spills, and any other service system that might enhance platform safety. The pneumatic and hydraulic supply system provides a control medium for the safety system, and the systems for discharging gas to the atmosphere provide a means for doing so under safe, controlled conditions.

D.2 Emergency support systems (ESS)

D.2.1 Emergency shutdown (ESD) system

D.2.1.1 Purpose

An ESD system is a system of manual control stations strategically located on a platform that, when activated, will initiate shutdown of all wells and other process stations. The ESD system may also initiate EDP through the system provided for discharging gas to atmosphere (see also D.5). The ESD system may also be initiated automatically when process conditions indicate a loss of control which requires ESD, e.g. low air pressure, high liquid level in a flare system. The system may include a number of independent process shutdown systems that can also be actuated separately. Activation of the ESD system should result in the termination of all production activity on the platform, including the closing of all pipeline SDVs. The ESD system should be designed to permit continued operation of electrical power generating stations and fire-fighting systems when needed in an emergency.

The ESD system provides a means for personnel to manually initiate platform shutdown when an abnormal condition is observed. Fusible elements of the fire loop, other types of fire and gas detection equipment and certain process protection devices may be integrated with the ESD system.

D.2.1.2 Shutdown stations

Stations for manual activation of the ESD system for complete platform shutdown should be installed at the following locations:

a) helicopter decks;

b) exit stairway landings at each deck level;

c) boat landings;

d) at the centre or each end of a bridge connecting two platforms;